Sicherheit der Washington DC-Plattform

Zuletzt aktualisiert: 17.12.2025

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung.®ine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken
sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern. Andere Unternehmens- und
Produktnamen können Marken der jeweiligen Unternehmen sein,
denen sie zugeordnet sind.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Automatische Übersetzung

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsverzeichnis

Instanz sichern **9**

Platform-Sicherheit **18**

Zertifikate 20

Zertifikate erkunden 21

Generieren eines LDAP-Client-Zertifikats 22

Ein Zertifikat wird in eine Instanz hochgeladen 24

Codesignatur 25

Codesignatur erkunden 29

Codesignatur konfigurieren 31

Codesignatur verwenden 47

Codesignaturreferenz 64

Sicherheitsrollen 69

Explizite Rollen 70

Rollen mit erhöhten Berechtigungen 77

Security Center 80

Homepage 82

Sicherheitshärtung 83

Sicherheitsscanner 90

Sicherheitsmetriken 93

Kritische Updates 98

Sicherheitslernen 101

Instanz-Sicherheitszentrum 101

Migration von Instance Security Center zu ServiceNow Security Center 111

Überwachen Sie Sicherheits-Ereignisse 114

Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften 120

Suchen Sie nach falschen Sicherheitsdefinitionen 130

Überwachen Sie Instanzmetriken 131

Aktivieren Sie die ISC-Schnittstelle Virtual Agent 144

Andere Einstellungen und Sicherheitsressourcen 146

Härtungseinstellungen für die Instanzsicherheit 148

Härtungseinstellungen 261

Baseline der Härtungseinstellungen 263

Zugriffssteuerung 279

API und Webservice 335

Architektur, Design und Bedrohungsmodellierung 350

Authentifizierung 361

Geschäftslogik 389

Kommunikation 392

Konfiguration 397

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz 408
Fehlerbehandlung und -protokollierung 411
Datei und Ressourcen 418
Böswilliger Code 426
Sitzungsverwaltung 428
Gespeicherte Kryptografie 443
Validierung, Bereinigung und Codierung 444
Encryption and Key Management 478
Key Management Framework erkunden 479
[store-future: BEGIN review]
[End]
Abonnementpaket für Verschlüsselung und Schlüsselverwaltung 481
Key Management Framework verstehen 482
Schlüsselverwaltungsaktionen 515
Importieren Sie einen Schlüssel aus einem Webservice 518
Key Management Framework Gesundheit 521
Bereiten Sie Ihre Instanz auf die Einstellung von GlideEncrypter vor 523
GlideEncrypter-Nutzung von 3DES für Passwort2-Felder veraltet 524
Key Management Framework Ressourcenaustausch 527
Verschlüsselung auf Spaltenebene 535
Column Level Encryption Enterprise 544
Infrastruktursicherheit 580
Password2-Verschlüsselung mit dem Key Management Framework (KMF) 582
Cloud-Verschlüsselung mit Schlüsselverwaltung 585
Datenbankverschlüsselung 607
Vollständige Festplattenverschlüsselung 612
Edge Encryption 613
Protokolle 753
Systemprotokolle 755
Log Export Service (LES) 769
Protokollierung, Audits und Fehler 785
Geheimnisverwaltung 786
Geheimnisverwaltung erkunden 787
Vom Client zugängliche geheime Schlüssel konfigurieren 791
Dashboard „Geheimnisverwaltung“ 805
ServiceNow Vault 816
Plattform-Datenschutz 820
Zugriffskontrolllistenregeln 821
Durchsuchen von Zugriffssteuerungslisten 822
Konfigurieren einer ACL-Regel 839
Contextual Security Manager 842
Erweiterte ACL-Konfiguration 847

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsattribute – Homepage....859
Sicherheitsattribute – Grundlagen....860
Erstellen Sie Sicherheitsattribute....861
Sicherheitsattribut Umfang....863
Data Classification....864
Datenklassifizierung erkunden....865
Demodaten des Plugins Data Classification werden installiert....867
Erstellen von Datenklassifizierungen....868
Datenklassifizierungen zu Wörterbucheinträgen zuweisen....869
Analysieren von Datenklassifizierungen mit dem Übersichts-Dashboard....870
Domänentrennung und Data Classification....873
Datenfilterung....873
Datenfilterung erkunden....874
Datenfilterung wird aktiviert....877
Erstellen von Datenfilterungsregeln....877
Betreffkriterien werden erstellt....880
Debugging von Datenfilterung....884
Datenschutz....885
Datenschutz erkunden....887
Domänentrennung und Datenschutz....888
Unterstützte Feldtypen für die Anonymisierung....888
Datenschutzrollen....889
Datenschutz (klassisch)....891
Datenschutz....903
Datenerkennung....921
Datenerkennung erkunden....922
Datenerkennung aktivieren....924
Klassifizieren Sie Daten auf der Seite Datenerkennung „ Ergebnisse“....925
Datenerkennung Aufträge....925
Datenerkennung Rollen....930
Datenerkennung Auftragsergebnisse....932
Daten-Discovery-API....933
Domänentrennung für Service Provider....937
Domänentrennung erkunden....939
Anwendungssupport für die Domänentrennung....958
Empfohlene Domain Separation-Verfahren für Service Provider....966
Hilfe zur Domänentrennung....1008
Einrichtung und Verwaltung der Domänentrennung....1010
Domain Separation Center....1047
Identität....1055
Zugriffsanalyse....1056
Zugriffsanalyse erkunden....1058

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsanalyse verwenden....1059
Berechtigungsauswertung....1079
Häufige Fragen....1081
Globale Identität....1087
Verbund-ID wird untersucht....1089
Zugriff auf Kriterien für föderierte IDs....1090
ID-Felder werden aktualisiert....1091
Identitäts- und Zugriffsaudit....1092
Identitäts- und Zugriffsaudit erkunden....1094
Audit-Ergebnisse....1095
Prüfbare Felder für Sicherheit....1099
Felder, die für Identitätszugriff und -audit unterstützt werden und nicht unterstützt werden....1103
Identity Center....1104
Identity Center erkunden....1106
Identity Center wird aktiviert....1106
Identity Center für -Benutzer....1106
Identitätsmetriken für Administratoren....1110
System für domänenübergreifendes Identitätsmanagement (SCIM)....1110
SCIM-Anbieter....1111
SCIM-Client....1131
Zugriffsverwaltung....1150
Authentifizierung....1151
Adaptive Authentifizierung....1154
API-Authentifizierung....1213
API-Zugriffsrichtlinie....1224
Zertifikatbasierte Authentifizierung....1254
Benutzerdefinierte URLs, die Ihrer Instanz zugeordnet sind....1262
LDAP-Integration....1270
Begrenzen Sie gleichzeitige Sitzungen....1338
Multifaktor-Authentifizierung (MFA)....1343
Single Sign-on (SSO) für mehrere Anbieter....1392
Eingehende und ausgehende OAuth-Authentifizierung....1493
Anforderungen an die Passwortkomplexität....1530
Selbstregistrierung bei Instanz ServiceNow....1543
Tokenbasierte Authentifizierung (Benutzeranmeldungen)....1555
Zero Trust-Zugriff....1569
Verbindung und Anmeldeinformationen....1583
Durchsuchen von Anmeldeinformationen, Verbindungen und Aliassen....1585
Erste Schritte mit Verbindungen....1600
Erste Schritte mit Anmeldeinformationen....1612
Authentifizierungsalgorithmen....1685
Sicherheit bei Anmeldung und Authentifizierung....1696

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden der Sicherheit bei Anmeldung und Authentifizierung....1698
Bestätigungsaufforderung für Abmeldung konfigurieren....1699
Anmeldeszenarien definieren....1699
Referenzbeispiel: Der Standard-Selfservice-Prozess Passwortzurücksetzung 1703
Webservice-Sicherheit....1717
Sicherheit von Webservices erkunden....1718
Konfigurieren der gegenseitigen Authentifizierung....1720
Referenz: WS-Security....1723
Allgemeine Einstellungen für Plattformsicherheit....1726
Antivirus-Scanning....1728
Antivirus-Scanning erkunden....1729
Antivirus-Scanning konfigurieren....1731
Dateien in Quarantäne werden überprüft....1732
Wissen über Wörterbuchattribute für Antivirus-Scanning....1733
Auditing....1733
Auditing erkunden....1735
Auditing für eine Tabelle konfigurieren....1737
Anzeigen von Sys-Audit- und Audit-Beziehungsänderungstabellen....1740
Wissen über Verlaufssätze....1741
Strenge Sicherheitseinstellungen....1753
Strenge Sicherheitseinstellungen erkunden....1754
Konfigurieren der Skript-Sandbox-Eigenschaft....1766
Strenge Sicherheitseinstellungen werden aktiviert....1770
HTML-Bereinigung....1773
Durchsuchen der HTML-Bereinigung....1774
Konfigurieren der HTML-Bereinigung....1777
Aktivieren der HTML-Bereinigung....1778
Andere Einstellungen und Sicherheitsressourcen....1780
[store-future: BEGIN review]
Eigenschaften der Sicherheitseinstellungen....1781
Leitfaden zur sicheren MID Server-Bereitstellung....1787
Umkehrbares Verhalten....1792
Veraltete Sicherheitseigenschaften....1792
Verwenden der JavaScript-Inhaltszugriffssteuerung....1794
Andere Sicherheitshärtungsressourcen....1795
[End]
ServiceNow®-Zugriffssteuerung....1795
ServiceNow® Zugriffssteuerung erkunden....1797
ServiceNow® Zugriffssteuerung wird aktiviert....1799
ServiceNow® Zugriffssteuerung konfigurieren....1802
Audit-Protokollierung....1803
Virtuelles privates Netzwerk (VPN)....1803

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtual Private Network (VPN) erkunden....1804
Aktivieren eines VPN-Service....1807
Adresse für die VPN-Kommunikation konfigurieren.... 1807

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

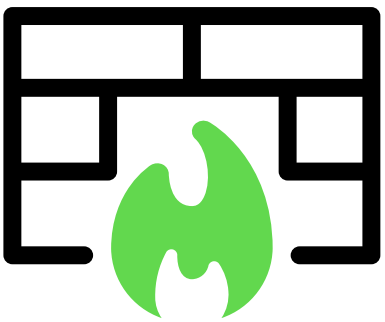
Instanz sichern

Mit Now Platform® Security können Sie Ihre Instanz schützen, Ihre Daten verschlüsseln, die Identität überprüfen, Benutzer authentifizieren und Ihre aktuellen Compliancestufen basierend auf Standards der Anwendungssicherheit anzeigen.

Sicherheit ist auf allen Ebenen von Now Platform integriert. Implementieren Sie die Sicherheitsfunktionen, die für Ihre Organisation geeignet sind, von der Verwaltung fehlgeschlagener Anmeldungen und dem verschlüsselten Passwortschutz bis hin zu Zugriffssteuerungsregeln und Auditprotokollen.

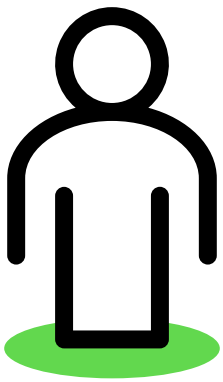
Klicken Sie auf eine dieser Kacheln, um zu beginnen.

Platform-Sicherheit



ServiceNow® Die Anwendung Platform Security von verfügt über eine Reihe von Funktionen, die Ihre Instanz vor Sicherheitsverletzungen schützen und Ihre Daten schützen.

Plattform-Datenschutz



Mit Plattform-Datenschutz können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren. Nachdem sie anonymisiert wurden, gelten sie nicht mehr als persönliche Daten, die Vorschriften unterliegen.

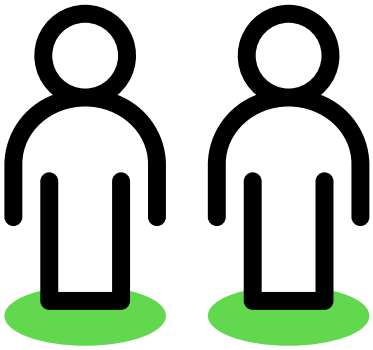
Identität

ServiceNow® Die Anwendung Platform Identity von verfügt über eine Reihe von Funktionen, um die Identitäten in der Instanz zu kennen.

Automatische Übersetzung

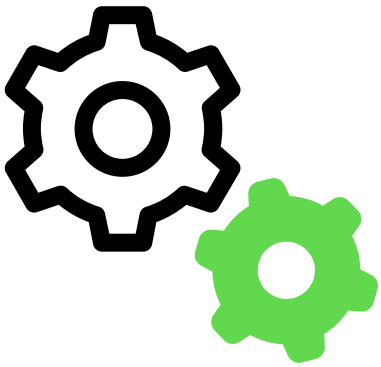
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsverwaltung



ServiceNow® Die Zugriffsverwaltung von ermöglicht die Authentifizierung eines Benutzers, der auf eine Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Auftragsfunktion des Benutzers entsprechen.

Allgemeine Einstellungen für Plattformsicherheit



Erfahren Sie mehr über die allgemeinen Einstellungen für Plattformsicherheit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz sichern

Sicherheit ist auf allen Ebenen von Now Platform integriert. Implementieren Sie die Sicherheitsfunktionen, die für Ihre Organisation geeignet sind, von der Verwaltung fehlgeschlagener Anmeldungen und dem verschlüsselten Passwortschutz bis hin zu Zugriffssteuerungsregeln und Auditprotokollen.

ServiceNow Vault

Verwenden Sie die ServiceNow Vault-Produktreihe von Datensicherheitstools, um vertrauliche Daten während ihres gesamten Lebenszyklus vor unbefugtem Zugriff, Beschädigung oder Diebstahl zu schützen. Wenden Sie Schutzmaßnahmen wie Verschlüsselung, Geheimnisverwaltung und Datenschutz zur Schwärzung und Prüfung vertraulicher Informationen an. Die Homepage von ServiceNow Vault stellt einen zentralen, gut erreichbaren Ausgangspunkt dar, um nach ServiceNow Vault-Datensicherheitsprodukten zu suchen und zu ihnen navigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risiken für vertrauliche Daten reduzieren

Verschlüsseln Sie Plattformdaten mit Key Management Framework und Verschlüsselung auf Spaltenebene Enterprise, womit Sie Schlüssel schützen und den Schlüssellebenszyklus für die Feldverschlüsselung auf Anwendungsebene verwalten können.

Daten während der Ausführung verschlüsseln

Verschlüsseln Sie Daten in Ihrem Netzwerk, das vertrauliche Daten während der Übertragung zwischen Ihrem Rechenzentrum und der ServiceNow-Cloud verschlüsselt und entschlüsselt.

Zugriff auf Ihre Instanz sichern

Validieren Sie die Identität eines Benutzers, der auf eine Instanz zugreift, und autorisieren Sie den Benutzer dann für Funktionen, die der Rolle oder Aufgabenfunktion des Benutzers entsprechen.

Persönlich identifizierbare Informationen (PII) anonymisieren

Legen Sie fest, ob alle Informationen für alle Benutzer oder für eine Teilmenge von Benutzern anonymisiert werden sollen. Wenn sie anonymisiert sind, werden die Daten für die ausgewählten Benutzerdatensätze durch randomisierte Werte oder von Ihnen definierte Werte ersetzt. Beim Ersetzen von Werten kann die Datenstruktur mit verschiedenen Techniken beibehalten werden. Dadurch wird sichergestellt, dass Daten wie E-Mail-Adressen oder physische Adressen durch ähnlich formatierte, aber anonymisierte Versionen ersetzt werden.

Schnell auf Risiken reagieren

Erhöhen Sie die Sichtbarkeit der Sicherheit mit einem Echtzeitdashboard, maßgeschneiderten Empfehlungen und geführten Schritten zur schnellen Behebung von Sicherheitsmängeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risiken für vertrauliche Daten mit Column Level Encryption reduzieren

Verschlüsselung auf Spaltenebene Enterprise nutzt das Key Management Framework und ermöglicht die Anwendung von Best Practices bei der Verwaltung des Schlüssellebenszyklus, um in Ihrer Instanz granulare Spezifikationen zum Verschlüsseln und Entschlüsseln anzupassen und zu verwalten. Sie müssen ein Abonnement für Verschlüsselung auf Spaltenebene Enterprise erwerben, Key Management Framework ist jedoch standardmäßig für alle Instanzen verfügbar.

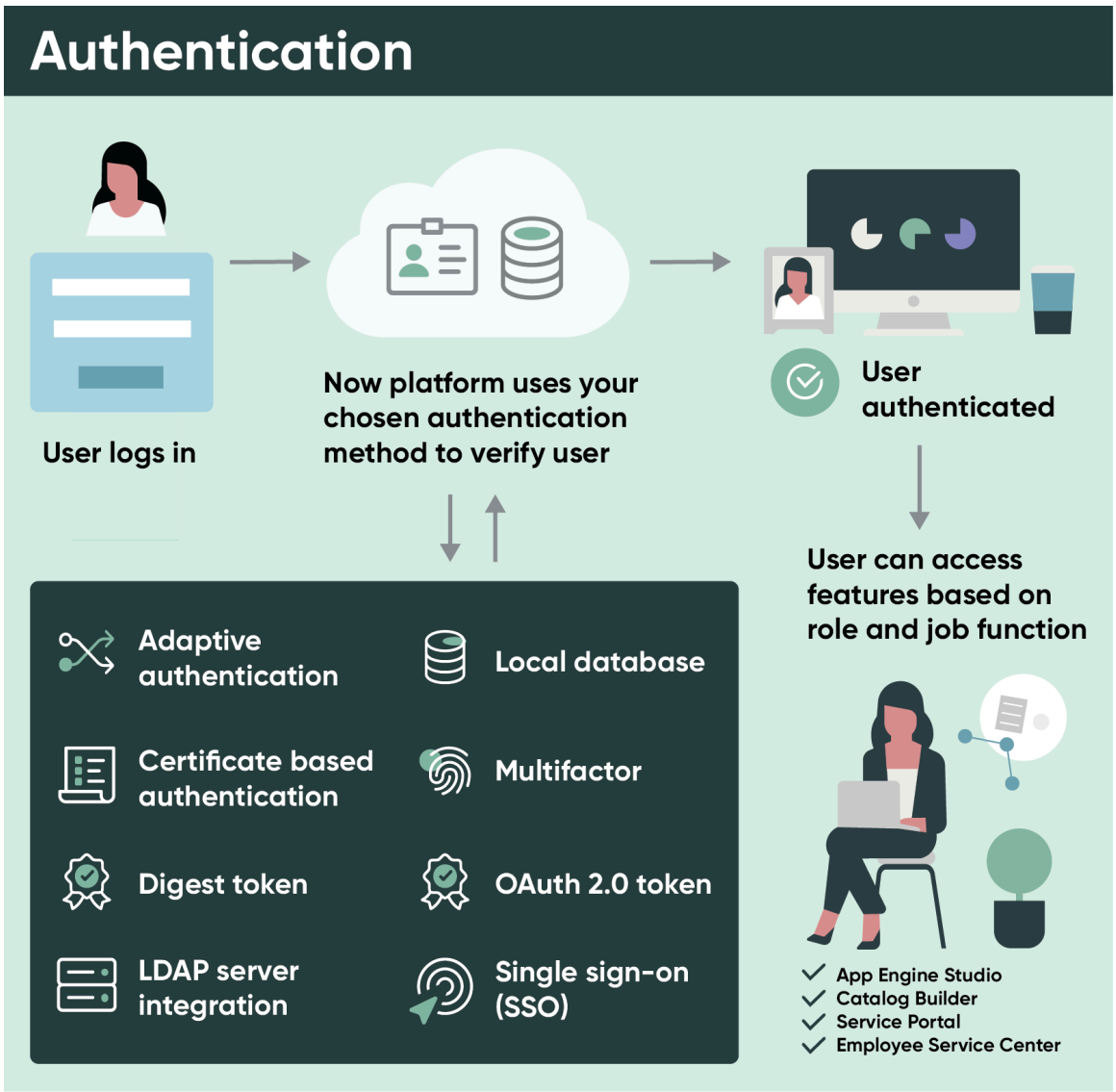
Daten während der Übertragung mit Edge Encryption verschlüsseln

Edge Encryption verschlüsselt vertrauliche Daten in Ihrem Unternehmen, bevor sie über das Internet an Ihre Instanz gesendet werden (Verschlüsselung bei der Übertragung), wo sie im Ruhezustand verschlüsselt bleiben. Edge wird auch als clientseitige Verschlüsselung bezeichnet und macht es erforderlich, dass der gesamte bidirektionale Benutzerdatenverkehr durch Proxys geleitet werden muss, die in Ihrer Infrastruktur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwaltet werden. Sie haben die vollständige Kontrolle über Ihre Schlüsselverwaltung, da die Schlüssel in Ihrem Proxy in Ihrer Infrastruktur gespeichert werden.

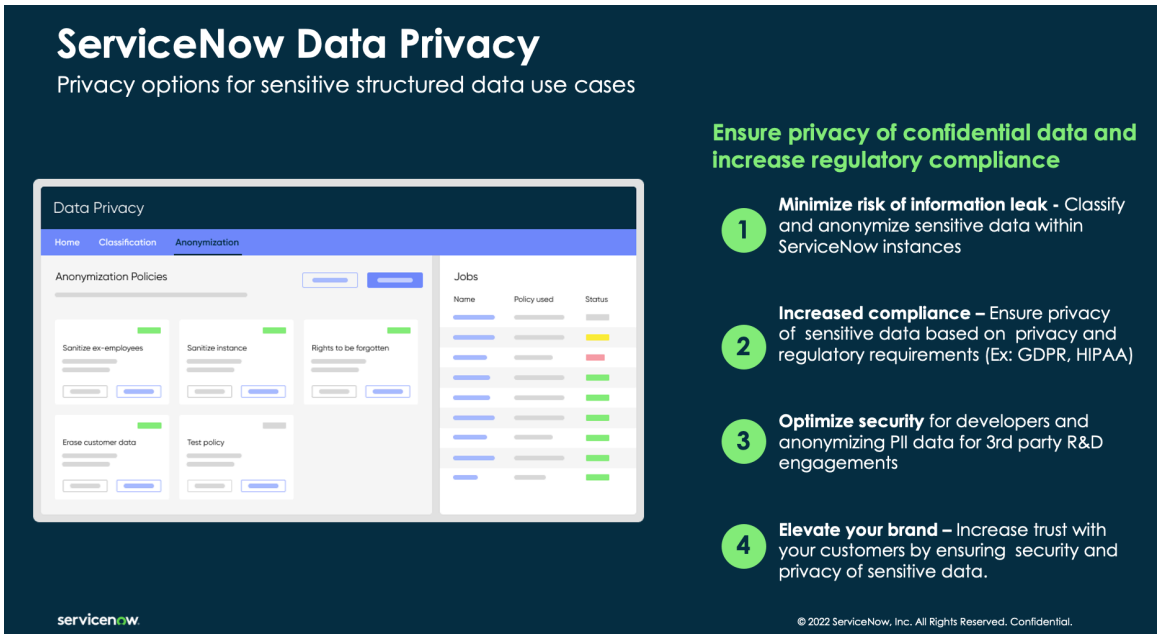
Zugriff auf Ihre Instanz sichern



Wählen Sie die Art der Authentifizierung aus, die den Anforderungen Ihres Unternehmens entspricht. Sie können Benutzer authentifizieren, Single Sign-on aktivieren, Webclients für den Zugriff auf Ihre Instanz autorisieren usw.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persönlich identifizierbare Informationen (PII) anonymisieren

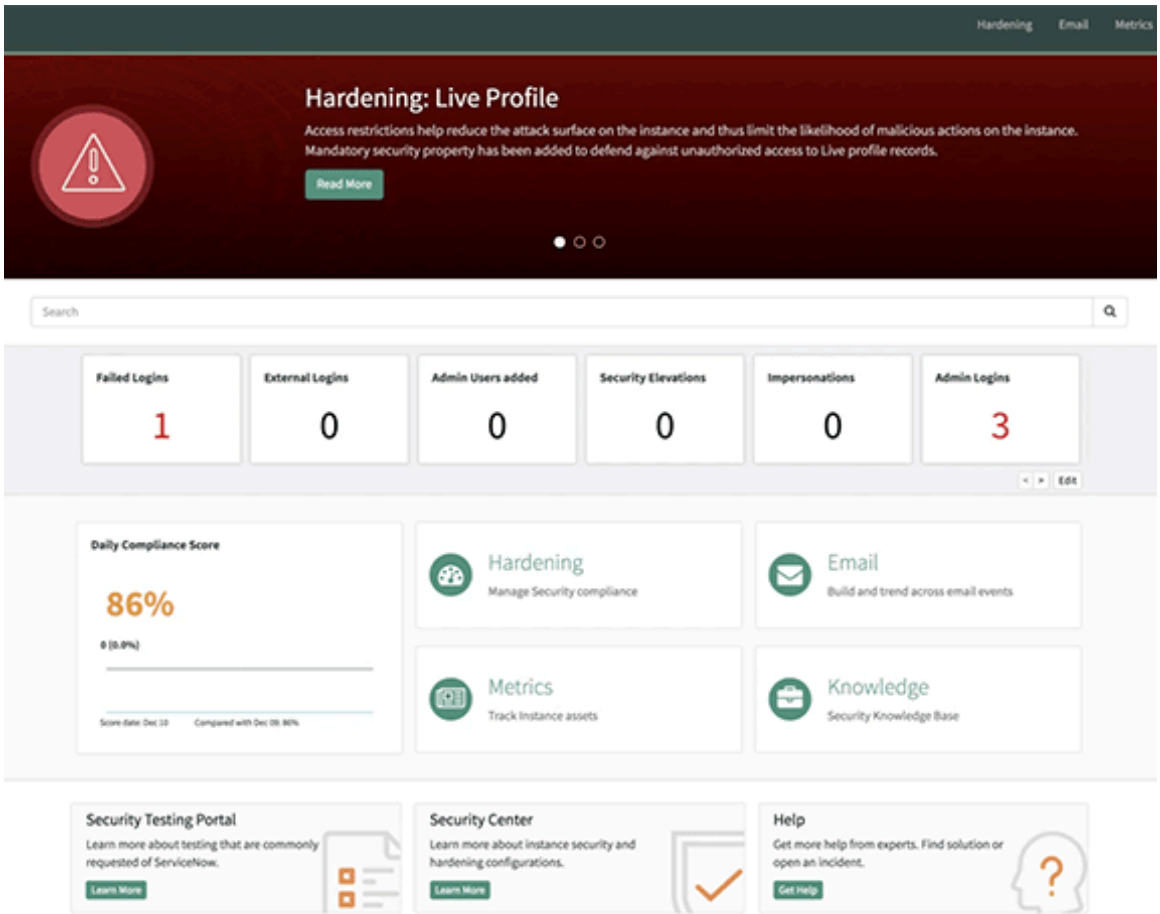


Mit Data Privacy können Sie personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren. Stellen Sie sicher, dass Ihre Benutzerdaten nicht mehr als persönliche Daten gelten, die Vorschriften unterliegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schnell auf Risiken reagieren



Überwachen Sie die Compliancestufe von Instanzsicherheitskontrollen, zeigen Sie Metriken zur Überwachung von Sicherheits-Events an, und konfigurieren und verwalten Sie Instanzsicherheitseinstellungen – alles im Instance Security Center. Das Instance Security Center konsolidiert mehrere wichtige Sicherheitskomponenten in einer einzigen Steuerungskonsole, mit der Sie instanzbasierte Sicherheits-Events erkennen, schützen und darauf reagieren können.

Produkte

- Regeln der Zugriffssteuerungsliste
- Antivirus Scanning
- Auditing
- Authentifizierung
- Zertifikate
- Verbindung und Anmeldeinformationen
- Datenklassifizierung
- Datenfilterung
- Datenschutz
- Domänentrennung für Service Provider

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Encryption and Key Management
- Explizite Rollen
- Identität
- Sicherheitscenter der Instanz
- Härtungseinstellungen für die Instanzsicherheit
- Vault
- Virtuelles privates Netzwerk (VPN)

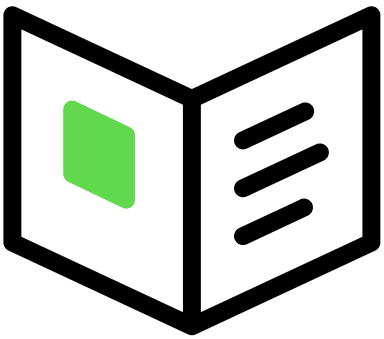
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Platform-Sicherheit

Die Plattformsicherheit bietet Funktionen zum Sichern der Instanz.

Zertifikate



Verwenden Sie Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

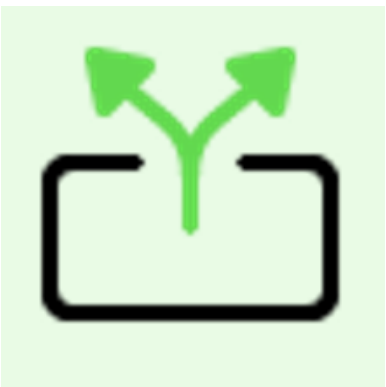
Codesignatur

Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen.

Sicherheitsrollen

Sicherheitsrollen bieten zusätzliche Sicherheit. Jeder Benutzer muss mindestens eine Rolle haben, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Protokolle



Das Modul „Logs“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben von Problemen und zum Debuggen von Transaktionen und Events innerhalb der Instanz verwenden können.

ServiceNow Vault

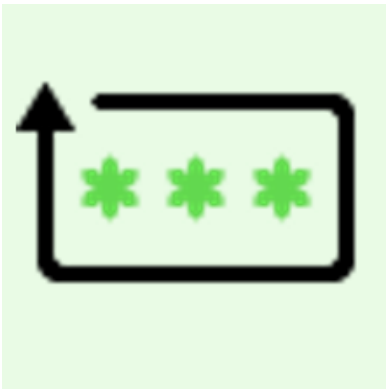
Verwenden Sie die ServiceNow Vault-Produktreihe von Datensicherheitstools, um vertrauliche Daten während ihres gesamten Lebenszyklus vor unbefugtem Zugriff, Beschädigung oder Diebstahl zu schützen.

Sicherheitscenter

Ermöglichen Sie Administratoren, kontinuierlich die höchste Sicherheitsstufe aufrechtzuerhalten und unsichere Ereignisse und Verhaltensweisen einfach zu überwachen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Encryption and Key Management	Geheimnisverwaltung	
		
Verschlüsselung ist ein kryptografisches Verfahren, das Klartext in Geheimtext umwandelt, um die Offenlegung von Informationen zu steuern.	Verwenden Sie ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter, die Ihren Geschäftsanforderungen entspricht.	

Zertifikate

Zertifikate werden für Funktionen wie LDAPS, gegenseitige Authentifizierung für ausgehende Webservices, Web-Sicherheitsservice und MID Server verwendet, um sichere Verbindungen herzustellen und Signaturen zu validieren.

Codesignatur

Codesignatur kann zur Verbesserung der Sicherheit beitragen, indem vertrauliche Anwendungskonfigurationsdaten und Skripts validiert werden, bevor sie verwendet werden. Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Codesignatur ist ein Modul, das als Komponente von ServiceNow Vaultlizenziert ist.

Sicherheitsrollen

Sicherheitsrollen bieten zusätzliche Sicherheit. Jeder Benutzer muss mindestens eine Rolle haben, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Encryption and Key Management

Verschlüsselung ist ein kryptografisches Verfahren, das Klartext in Geheimtext umwandelt, um die Offenlegung von Informationen zu steuern.

Sicherheitscenter

Mit Security Center können Administratoren kontinuierlich die höchste Sicherheitsstufe aufrechterhalten und auf einfache Weise unsichere Ereignisse und Verhaltensweisen überwachen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolle

Das Modul „Logs“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben von Problemen und zum Debuggen von Transaktionen und Events innerhalb der Instanz verwenden können.

Geheimnisverwaltung

ServiceNow Secrets Management bietet eine granulare Verwaltung des Zugriffs auf Ihre Passwörter, die Ihren Geschäftsanforderungen entspricht.

ServiceNow Vault

ServiceNow Vault Das Produkt hilft bei der Einrichtung von Datensicherheitstools, die vertrauliche Informationen während ihres gesamten Lebenszyklus vor unbefugtem Zugriff, Beschädigung oder Diebstahl schützen. Wenden Sie Schutzmaßnahmen wie Verschlüsselung, Geheimnisverwaltung und Datenschutz zur Schwärzung und Prüfung vertraulicher Informationen an.

Zertifikate

Ihre Instanz erfordert Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

Erkunden	Konfigurieren
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Zertifikaten kennen.	Planen Sie Ihre Kernkonfigurationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hochladen Planen und richten Sie die Anwendung ein.	

Zertifikate erkunden

Ihre Instanz erfordert Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

Zertifikate werden für Funktionen wie die folgenden verwendet:

- LDAPS
- Outbound web service mutual authentication
- Webservice-Sicherheit
- MID Server

Um ein Zertifikat zu verwenden, müssen Sie ein Zertifikat für den gesicherten Server oder Client generieren oder erwerben und in eine Instanz hochladen.

LDAP-Zertifikate

Ein SSL-Zertifikat ist erforderlich, damit die Instanz eine LDAP-über-SSL-Verbindung (LDAPS-Protokoll) mit einem LDAP-Server herstellen kann.

Die Instanz akzeptiert zwei Arten von LDAP-Zertifikaten:

Zertifikat	Typ	Erforderlich für
LDAP-Serverzertifikat	Beliebiger unterstützter Typ	Alle LDAP-Konfigurationen
LDAP-Client-Zertifikat	Java-Schlüsselspeichertyp	Gegenseitige Authentifizierung

Wenn mehrere Serverzertifikate vorhanden sind, testet die Instanz jedes Serverzertifikat nacheinander, bis der LDAP-Server die Verbindung zulässt. Wenn Sie mehrere LDAP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Server verwenden, stellen Sie sicher, dass Sie das SSL-Zertifikat für jeden LDAP-Server einbeziehen.

Die gegenseitige Authentifizierung erfordert, dass der Client zusätzlich zum Server ein Zertifikat vorlegt. Wenn Ihr LDAP-Server eine gegenseitige Authentifizierung erfordert, müssen Sie auch das Client-Zertifikat Ihres LDAP-Servers in einem Java-Schlüsselspeicher-Zertifikat angeben.

Zertifikatkriterien

Ein gültiges Zertifikat muss die folgenden Kriterien erfüllen:

- Das Zertifikat kann eine Schlüsselgröße von bis zu 2048 Bit haben.
- Das Zertifikat muss eine der folgenden Dateierweiterungen haben:

Erweiterung	Beschreibung
DER	Das Format „*Distinguished Encoding Rules*“ ist eine binäre Nachrichtenübertragungssyntax. Dieses Format unterstützt auch die Dateierweiterungen .CER und .CRT.
CER	Zertifikatdateierweiterungen für Zertifikate, die das Format „Distinguished Encoding Rules“ verwenden.
CRT	Zertifikatdateierweiterungen für Zertifikate, die das Format „Distinguished Encoding Rules“ verwenden.
PEM	Das *Privacy Enhanced Mail* -Format ist ein base64-codiertes DER-Zertifikat, das zwischen den Textzeichenfolgen „-----BEGIN CERTIFICATE-----“ und „----END CERTIFICATE-----“ eingeschlossen ist.

Zertifikatvertrauen

Standardmäßig vertraut Ihre Instanz nur Zertifikaten einer Zertifizierungsstelle (CA), die in der Java Virtual Machine (JVM) erkannt wird. Selbstsignierten und unternehmenssignierten Zertifikaten wird nicht vertraut.

Hinweis:
Weitere Informationen zu den Eigenschaften, die sich auf die Verwendung von Zertifikaten auswirken, finden Sie unter Sichere Kommunikation in den Härtungseinstellungen für die Instanzsicherheit.

Generieren eines LDAP-Client-Zertifikats

Generieren Sie ein LDAP-Client-Zertifikat für die gegenseitige Authentifizierung mit OpenSSL. Die endgültige Ausgabe ist ein PKCS#12-Zertifikat, das in einem Java-Schlüsselspeicher gespeichert ist.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Generieren von Zertifikaten finden Sie in der OpenSSL-Dokumentation. Bei diesen Schritten wird davon ausgegangen, dass Sie Zugriff auf OpenSSL haben.

Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Generieren Sie ein selbstsigniertes Client-Zertifikat.

   Example
   Beispiel: Dieser Befehl erstellt ein Client-Zertifikat test1-cert.crt basierend auf dem privaten Schlüssel test1-key.key.

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout test1-key.key -out
    test1-cert.crt
   ```

2. Konvertieren Sie sowohl die Zertifikatdatei als auch den privaten Schlüssel in PKCS#12 (eine Datei mit der Erweiterung .pfx oder .p12).

   Example
   Dieser Befehl konvertiert beispielsweise das Client-Zertifikat und den privaten Schlüssel in ein PKCS#12-Zertifikat mit der Bezeichnung test1-certificate.pfx.

   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key -in test1-cert.crt
   ```

3. Generieren Sie den Java Key Store, und importieren Sie die pkcs12-Datei darin.

   Example
   Mit diesem Befehl wird beispielsweise das Zertifikat in den Java-Schlüsselspeicher test1.jks importiert.

   ```
   keytool -importkeystore -srckeystore test1-certificate.pfx -srcstoretype PKCS12
    -destkeystore test1.jks
   ```

4. Laden Siedas Zertifikat in die Schlüsselspeicherdatei (`test1.jks`) in die Instanz hoch.

Hinweis:

Wenn Sie mit einem Zertifikat mit der Erweiterung „.jks“ in eine lokale Instanz hochladen und die Fehlermeldung „Kein gültiges Zertifikat für die Verarbeitung des Anwendungsuploads gefunden“ erhalten, verwenden Sie stattdessen ein Zertifikat mit der Erweiterung „.pfx“.

Nächste Maßnahme
Ein Zertifikat wird in eine Instanz hochgeladen

Ein Serverzertifikat wird generiert

Sie können keytool verwenden, um eine neue Java-Schlüsselspeicherdatei zu generieren, eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) zu erstellen und den privaten Schlüssel, das öffentliche Zertifikatpaar und die signierten Zertifikate in den Schlüsselspeicher zu importieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zum Generieren von Schlüsseln und CSRs finden Sie in der Dokumentation zum Java- Keytool.

Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

   Example
   Mit diesem Befehl wird beispielsweise ein Schlüsselspeicher namens my.keystore erstellt und ein privater Schlüssel namens mydomain innerhalb des Schlüsselspeichers generiert.

   ```
   keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
   ```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

   Example
   Dieser Befehl generiert beispielsweise eine CSR namens mydomain.csr oder den mydomain-Schlüssel.

   ```
   keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
   ```

3. Importieren Sie ein Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle (*Certificate Authority*, CA) in den Java-Schlüsselspeicher.

   Example
   Mit diesem Befehl wird beispielsweise das CA-Zertifikat für Thawte importiert. Dieser Befehl geht davon aus, dass Thwate die Zertifizierungsstelle war, die die CSR signiert hat.

   ```
   keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
   ```

4. Importieren Sie ein signiertes primäres Zertifikat in den Java-Schlüsselspeicher.

   Example
   Mit diesem Befehl wird beispielsweise das signierte Zertifikat mydomain.crt in den Schlüsselspeicher importiert.

   ```
   keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
   ```

5. Laden Sie das Zertifikat in die Schlüsselspeicherdatei (my.keystore) in die Instanz hoch.

Nächste Maßnahme
Ein Zertifikat wird in eine Instanz hochgeladen

Ein Zertifikat wird in eine Instanz hochgeladen

Fügen Sie der Instanz ein Zertifikat aus dem Modul „Zertifikate“ hinzu.

Laden Sie ein Zertifikat in eine Instanz hoch

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Zertifikat auf dem ADFS-Server aktualisiert wird, müssen Sie auch ein aktualisiertes Zertifikat in die Instanz hochladen.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder des Formulars aus.

4. Klicken Sie auf **Absenden**.

   Während des Uploads extrahiert das Modul die schreibgeschützten Eigenschaften des Zertifikats und zeigt sie in den folgenden Feldern an:

   - Gültig ab Datum
   - Ablaufdatum
   - Bearbeiter
   - Betreff des Zertifikats

5. Klicken Sie auf **Speicher/Zertifikate validieren**, um zu überprüfen, ob das Zertifikat korrekt ist. Wenn bei der Instanz Fehler beim Zertifikat oder Schlüsselspeicher auftreten, wird eine Fehlermeldung angezeigt.

Ein vertrauenswürdiges Serverzertifikat wird hochgeladen

Durch das Hochladen des vertrauenswürdigen Serverzertifikats des Service Providers stellt die Instanz sicher, dass eine Verbindung zu einem gültigen und sicheren Service hergestellt wird.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Instanz validiert ausgehende Webserviceaufrufe mithilfe des vom Service Provider bereitgestellten Zertifikats.

Prozedur

1. Erstellen Sie einen neuen Zertifikatdatensatz vom Typ **Trust Store**-Zertifikat.
2. Führen Sie eine der folgenden Aktionen aus:
   - Hängen Sie das DER-formatierte Zertifikat des Service Providers an.
   - Kopieren Sie das PEM-Formatzertifikat des Service Providers, und fügen Sie es in das Feld **PEM-Zertifikat** ein.

Codesignatur

Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Codesignatur ist ein Modul, das als Komponente von ServiceNow Vaultlizenziert ist.

Codesignatur und Vertrauenskreis

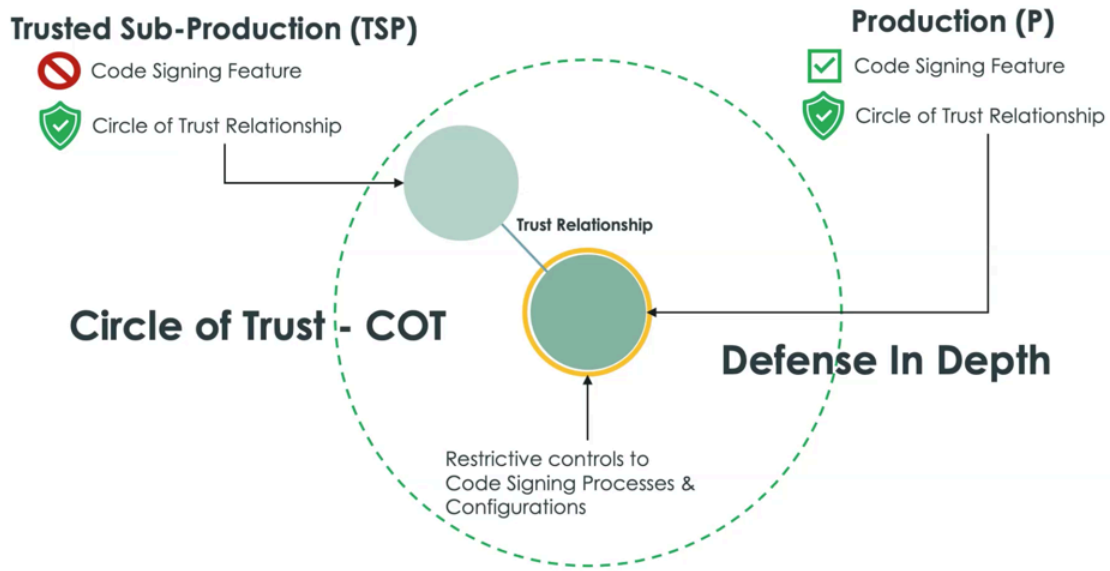
Circle of Trust (COT) ist eine Voraussetzung für die Codesignatur, die eine sichere Kommunikation zwischen Ihren vertrauenswürdigen und Produktionsinstanzen schafft, um sicherzustellen, dass nur autorisierte Benutzer auf die Codesignaturfunktion zugreifen können.

Mehrere Sicherheitsmaßnahmen verhindern, dass böswillige Akteure die Codesignatur deaktivieren oder missbrauchen, wenn eine Produktionsinstanz gefährdet ist. Im Rahmen der „Defense-in-Depth“-Strategie verwendet COT die folgenden Komponenten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In der Produktionsinstanz werden Steuerungen eingerichtet, die selbst die umfangreichsten Administratorkonten einschränken, um Codesignaturprozesse und -konfigurationen zu schützen.
- Vertrauenswürdige (TSP) Instanzen sind erforderlich, um mit Produktionsinstanzen zusammenzuarbeiten und die Beziehung Circle of Trust herzustellen. Mindestens eine vertrauenswürdige Instanz ist erforderlich, es können jedoch mehrere TSP-Instanzen für die Zusammenarbeit mit der Produktionsinstanz konfiguriert werden.

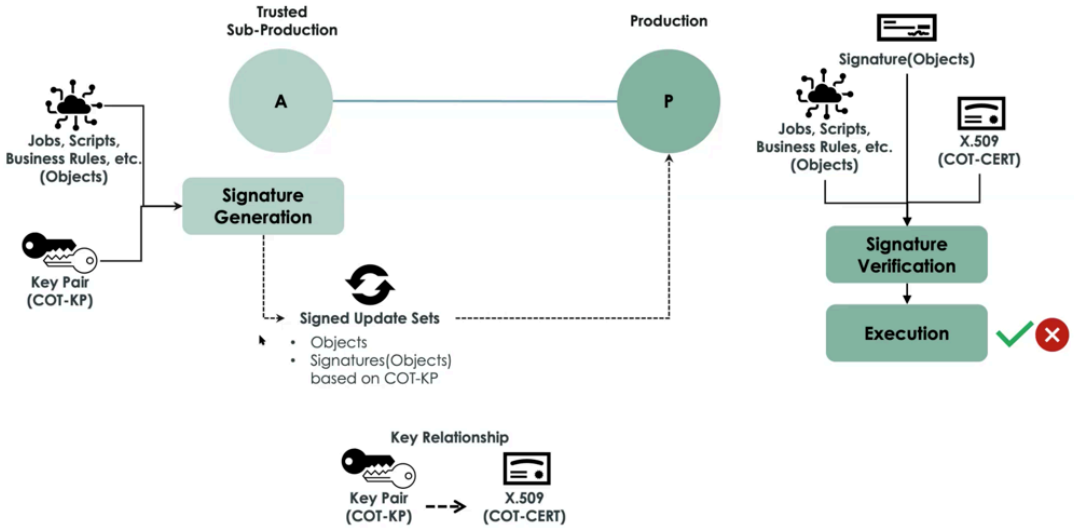
Übersicht über den Vertrauenskreis



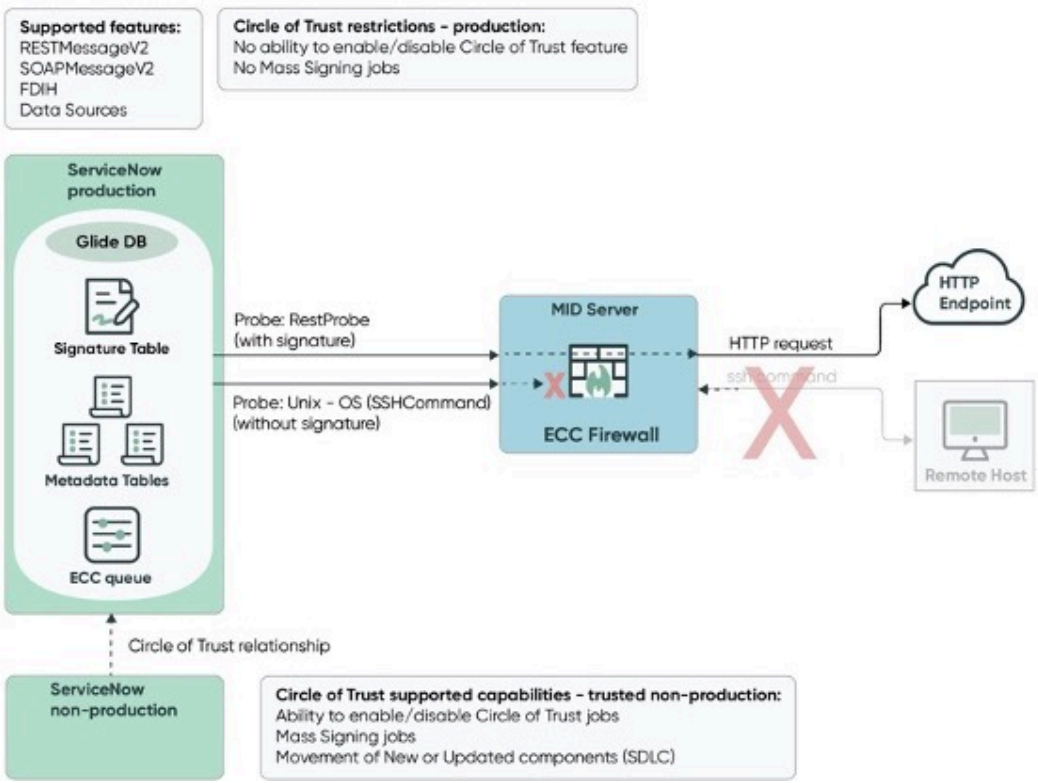
Circle of Trust verwendet Jobs, Skripts und Geschäftsregeln zusammen mit einem Schlüsselpaar, um Signaturen zum Signieren von Update Sets für die Produktionsinstanz zu generieren. Wenn die Aufgabe aufgerufen wird, wird die Signatur zusammen mit dem vertrauenswürdigen Zertifikat überprüft, um Aktualisierungen der Produktionsinstanz auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess für vertrauenswürdige Update Sets



Codesignatur-Flow



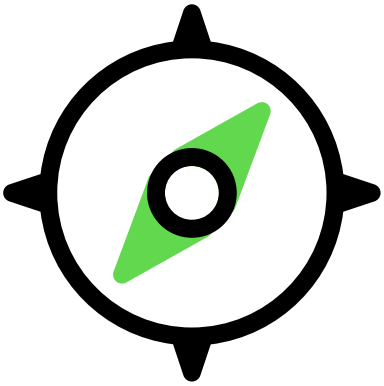
Automatische Übersetzung

Circle of Trust erfordert eine anfängliche Vertrauensstellung zwischen vertrauenswürdigen und Produktionsinstanzen, die verhindert, dass nicht autorisierte Benutzer mit beliebiger Autorisierungsebene auf nicht genehmigte Aktivitäten zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

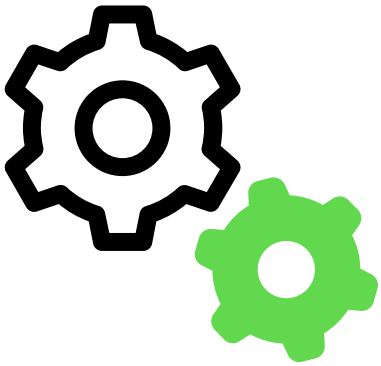
Erste Schritte

Erkunden



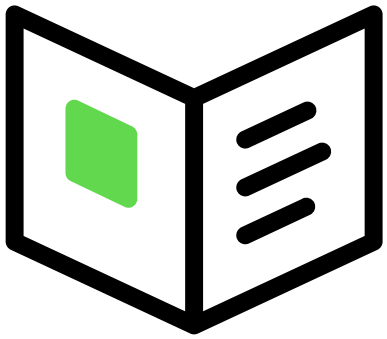
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen der Codesignatur kennen.

Konfigurieren



Aktivieren und konfigurieren Sie die Codesignatur.

Referenz



Rufen Sie Details zu Eigenschaften und Problembehandlung ab

Verwenden

Erfahren Sie, wie Sie mithilfe der Codesignatur die Authentizität und Integrität Ihrer Daten überprüfen können.

Problembehandlung und Hilfe

- https://www.servicenow.com/community/secops/ct-p/security-operations
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur erkunden

Codesignatur kann zur Verbesserung der Sicherheit beitragen, indem vertrauliche Anwendungskonfigurationsdaten und Skripts vor der Verwendung validiert werden.

Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Codesignatur ist ein Modul, das als Komponente von ServiceNow Vaultlizenziert ist.

Hinweis:
Das Team Kundenservice und Support muss Zugriff auf Codesignatur gewähren.

Codesignatur erklärt die Absicht hinter dem durchgeführten Vorgang und validiert, ob die Ressource oder der Datensatz für den beabsichtigten Zweck verwendet werden kann. Um die Codesignatur zu erleichtern, verwendet Key Management Framework (KMF) digitale Zertifikate und asymmetrische Verschlüsselung nach Branchenstandard für digitale Signaturen.

Verwenden Sie die Codesignatur intern auf der Plattform- und Infrastrukturseite. Codesignatur bietet eine Möglichkeit, den Inhalt bestimmter Tabellen oder einer Teilmenge von Datensätzen in einer bestimmten Metadatentabelle zu signieren.

Codesignatur verwendet eine sichere Circle of Trust (COT) zwischen Ihren vertrauenswürdigen und Produktionsinstanzen, um sicherzustellen, dass nur autorisierte, sichere vertrauenswürdige Instanzen auf die Codesignaturfunktion zugreifen können.

Anwendungsfälle

Codesignatur kann für Vorgänge mit MID-Server und IntegrationHubverwendet werden. Notarisierung ist die Verwendung von Codesignatur zum Erstellen digitaler Signaturen für ECC-Warteschlangendatensätze, die in MID Server-Vorgängen und Integration Hub-Vorgängen verwendet werden.

Beispielsweise wird eine von ServiceNow geschriebene Skripteinbindung zum Erstellen von ECC-Warteschlangendatensätzen zur Laufzeit als „Basissysteminhalt“ signiert. Er wird als „ordnungsgemäß von der ServiceNow -Instanz ausgegeben“ signiert, im Gegensatz zu einer Einfügung in die ECC-Warteschlange aus einem Hintergrundskript oder einem anderen Ursprung, der nicht validiert und signiert ist.

IntegrationHub kann Codesignatur verwenden, um dynamische Inhalte zu signieren, die auf der Plattform generiert wurden, und kritische Teile der Anwendungsdaten zu validieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp:

Zeitstempel stellen sicher, dass signierte Datensätze nicht ablaufen, wenn das Zertifikat abläuft, solange der Datensatz vor Ablauf des Zertifikats signiert wurde. Es gibt eine Toleranzfrist von vier Stunden um das Zertifikatgültigkeitsfenster, um sicherzustellen, dass Zeitunterschiede zwischen Servern Zertifikate nicht absichtlich ungültig machen.

Validierung und Aufträge der Codesignatur

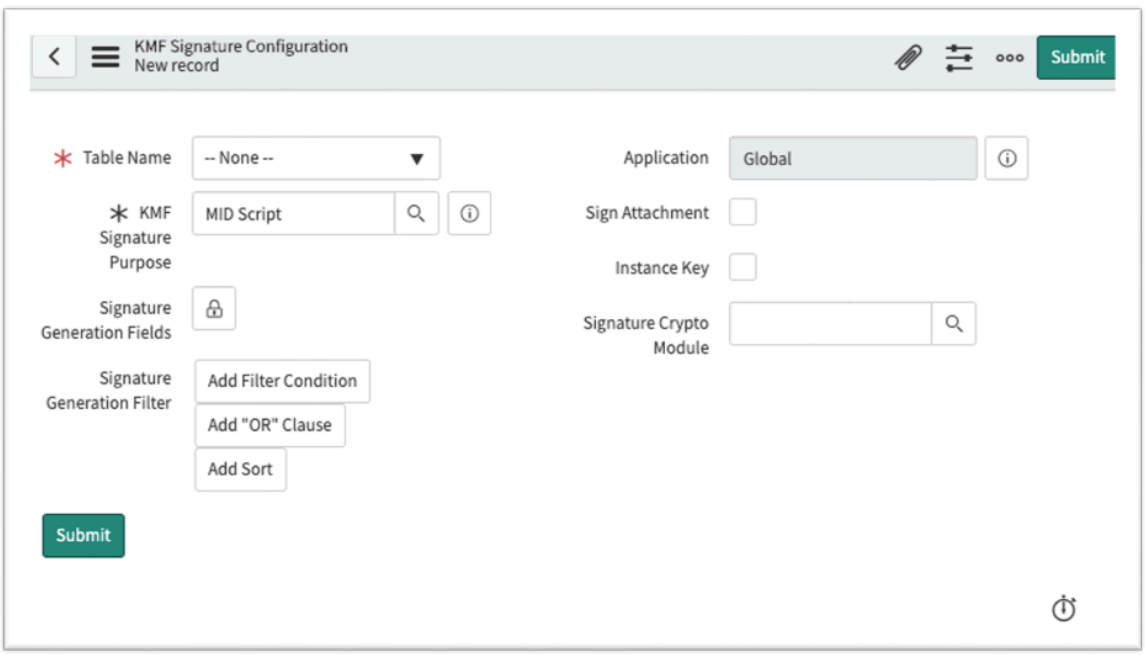
Alle Metadatentabellen mit gültigen Konfigurationen werden zur Build-Zeit mit dem Code Signing-Metadaten-Plugin (`com.glide.code_signing`) signiert. Wenn Sie Tabellen signieren, haben Administratoren mit der Rolle „Sicherheitsadministrator“ Zugriff auf Codesignatur-Verschlüsselungsaufträge☒

- Update Sets signieren.
- Massensignaturdatensätze.
- Massensignaturanhänge.

Signieren Sie das Update Set

Dieser Auftrag signiert Datensätze, die einer Signaturkonfiguration im Update Set entsprechen. Die Aufgabe fügt dem Update Set auch alle neuen Signaturdatensätze und Verifizierungszertifikate hinzu.

KMF-Signaturdatensatz für Update Set



Massensignaturdatensätze

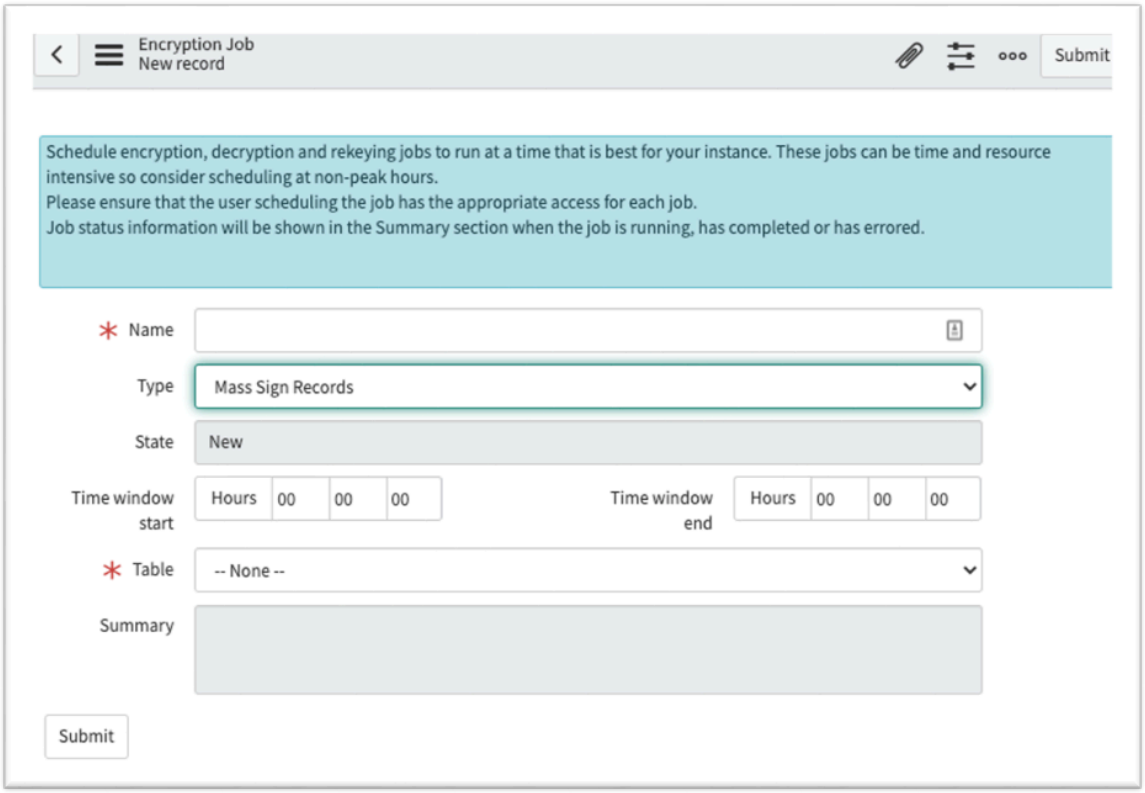
Dieser Auftrag signiert alle Datensätze, die der Signaturkonfiguration entsprechen, die auf eine bestimmte Metadatentabelle angewendet wird.

Massensignaturanhänge

Dieser Auftrag signiert alle Anhangsdatensätze, die an eine Tabelle angehängt sind, die einer angegebenen Signaturkonfiguration entspricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselungsauftrag zum Massensignieren von Datensätzen



Codesignatur konfigurieren

Aktivieren und konfigurieren Sie die Codesignatur, um die Authentizität und Integrität Ihrer Daten sicherzustellen.

Konfiguration – Übersicht

Codesignatur erfordert eine anfängliche Vertrauensstellung zwischen vertrauenswürdigen und Produktionsinstanzen, die verhindert, dass nicht autorisierte Benutzer mit beliebiger Autorisierungsebene auf nicht genehmigte Aktivitäten zugreifen.

In den einzelnen Themen finden Sie Informationen zum Ausführen der Konfigurationsschritte zum Einrichten von Circle of Trust mit Codesignatur:

Codesignatur aktivieren

Aktivieren Sie Codesignatur für Ihre vertrauenswürdige Instanz, um die vertrauenswürdigen Instanzen zu identifizieren, die mit Ihrer Produktionsinstanz verknüpft sind.

Erstellen Sie Schlüsselpaare und Zertifikate für die Codesignatur

Erstellen Sie zwei Schlüsselpaare für signierte Zertifikate, um eine Vertrauensstellung zwischen Ihren Produktions- und vertrauenswürdigen Instanzen herzustellen.

Laden Sie die erforderlichen Schlüsselpaare und Zertifikate für die Codesignatur

Richten Sie die Beziehung Circle of Trust in einer designierten vertrauenswürdigen Instanz mithilfe von Codesignatur ein. Dieser erste Schritt lädt einen kryptografischen Schlüssel in die Nicht-Produktionsumgebung, um eine vertrauenswürdige Quelle für Updates für die Produktionsinstanz einzurichten.

Bereiten Sie Zertifikate für den Vertrauenskreis vor

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Update Set in der vertrauenswürdigen Instanz, um das vertrauenswürdige Zertifikat in die Produktionsumgebung zu exportieren.

Importieren und installieren Sie Zertifikate für den Vertrauenskreis

Rufen Sie das Update Set in der Produktion ab, um die Vertrauensstellung zwischen den beiden Instanzen herzustellen, nachdem das Update Set aus der vertrauenswürdigen Umgebung exportiert wurde. Die Zertifikate, die erstellt wurden, um das Vertrauen in die vertrauenswürdige Instanz darzustellen, müssen in die Produktionsinstanz akzeptiert werden.

Geben Sie benutzerdefinierte Regeln in der ECC-Firewall an

Konfigurieren Sie die ECC-Firewall (Externer Kommunikationskanal) in Ihrem MID-Server, um benutzerdefinierte Regeln zu erstellen, die eingehende Nachrichten selektiv zulassen oder ablehnen, und die Codesignaturkonfiguration zu überschreiben.

Laden Sie die erforderlichen Schlüsselpaare und Zertifikate für die Codesignatur

Richten Sie die Beziehung mithilfe von Codesignatur in einer festgelegten Nicht-Produktionsinstanz ein. Dieser erste Schritt lädt zwei kryptografische Schlüssel in die Nicht-Produktionsumgebung, um eine vertrauenswürdige Quelle für Updates für die Produktionsinstanz zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Der erste Schritt beim Herstellen der Beziehung besteht darin, die Vertrauensbasis in einer festgelegten Nicht-Produktionsinstanz mithilfe von Codesignatur herzustellen. Um diese Aufgabe auszuführen, benötigen Sie Folgendes.

- Sie benötigen zwei öffentlich/private 4096-Bit-RSA-Schlüsselpaare zum Laden in kryptografische Codesignaturmodule:
  - Ein Paar für das kryptografische Modul cm_code_signing
  - Ein Paar für das kryptografische Modul cm_code_attest

  Weitere Informationen zu diesen Schlüsseln finden Sie unter Erstellen Sie Schlüsselpaare und Zertifikate für die Codesignatur.

  Wichtig:
  Diese Schlüsselpaare müssen von einer öffentlichen Zertifizierungsstelle oder von der internen Zertifizierungsstelle Ihrer Organisation signiert sein. Das Zertifikat kann nicht selbst signiert werden.

- Eine Public Key Kryptography Standard #12-Datei (.p12), die Ihr Verteilungszertifikat enthält.

Prozedur

1. Importieren Sie Ihre Schlüssel aus dem -Schlüsselspeicher.
   a. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**.
   b. Suchen und öffnen Sie das kryptografische Modul mit dem Namen `cm_code_signing`.
   c. **Wählen** Sie in der Liste „Krypto-Spezifikationen“ den Namen der Krypto-Spezifikation aus, um sie zu öffnen.
   d. Wählen Sie im Bildschirm **„Import key from keystore“** (Schlüssel aus Schlüsselspeicher importieren) die Option **Import key**(Schlüssel importieren) aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wiederholen Sie den ersten Schritt, um das kryptografische Modul mit dem Namen `cm_code_attest`zu importieren.
3. **Geben Sie im Feld Schlüsselspeicher-Passwort** eingeben das Abfragepasswort ein, das Sie beim Generieren Ihres RSA-Zertifikats erstellt haben.

> **Hinweis:**
> Das von Ihnen erstellte Abfragepasswort wird hier als **Schlüsselspeicher-Passwort**bezeichnet. In anderen Teilen des Prozesses kann dies entweder als **Importpasswort** oder **Exportpasswort**bezeichnet werden. In allen Fällen ist dieses Passwort dasselbe Abfragepasswort, das Sie in den vorherigen Schritten erstellt haben.

4. Wählen Sie die Schaltfläche **Durchsuchen** neben **Schlüsselspeicher/Zertifikat importieren aus**.
5. Wählen Sie die p12-Datei aus (die im Abschnitt „Bevor Sie beginnen“ oben in diesem Dokument erwähnt wird), und wählen Sie dann **Alle herunterladen**aus.
6. Wählen Sie **OK**.

> **Wichtig:**
> Wenn Sie Ihre eigene interne Zertifizierungsstelle verwenden, müssen Sie die Zwischenzertifikate der internen Zertifizierungsstelle mithilfe des Prozesses in den Schritten 5 bis 6 hochladen.

Bei einem erfolgreichen Import Ihres Schlüssels und Ihrer Zertifikate wird eine Bestätigungsmeldung angezeigt.

Sie können anhand der Tabelle „X.509-Zertifikate“ [sys_certificate] überprüfen, ob der Schlüssel und die Zertifikate in Ihrer Instanz vorhanden sind. Diese Datensätze haben den Typ **Truststore**-Zertifikat.

Sie können Ihren Schlüssel in der Tabelle „Kryptografische Module“ [sys_kmf_crypto_module] validieren.

Nächste Maßnahme
Exportieren Sie das Zertifikat in die Produktion. Weitere Informationen finden Sie unter.

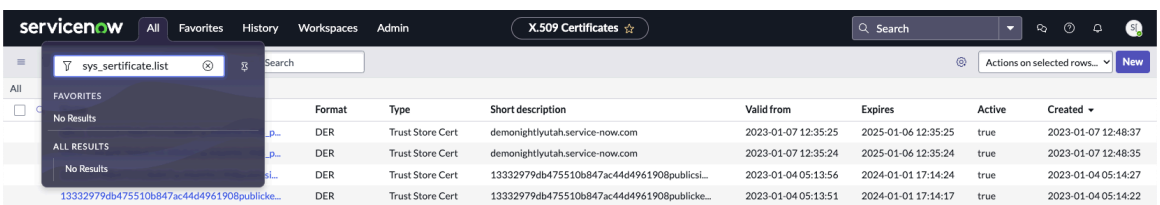
Bereiten Sie Zertifikate für den Vertrauenskreis vor

Erstellen Sie ein Update Set in der vertrauenswürdigen Umgebung, um das vertrauenswürdige Zertifikat in die Produktionsumgebung zu exportieren.

Vorbereitungen
Erforderliche Rolle: admin, security_admin

Prozedur

1. Navigieren Sie in der vertrauenswürdigen Umgebung zu **sys_certificate.list**.

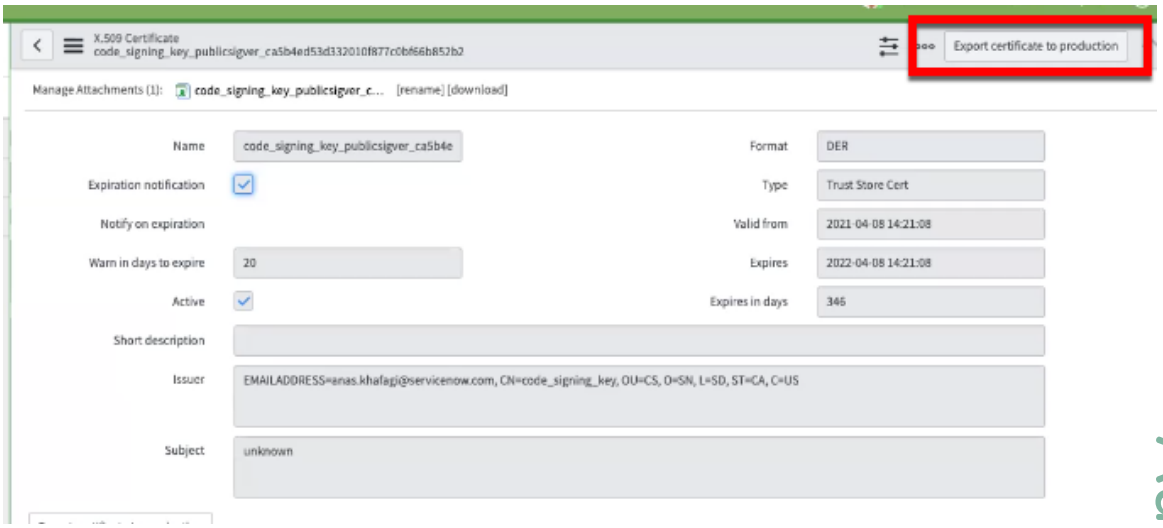


2. Öffnen Sie das zuletzt erstellte X.509-Zertifikat, das mit dem Typ **Truststore**-Zertifikat generiert wurde. Möglicherweise müssen Sie das Feld **Erstellt** der Liste hinzufügen, um den neuesten Datensatz zu finden. Siehe Persönliche Listen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

3. Wählen Sie **Zertifikat in Produktion exportieren aus**.



Zusammen mit dem Zertifikat wird eine Signatur erstellt.

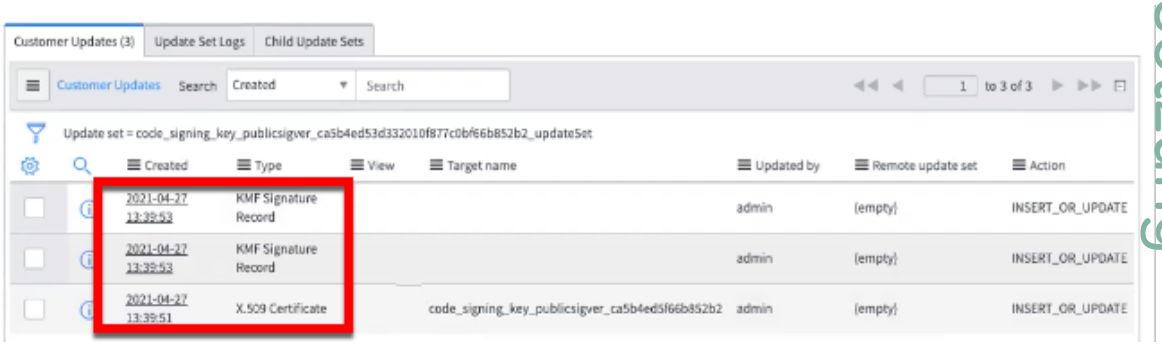
4. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**.
5. Suchen und öffnen Sie das Codesignatur-Update.

   Dieses Update beginnt mit dem Text `code_signing_key_publicsigver`.

   In den vorherigen Schritten wurde ein neuer Datensatz für das Codesignatur-Update Set erstellt. Um diesen Datensatz zu finden, sortieren Sie die Liste mit dem Feld **Erstellt von** und suchen Sie nach Datensätzen mit im Feld **Name**.

6. Zeigen Sie die relevanten Signaturdatensätze und das X.509-Zertifikat an.

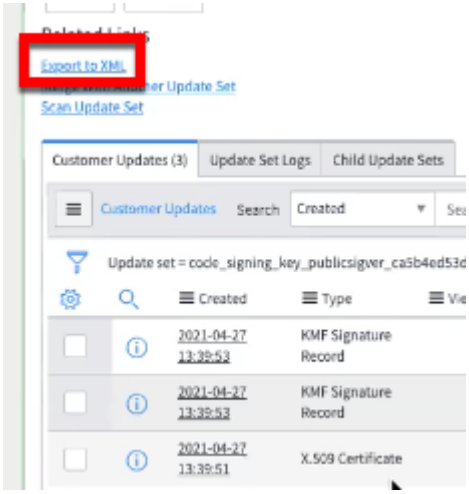
   Das Update Set enthält den Anhang für den Signaturdatensatz zusammen mit dem Eintrag der Signatur in die Tabelle und das Zertifikat.



7. Klicken Sie **auf den zugehörigen Link In XML** exportieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Rufen Sie das Update Set in der Produktion ab.
   Details siehe Retrieve an update set .

> **Wichtig:**
> Wiederholen Sie diese Schritte für Ihr zweites Schlüsselpaar. Denken Sie daran, dass es einen Schlüssel für die kryptografischen Module cm_code_attest und cm_code_signing gibt.

Importieren und installieren Sie Zertifikate für den Vertrauenskreis

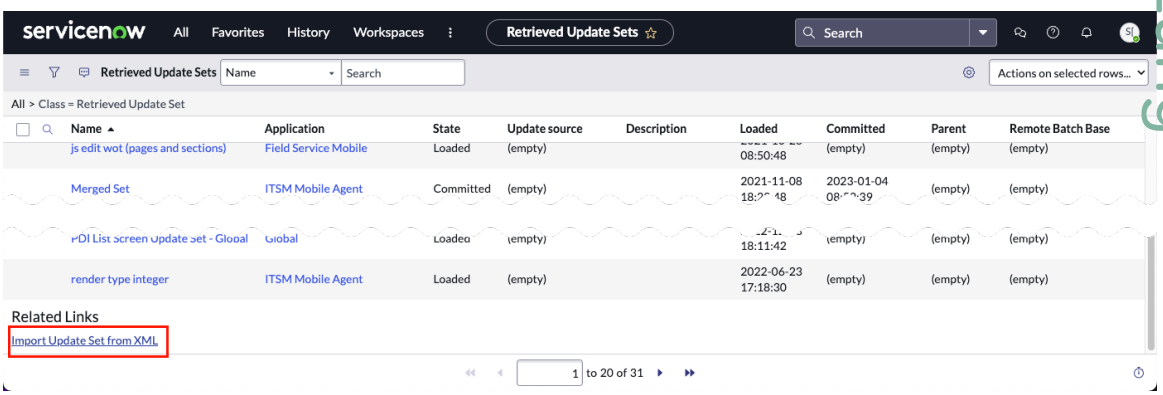
Rufen Sie das Update Set in der Produktion ab, um die Vertrauensstellung zwischen den beiden Instanzen herzustellen. Die Zertifikate, die erstellt wurden, um das Vertrauen in die vertrauenswürdige Instanz darzustellen, müssen in die Produktionsinstanz akzeptiert werden.

Vorbereitungen

Erforderliche Rolle: admin, security_admin

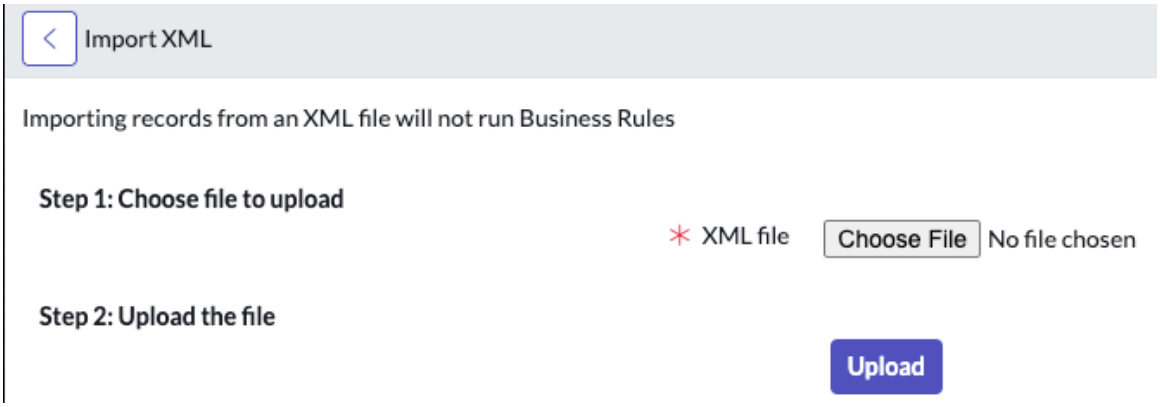
Prozedur

1. Navigieren Sie in der Produktionsinstanz zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.
2. Klicken Sie links unten auf dem Bildschirm auf die Schaltfläche **Update Set aus XML** importieren.

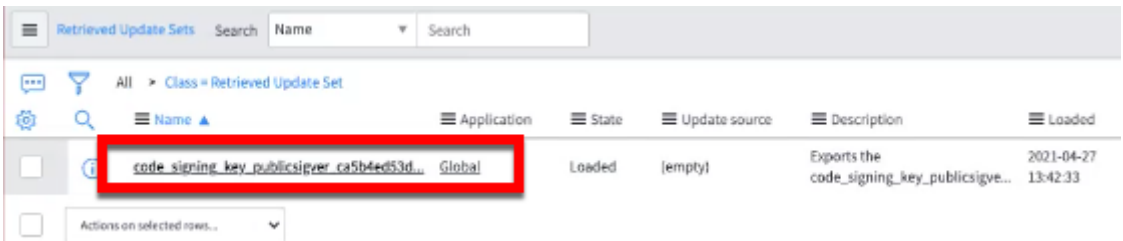


3. Wählen **Sie Datei wählen** aus, und navigieren Sie zur XML-Datei, die Sie in Bereiten Sie Zertifikate für den Vertrauenskreis vorexportiert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

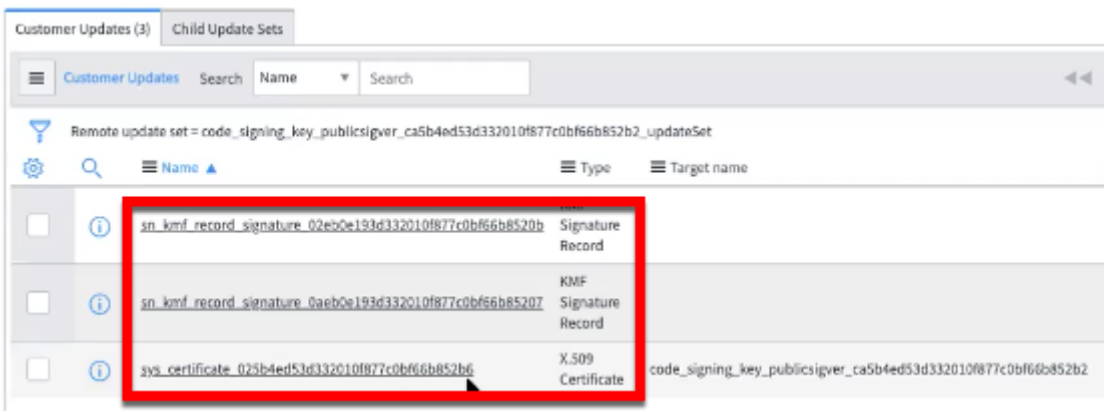


4. Wählen Sie **Hochladen** aus.
   Das Codesignatur-Update Set wird der Tabelle „Abgerufene Update Sets“ hinzugefügt.



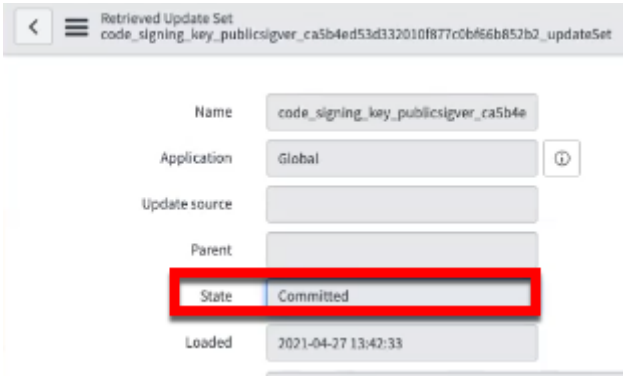
Hinweis:
Wenn Ihr Update Set nicht angezeigt wird, filtern Sie Ihre Liste nach Datensätzen im Status „Geladen“, und sortieren Sie die Liste nach dem Feld „ **Geladen** “.

5. Öffnen Sie den Update Set-Datensatz, um sicherzustellen, dass die Tabelle „Kunden-Updates“ die folgenden drei Datensätze enthält:
   - Zwei KMF Signaturdatensätze
   - X.509-Zertifikat



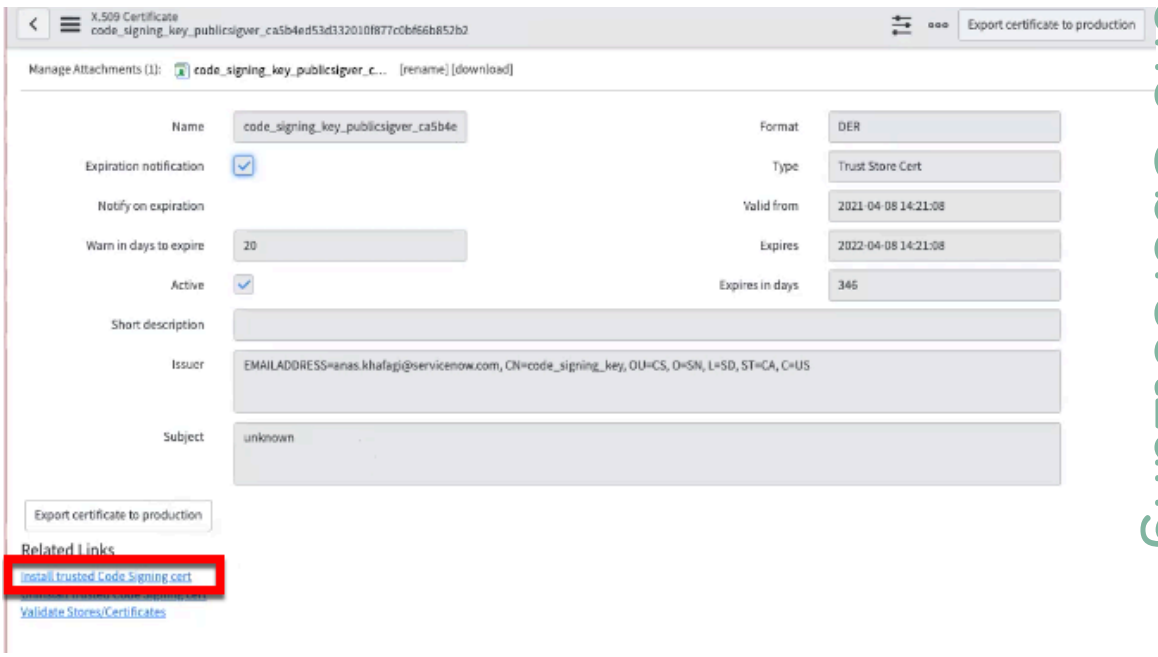
6. Wählen Sie **Vorschau auf Update Set aus**.
7. Wählen Sie **Update Set festlegen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Status des abgerufenen Update Sets wird auf „ **Festgelegt** “ aktualisiert.

8. Geben Sie im Navigator `sn_kmf_record_signature.list` ein, um die Liste der **KMF-Signaturdatensätze** zu öffnen.
9. Suchen Sie die beiden Signaturdatensätze KMF.
   Diese Datensätze sind die zuletzt erstellten Datensätze, bei denen das Feld **KMF-Signaturzweck** den Wert `Kreis des Vertrauens`aufweist. Möglicherweise müssen Sie das Feld **Erstellt** zu Ihrer Liste hinzufügen oder nach Datensätzen filtern, die am aktuellen Datum erstellt wurden.
10. Geben Sie im Navigator `sys_certificate.list` ein, und öffnen Sie den Datensatz mit dem Wert **Kurzbeschreibung***`code_signing_key`* und dem Wert **Typ**`Trust Store`-Zertifikat.
11. Wählen **Sie Trusted Codesignaturzertifikat installieren aus**.



Der Zertifikattyp wird auf *`Trusted CodeSigning`*Certificate aktualisiert.

> **Wichtig:**
> Wiederholen Sie diese Schritte für Ihr zweites Zertifikat. Denken Sie daran, dass es ein Zertifikat für die kryptografischen Module cm_code_attest und cm_code_signing gibt.

Ergebnisse

Die Vertrauensstellung wird zwischen vertrauenswürdigen Instanzen und Produktionsinstanzen hergestellt. Sie sind bereit, die Codesignatur zu aktivieren. Informationen zum Ausführen der Schritte finden Sie unter Codesignatur aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur aktivieren

Aktivieren Sie Codesignatur in Ihrer vertrauenswürdigen Nicht-Produktionsinstanz, um die vertrauenswürdigen Instanzen zu identifizieren, die mit Ihrer Produktionsinstanz verknüpft sind.

Vorbereitungen

Erforderliche Rollen: security_admin und entweder sn_kmf.crypto_manager oder sn_kmf.admin

Bevor Sie die Codesignatur aktivieren, müssen Sie sich an das Team Kundenservice und Support wenden, um das Plugin „Codesignatur-Framework“ [com.glide.code_signing] zu aktivieren.

Warum und wann dieser Vorgang ausgeführt wird

Codesignaturaufträge mit signierten Update Sets werden verwendet, um die Codesignaturfunktion ein- oder auszuschalten. Es gibt keine andere Methode für diese Funktionalität. Dieser Prozess umfasst Folgendes:

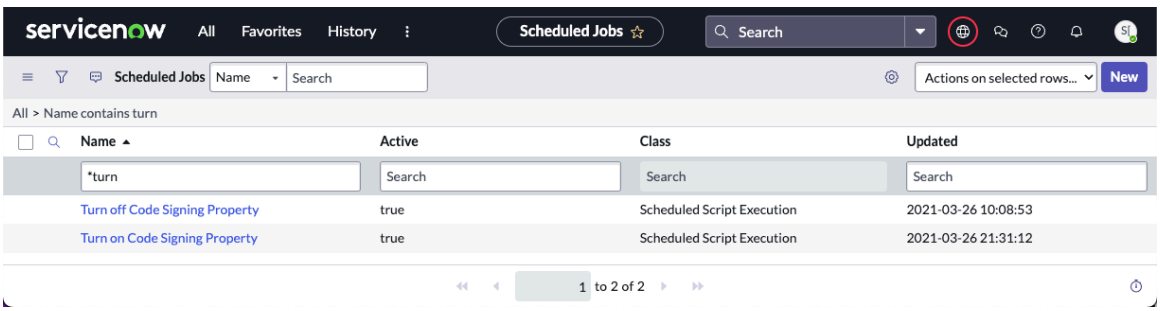
- Erstellen Sie zwei vertrauenswürdige Codesignaturaufträge, einen zum Aktivieren der Codesignatur und einen zum Deaktivieren der Codesignatur.
  - Die **geplante** Aufgabe Aktivieren startet den Prozess der MID Server-Validierung des signierten Codes.
  - Die regelmäßige Aufgabe „ **Ausschalten“** stoppt die MID Server-Validierung des signierten Codes.

Hinweis:
Beim Deaktivieren der Codesignatur wird die Systemeigenschaft auf „ **false**“ gesetzt, die Liste der vertrauenswürdigen Freunde der Codesignatur ist jedoch weiterhin verfügbar.

- Platzieren Sie die Aufgabe „ **Codesignatureigenschaft aktivieren** “ in einem Update Set.
- Bringen Sie den Auftrag in die Produktion.
- Verwenden Sie die Aufgabe **„Codesignatureigenschaft aktivieren** “ in der Produktion, wenn verifiziert wird, dass die Signatur von einer vertrauenswürdigen vertrauenswürdigen Instanz stammt.

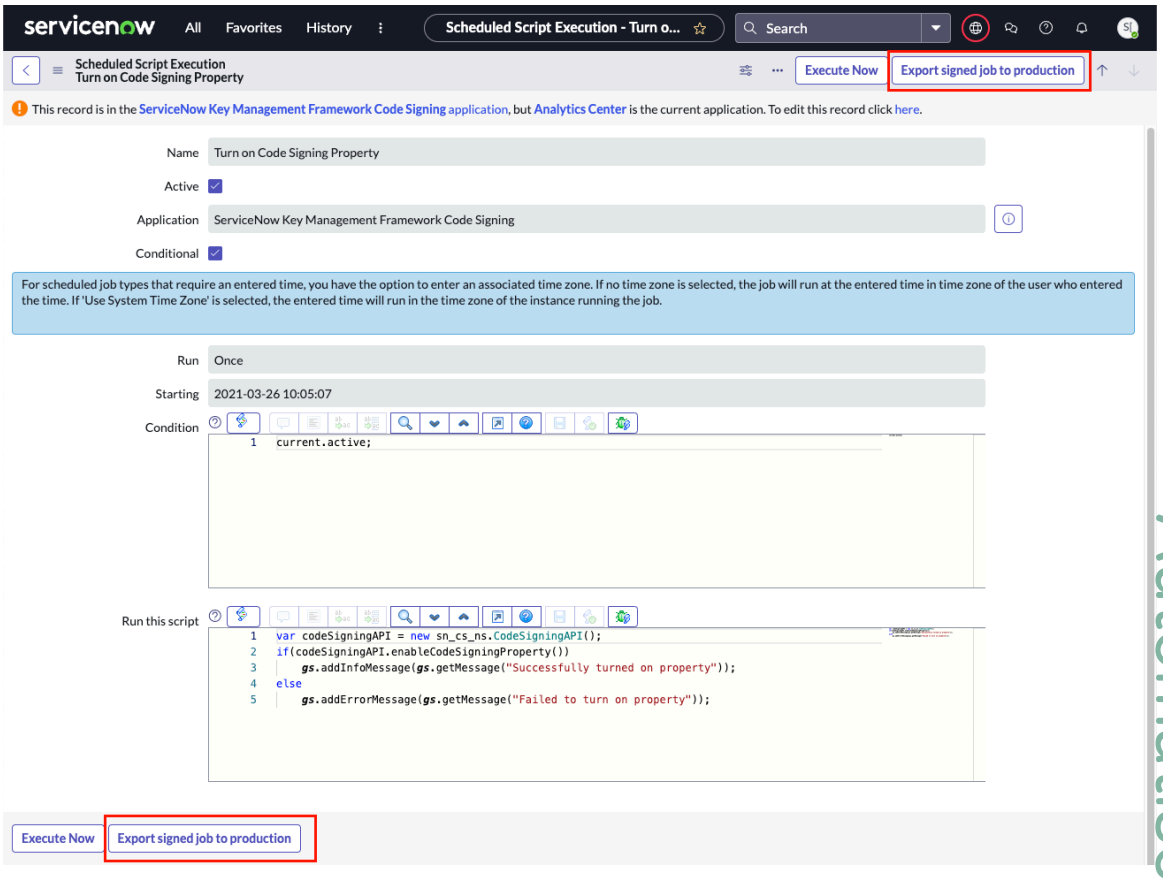
Prozedur

1. Navigieren Sie in Ihrer vertrauenswürdigen Instanz zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
2. Suchen Sie im Namensfeld nach „*turn“.
3. Wählen **Sie Codesignatureigenschaft aktivieren aus**.

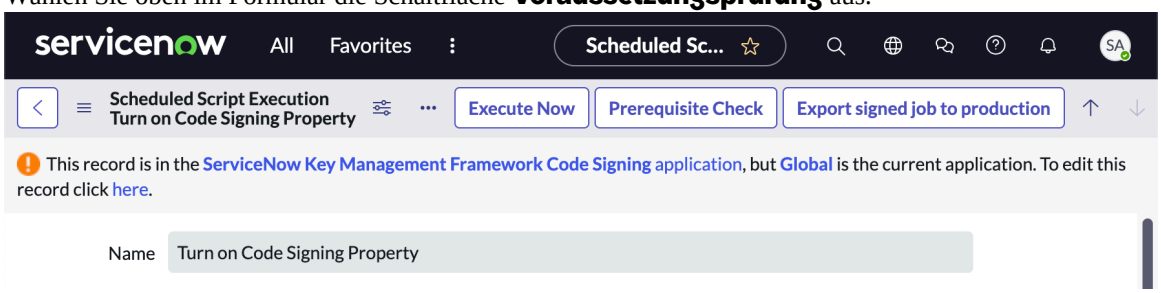


Das Formular „ **Geplante Skriptausführung“** wird geladen. Dieses Formular enthält Informationen zum Aktivieren der Codesignatureigenschaft. Die Aufträge erstellen Update Sets, die die Aufträge und validierten Signaturen über den Codesignaturprozess enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Um das Skript sofort auszuführen, signieren Sie das Zertifikat, erstellen Sie das Update Set, und wählen Sie **Signierten Job in Produktion exportieren aus**.
   Sie können das Skript auch so konfigurieren, dass es nach einem bestimmten Zeitplan ausgeführt wird.
5. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**.
6. Öffnen Sie jedes der Update Sets für Codesignatur-Eigenschaften, und wählen Sie **In XML exportieren aus**.
7. Melden Sie sich bei der Produktionsinstanz an.
8. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.
9. Klicken Sie auf die Schaltfläche **Update Set aus XML** importieren, und wählen Sie das Update Set für die Codesignatur-Eigenschaft aus.
10. Wählen **Sie Datei** auswählen, laden Sie die Update Sets hoch, und schreiben Sie sie fest.
11. Kehren Sie zur Liste der geplanten Aufgaben zurück, indem Sie zu navigieren **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
12. Öffnen Sie den Datensatz der Aufgabe **„Codesignatureigenschaft aktivieren** “.
13. Wählen Sie oben im Formular die Schaltfläche **Voraussetzungsprüfung** aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

14. Klicken Sie nach Abschluss der Prüfung der Voraussetzungen auf die Schaltfläche **Jetzt** ausführen.
Die regelmäßige Aufgabe **„Codesignatureigenschaft aktivieren** “ startet den Prozess der MID Server-Validierung des signierten Codes.
15. Geben Sie im Navigator sn_kmf_record_signature.list ein, um die Liste der **KMF-Signaturdatensätze** zu öffnen, und filtern Sie nach Datensätzen, bei denen der **KMF-Signaturzweck**Kreis des Vertrauensist. Die Vertrauensstellung hat die Aufträge verschoben, und wenn die Aufträge verwendet werden, wird der Signaturverifizierungsprozess ausgeführt. Wenn die Jobs, Signaturen und Zertifikate alle Teil von Circle of Trustsind, kann die Codesignatur mit Circle of Trust aktiviert werden.
16. Geben Sie im Navigator sys_properties.list ein, um die Liste der Systemeigenschaften zu öffnen.
17. Suchen Sie nach *com_snc_kmf_signature.validation.flag*, und stellen Sie sicher, dass der Wert auf **true**festgelegt ist.
18. Vergewissern Sie sich, dass eine neue Eigenschaft *com_snc_kmf_signature.validation.certificate* in der Tabelle aufgeführt ist.

Systemeigenschaften

com.snc.kmf.signature.validation.certifi...	{"trust_map": {"025b4ed53d332010f877c0bf6...	string	ServiceNow Key Management Framework
com.snc.kmf.signature.validation.flag	true	true | false	Global

Verwenden Sie den Auftrag Circle of Trust in der Produktion, um die Vertrauensstellung zu überprüfen. In der Produktion kann keine direkte Aufgabe ausgeführt werden, die versucht, Code zu signieren. Weitere Informationen zu Konfigurationsoptionen finden Sie unter .

Erstellen Sie Schlüsselpaare und Zertifikate für die Codesignatur

Erstellen Sie zwei Schlüsselpaare für signierte Zertifikate, um eine Vertrauensstellung zwischen Ihren Produktions- und vertrauenswürdigen Instanzen herzustellen.

Um eine Vertrauensstellung zwischen Ihren Instanzen herzustellen, müssen Sie für jedes der kryptografischen Module cm_code_attest und cm_code_signing ein Schlüsselpaar und ein Zertifikat erstellen.

Das Erstellen von Schlüsselpaaren und Zertifikaten erfolgt mit einem kryptografischen Tool, das auf Ihrem lokalen Gerät installiert ist, z. B. das OpenSSL-Tool. Weitere Informationen zu diesem Tool finden Sie unter https://www.openssl.org . Wenn Ihre Organisation andere kryptografische Tools wie LibreSSL oder GnuTLS verwendet, finden Sie in der Dokumentation für diese Produkte ähnliche Schritte.

Schlüsselpaarspezifikationen

Die von Ihnen erstellten Schlüsselpaare müssen diese Anforderungen erfüllen.

Typ	RSA
Schlüssellänge	4096
Signaturalgorithmus	RSASSA_PKCS1_V1_5_SHA_512

Zertifikatspezifikationen

Zertifikate müssen von einer öffentlichen Zertifizierungsstelle signiert sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie benutzerdefinierte Regeln in der ECC-Firewall an

Konfigurieren Sie die ECC-Firewall (Externer Kommunikationskanal) in Ihrem MID-Server, indem Sie die benutzerdefinierten Regeln angeben, um eingehende Nachrichten selektiv zuzulassen oder abzulehnen und die Codesignaturkonfiguration zu überschreiben.

Sicherheitsadministratoren können die ECC-Firewall-Tags verwenden, um die Codesignaturkonfiguration zu überschreiben und bestimmte Vorgänge für MID-Serverzuzulassen oder abzulehnen. Diese benutzerdefinierten Regeln müssen in der YAML-Datei des unter agent/boot-config.yaml angegeben werden.

Diese Tags sind spezifisch für ein Protokoll. Die für das übergeordnete Tag angegebene Konfiguration gilt für das untergeordnete Tag. Wenn beispielsweise das HTTP -Protokoll zulässig ist, sind auch die Protokolle REST und SOAP zulässig. In dieser Tabelle sind die verfügbaren übergeordneten und untergeordneten Tags aufgeführt.

Übergeordnetes Tag	Untergeordnetes Tag
DNS	
HTTP	• REST • SOAP
VERZEICHNIS_DIENSTLEISTUNGEN	LDAP
SNMP	
SSH	• SCP • SFTP
SYSLOG	
WINDOWS	• CIM • POWERSHELL • WMI • WINRM
JAVASCRIPT	
GROOVY	
VCS	GIT
DATENBASEN	JDBC
DATENQUELLEN	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DISCOVERY • EVENT_MANAGEMENT

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnetes Tag	Untergeordnetes Tag
	• HEALTH_LOG_ANALYSE • SERVICE_MAPPING
ORCHESTRATION	

So konfigurieren Sie die benutzerdefinierten Regeln:

1. Identifizieren Sie in MID-Serverdie Datei „ boot-config-sample.yaml“.
2. Benennen Sie die YAML-Datei in „ boot-config.yaml“ um, und verschieben Sie die Datei an den folgenden Speicherort: agent/boot-config.yaml.
3. Geben Sie in der YAML-Datei die benutzerdefinierten Regeln an, und speichern Sie die Änderungen. Ein Beispiel für die YAML-Datei:

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. Starten Sie MID-Serverneu.

Ändern Sie Ihre Root of Trust-Konfiguration

Vertrauen Sie Ihren eigenen Zertifikaten, anstatt sich auf ServiceNow Build-Zertifikate (Standard) zu verlassen, indem Sie Ihren Root of Trust (ROT) verwenden. ServiceNow Komponenten wie Skripteinbindungen, Business Rules usw. werden zur Build-Zeit mit einem ServiceNow Build-Zeitschlüssel signiert (Verifizierungszertifikat ist das ServiceNow Build-Zertifikat).

Ändern der Vertrauensbasis

Um den Root of Trust für diese Datensatzsignaturen zu ändern, müssen Sie dem Change des Root of Trust-Prozesses folgen.

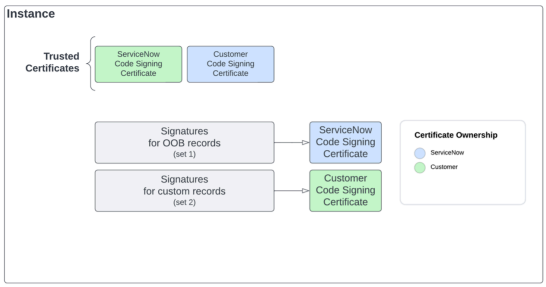
- Generieren und migrieren Sie mithilfe des bereitgestellten Zertifikats einen neuen Satz von Signaturen für alle bereitgestellten Komponenten.
- Deaktivieren Sie die Eigenschaft „Root of Trust“ mithilfe einer geplanten Aufgabe.

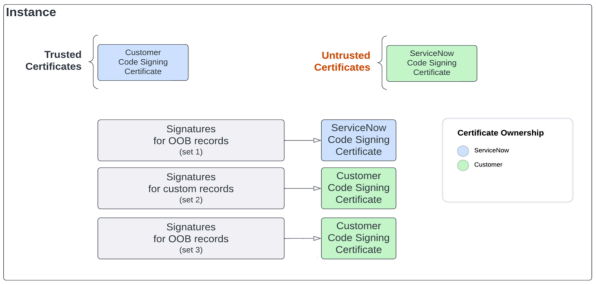
Weitere Informationen zu diesen Schritten finden Sie in Migrieren Sie Signaturen, um ein Kundenzertifikat zu verwenden und Deaktivieren Sie ServiceNow Root of Trust.

Auswirkung auf den Signaturgenerierungs- und -verifizierungsprozess

Standardmäßig wird den Build-Zertifikaten der Codesignatur während des Signaturüberprüfungsprozesses vertraut. Nach dieser Änderung akzeptiert Ihre Instanz nur Signaturen von Ihrem eigenen Codesignaturzertifikat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





ROT-Eigenschaft auf „falsch“ festgelegt (Standard)	ROT-Eigenschaft auf „true“ festgelegt
• Bei der Überprüfung wird Signaturen mit Build-Zertifikaten vertraut. • Wenn Sie beim Signieren keine Schlüssel angeben, wird der Instanzsignaturschlüssel als Sicherungsschlüssel verwendet. • Der Signatur-REST-Endpunkt *api/sn_kmf/signature/certificates* gibt ServiceNow Code Signing-Build-Zertifikate zusammen mit anderen in der Instanz vorhandenen Zertifikaten zurück.	• Bei der Überprüfung wird Signaturen mit Build-Zertifikaten nicht vertraut. • Wenn Sie beim Signieren keine Schlüssel angeben, wird das Signieren nicht ausgeführt. • Der Signatur-REST-Endpunkt *api/sn_kmf/signature/certificates* schließt ServiceNow Build-Zertifikate aus (San Diego, Vancouver PKI, W PKI).

Auswirkung auf Ihren MID Server

Wenn die ROT-Eigenschaft auf „false“ festgelegt ist

Wenn Sie die ROT-Eigenschaft auf dem Standardwert (falsch) belassen, hat dies keine Auswirkungen auf Ihren MID Server.

Wenn Codesignatur aktiviert und die ROT-Eigenschaft auf „true“ festgelegt ist

- Die API *isTrusted()* gibt für Signaturen mit einem Build-Zertifikat „ false “ zurück.
- Die API *isTrusted()* gibt für Signaturen mit Ihrem Zertifikat „ true “ zurück.
- Der REST-API-Aufruf für Zertifikate schließt Build-Zertifikate aus.
- Möglicherweise werden in den Protokollen MID Server-Probleme angezeigt, z. B. Meldungen zu fehlgeschlagenen Signaturvalidierungen.

Migrieren Sie Signaturen, um ein Kundenzertifikat zu verwenden

Führen Sie einen Signierauftrag aus, um Ihre Signaturen zum Root of Trust (ROT) eines Kunden zu migrieren.

Vorbereitungen

Erforderliche Rolle: admin, security_admin und sn_kmf.cryptographic_manager

Codesignatur muss für Ihre Produktionsinstanzen und vertrauenswürdigen Instanzen aktiviert sein. Sie können überprüfen, ob die **Systemeigenschaft com.snc.kmf.signature.validation.flag** auf truefestgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Verfahren ist Teil einer Reihe von Verfahren zum Ändern des Root of Trust (ROT) eines Kunden in Ihren Instanzen. Eine Übersicht über diesen Prozess finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.

Prozedur

1. Melden Sie sich bei Ihrer Produktionsinstanz an.
2. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
3. Suchen und öffnen Sie die geplante Aufgabe **„ROT – Aktualisierungssatz von Datensätzen generieren, um Signaturen mithilfe des Kundenzertifikats zu migrieren“**.
4. Wählen Sie am unteren Rand des Formulars **Jetzt ausführen**aus.
5. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen**.
6. Wählen Sie bei der Eingabeaufforderung **Signierauftrag**aus.
7. Füllen Sie im Formular **„Signierauftrag“** die Felder nach Bedarf aus.

Feld	Wert
Name	Erstellen Sie einen eindeutigen Namen für Ihre Aufgabe.
Typ	Wählen Sie **Update Set signieren aus**.
Tabelle	Wählen Sie das in den vorherigen Schritten erstellte Update Set aus. Das Update Set hat einen Namen, der mit change_root_of_trust_updateSet beginnt.

8. Klicken Sie mit der rechten Maustaste auf die Formularkopfzeile, und wählen **Sie Speichern** aus, um diesen Datensatz zu speichern.
9. Klicken Sie mit der rechten Maustaste auf die Formularkopfzeile, und wählen Sie **Exportieren** > **XML (dieser Datensatz)** , um diesen Datensatz als XML-Datei zu exportieren.
10. Melden Sie sich bei Ihrer vertrauenswürdigen Instanz an.
11. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**.
12. Klicken Sie mit der rechten Maustaste auf die Listenkopfzeile, und wählen Sie **XML importieren**aus.
13. Wählen Sie im Formular „ **XML** importieren“ die **Option Datei** wählen aus, und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
14. Wählen Sie **Hochladen** aus.
15. Öffnen Sie in der Liste den importierten Sicherheitsauftrag.
16. Wählen Sie **Codesignaturauftrag in Produktion exportieren aus**.
    Mit dieser Aktion wird der Job signiert und in ein neues Update Set eingefügt, das Sie in Ihre Produktionsinstanz importieren können.

> **Wichtig:**
> Nach dem Signieren der Aufgabe müssen Sie die nächsten Schritte innerhalb von 10 Minuten ausführen. Wenn Sie diesen Zeitraum überschreiten, können Sie den Job mit diesen Schritten erneut signieren, wodurch ein weiteres signiertes Update Set erstellt wird.

17. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**.
18. Suchen Sie das in den vorherigen Schritten erstellte Update Set.
    Der Name beginnt mit SIGN_UPDATE_SET_updateSet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

19. Wählen Sie **XML** exportieren aus, um Ihr Update Set als XML-Datei zu exportieren.
20. Melden Sie sich bei Ihrer Produktionsinstanz an.
21. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.
22. Wählen Sie am Ende der Liste **Update Set aus XML importieren aus**.
23. Wählen Sie im Formular „ **XML** importieren“ die **Option Datei** wählen aus, und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
24. Wählen Sie **Hochladen** aus.
25. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**, und öffnen Sie das Update Set, das mit SIGN_UPDATE_SET_updateSet beginnt.
26. Wählen Sie **Vorschau auf Update Set aus**.
27. Nachdem die Vorschau abgeschlossen ist, wählen Sie **Update Set festlegen**aus.
28. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**.
29. Öffnen Sie den importierten Sicherheitsauftrag.
30. Wählen Sie **Start** aus, um den Sicherheitsauftrag auszuführen.

    Nach Abschluss der Sicherheitsaufgabe werden Informationen zum Status der Aufgabe im Feld **Zusammenfassung** angezeigt.

    Wenn sich die Aufgabe im Status „Fertig“ befindet, müssen alle Signaturen von Update Set-Datensätzen das vom Kunden bereitgestellte Zertifikat als Überprüfungszertifikat verwenden. Sie können dies in der Tabelle „KMF-Signaturdatensätze“ [sn_kmf_record_signature] überprüfen.

Nächste Maßnahme

Informationen zum Fortsetzen des Root of Trust-Konfigurationsprozesses finden Sie unter Deaktivieren Sie ServiceNow Root of Trust.

Deaktivieren Sie ServiceNow Root of Trust

Führen Sie eine regelmäßige Aufgabe für Ihre vertrauenswürdige Nicht-Produktionsinstanz aus, um Root of Trust zu deaktivieren.

Vorbereitungen

Erforderliche Rolle: admin, security_admin und sn_kmf.cryptographic_manager

Codesignatur muss für Ihre Produktionsinstanzen und vertrauenswürdigen Instanzen aktiviert sein. Sie können überprüfen, ob die **Systemeigenschaft com.snc.kmf.signature.validation.flag** auf truefestgelegt ist.

Dieses Verfahren ist Teil einer Reihe von Verfahren zum Ändern des Root of Trust (Root of Trust, ROT) eines Kunden in Ihren Instanzen. Eine Übersicht über diesen Prozess finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.

Prozedur

1. Melden Sie sich bei Ihrer vertrauenswürdigen Instanz an.
2. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
3. Öffnen Sie die geplante Aufgabe **Root of Trust für ServiceNow deaktivieren**.
4. Wählen Sie die **unterzeichnete Aufgabe in die Produktion exportieren aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**.
6. Suchen und öffnen Sie das Update Set **ServiceNow Root of Trust** deaktivieren.
7. Wählen Sie **XML** exportieren aus, um Ihr Update Set als XML-Datei zu exportieren.
8. Melden Sie sich bei Ihrer Produktionsinstanz an.
9. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.
10. Wählen Sie am Ende der Liste **Update Set aus XML importieren aus**.
11. Wählen Sie im Formular „ **XML** importieren“ die **Option Datei** wählen aus, und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
12. Wählen Sie **Hochladen** aus.
13. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**, und öffnen Sie das Update Set **ServiceNow Root of Trust** deaktivieren.
14. Wählen Sie **Vorschau auf Update Set aus**.
15. Nachdem die Vorschau abgeschlossen ist, wählen Sie **Update Set festlegen**aus.
16. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
17. Öffnen Sie die im Update Set importierte geplante Aufgabe.
18. Klicken Sie auf die Schaltfläche **Jetzt** ausführen, um die Aufgabe auszuführen.

Ergebnisse

Durch die Ausführung der geplanten Aufgabe wird die ROT-Eigenschaft auf „true“ festgelegt. Ihre Instanz ist so konfiguriert, dass sie den Root of Trust des Kunden verwendet.

Deaktivieren Sie die Codesignatur

Deaktivieren Sie die Codesignatur in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion, um die vertrauenswürdigen Instanzen zu identifizieren, die mit Ihrer Produktionsinstanz verknüpft sind.

Vorbereitungen

Erforderliche Rollen: security_admin und entweder sn_kmf.crypto_manager oder sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

Codesignaturaufträge mit signierten Update Sets werden zum Aktivieren und Deaktivieren der Codesignaturfunktion verwendet. Es gibt keine andere Methode für diese Funktionalität. Dieser Prozess umfasst Folgendes:

- Erstellen Sie zwei Codesignaturaufträge in Ihrer vertrauenswürdigen Instanz : einen zum Aktivieren der Codesignatur und einen zum Deaktivieren der Codesignatur.

  Hinweis:
  Beim Deaktivieren der Codesignatur wird die Systemeigenschaft auf **false**festgelegt, die Liste der vertrauenswürdigen Freunde der Codesignatur ist jedoch weiterhin verfügbar.

- Platzieren Sie die Aufgabe „ **Codesignatureigenschaft deaktivieren** “ in einem Update Set.
- Bringen Sie den Auftrag in die Produktion.
- Verwenden Sie den Auftrag in der Produktion, wenn verifiziert wird, dass die Signatur von einer vertrauenswürdigen Instanz stammt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
2. Suchen Sie im Namensfeld nach „*turn“.

> **Wichtig:**
> In der Tabelle werden zwei Aufgaben aufgelistet: **Codesignatureigenschaft aktivieren** und **Codesignatureigenschaft deaktivieren**. Führen Sie dieses Verfahren für jede dieser Aufgaben aus.

3. Wählen **Sie Codesignatureigenschaft deaktivieren**.
   Das Formular „Geplante Skriptausführung“ wird geladen und enthält Informationen zum Deaktivieren der Codesignatureigenschaft. Die Aufträge erstellen Update Sets, die die Aufträge und validierten Signaturen über den Codesignaturprozess enthalten.
4. Um das Skript sofort auszuführen, signieren Sie das Zertifikat, erstellen Sie das Update Set, und wählen Sie **Signierten Job in Produktion exportieren aus**.
   Sie können das Skript auch so konfigurieren, dass es nach einem bestimmten Zeitplan ausgeführt wird.
5. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**.
6. Öffnen Sie jedes der Update Sets für Codesignatur-Eigenschaften, und wählen Sie **In XML exportieren aus**.
7. Melden Sie sich bei der Produktionsinstanz an.
8. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.
9. Wählen Sie **Update Set aus XML importieren**, und wählen Sie das Update Set für die Codesignatur-Eigenschaft aus.
10. Wählen **Sie Datei** auswählen, laden Sie die Update Sets hoch, und schreiben Sie sie fest.
11. Wählen Sie jedes der Update Sets und dann **Execute Now**(Jetzt ausführen) aus.
12. Navigieren zu **KMF-Signaturdatensätze** > **Alle** und suchen Sie nach dem KMF Signaturzweck von Circle of Trust.
    Die Vertrauensstellung hat die Aufträge verschoben, und wenn die Aufträge verwendet werden, wird der Signaturverifizierungsprozess ausgeführt. Wenn die Jobs, Signaturen und Zertifikate alle Teil von Circle of Trustsind, kann die Codesignatur mit Circle of Trust deaktiviert werden.
13. Navigieren zu **Systemeigenschaften** > **Alle.**
14. Suchen Sie nach `com_snc_kmf_signature.validation.flag`, und stellen Sie sicher, dass der Wert auf **true**festgelegt ist.
15. Vergewissern Sie sich, dass eine neue Eigenschaft `com_snc_kmf_signature.validation.certificate` in der Tabelle aufgeführt ist.

Codesignatur verwenden

Erfahren Sie, wie Sie Datensätze, Nachrichten und Anhänge signieren, um die Authentizität und Integrität Ihrer Daten zu überprüfen.

Signieren Sie die Datensätze der JDBC-Datenquelle in der Produktionsinstanz

Verwenden Sie Update Sets, um die JDBC-Datenquellen zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

Signieren Sie die REST- und SOAP-Nachrichten in der Produktionsinstanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie Update Sets, um die REST- und SOAP-Nachrichten zu signieren und zu validieren, indem Sie die Codesignatur in Produktionsinstanzen und vertrauenswürdigen Instanzen aktivieren.

Signieren Sie die Flows, Subflows und Aktionen in der Produktionsinstanz

Verwenden Sie Update Sets, um die Flows, Subflows und Aktionen zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

Signieren Sie bestimmte Datensätze oder Anhänge

Erstellen Sie eine Sicherheitsaufgabe, um bestimmte Datensätze oder Anhänge und nicht alle Datensätze oder Anhänge in einer Tabelle zu signieren.

Eigenständiges Signier-Tool

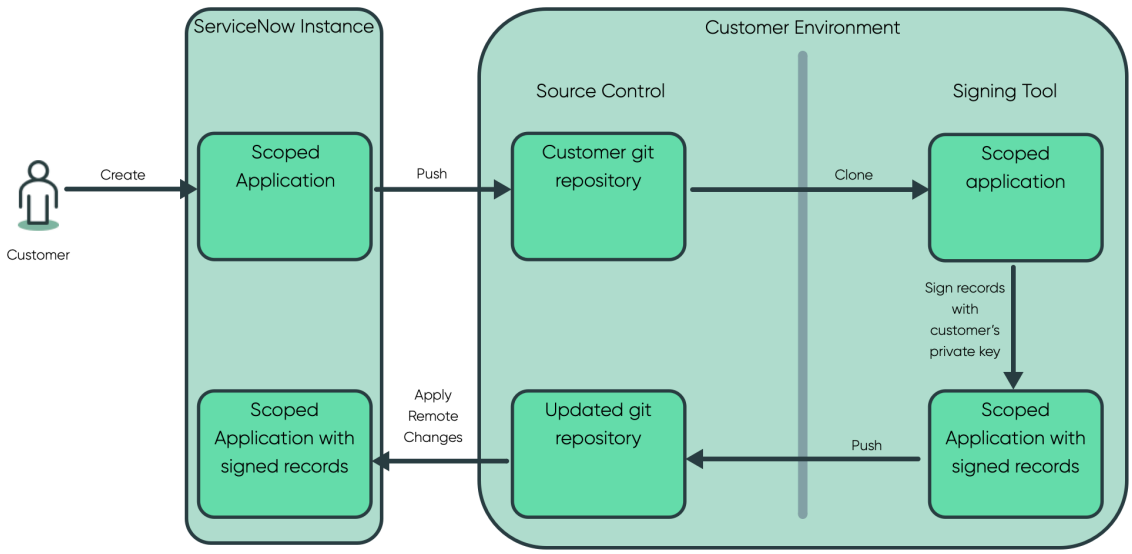
Verwenden Sie das eigenständige Signier-Tool, um unterstützte Datensätze in ServiceNow -Anwendungen mit Ihrem eigenen privaten Schlüssel zu signieren.

Eigenständiges Signier-Tool

Verwenden Sie das eigenständige Signier-Tool, um unterstützte Datensätze in ServiceNow -Anwendungen mit Ihrem eigenen privaten Schlüssel zu signieren.

Verwenden Sie das Signier-Tool, um Datensätze in ServiceNow -Apps zu signieren. Das Tool generiert Signaturen für Datensätze in Ihrer lokalen Umgebung mit Ihrem eigenen privaten Schlüssel.

Signaturtool-Workflow



1. Erstellen oder wählen Sie eine vorhandene ServiceNow Anwendung mit zu signierenden Datensätzen aus, z. B. Business Rules oder Skripteinbindungen.
2. Übertragen Sie die Anwendung in Ihr Git-Repository, das sich in Ihrer Umgebung befindet.

Hinweis:
Anwendungen können mithilfe der Quellcodeverwaltungsintegration zwischen einem Git-Repository und Ihrer Instanz synchronisiert werden. Weitere Informationen zur Konfiguration und Verwendung dieser Integration finden Sie unter Source Control integration .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klonen Sie die Anwendung in Ihrer lokalen Umgebung.
4. Verwenden Sie das Signaturtool (auch in Ihrer lokalen Umgebung), um die unterstützten Datensätze aus der geklonten Anwendung ServiceNow mit Ihrem privaten Schlüssel zu signieren. Das Signier-Tool erstellt Signaturdatensätze und X.509-Zertifikatdatensätze [sys_certificate]. Weitere Informationen zur Verwendung des Signaturtools finden Sie unter Verwenden des Signaturtools.
5. Übertragen Sie die aktualisierte Anwendung in Ihr Git-Repository.
6. Importieren Sie in Ihrer Instanz die aktualisierte Anwendung, indem Sie Remote-Changes anwenden.

Verwenden des Signaturtools

Erfahren Sie, wie Sie das Signier-Tool zum Signieren unterstützter Datensätze in ServiceNow -Anwendungen verwenden.

Vorbereitungen
Erforderliche Rolle: admin

Um diese Schritte auszuführen, benötigen Sie Folgendes:

- Eine ServiceNow -Anwendung mit zu signierenden Datensätzen.
- Ein privater Schlüssel zum Signieren von Datensätzen.
- Das Skript *signRecords.sh* in Ihrer lokalen Umgebung mit Ausführungsberechtigung.

> **Wichtig:**
> Das Skript *signRecords.sh* ist als Teil der JAR-Datei für das Signaturtool enthalten, die Sie anfordern müssen ServiceNow Kundensupport .

Prozedur

1. Navigieren Sie in Ihrer lokalen Umgebung zu dem Verzeichnis mit dem Skript *signRecords.sh*.
2. Verwenden Sie das folgende Befehlsformat, um Ihre Datensätze zu signieren:

```
./signRecords.sh -d [Path to the root directory of the ServiceNow Application to Sign] -f [Path to the Keystore file]
```

   Beispiel:

```
./signRecords.sh -d /users/abc/ServiceNow-App-1 -f /users/abc/codesigning.p12
```

3. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für den Schlüsselspeicher ein.
   Drücken Sie die Eingabetaste, wenn kein Passwort vorhanden ist.
4. Überprüfen Sie die Ausgabe, um eine erfolgreiche Signierung zu bestätigen.

```
Sep 26, 2022 2:41:09 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: executing codesigning...
Sep 26, 2022 2:41:09 PM com.snc.core.codesigning.CodeSignerSupplier get
INFO: CODESIGN: signing record for documentId: 65e811327702111057416efe7c5a994f
Sep 26, 2022 2:41:11 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: codesigning successfully completed!
```

   Im vorherigen Ausgabebeispiel hat das Signaturtool die bereitgestellte Schlüsselspeicherdatei zum Signieren des Datensatzes verwendet. Sie können auch Folgendes sehen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Skript hat den unterstützten Datensatz `65e81132770211057416efe7c5a994f` gefunden und signiert.
- Im Verzeichnis ServiceNow-App-1 werden zwei Datensätze erstellt: `sys_certificate.xml` und `sn_kmf_record_signature.xml`.

5. Importieren Sie die aktualisierte Anwendung zurück in Ihre Instanz, indem Sie Remote-Changes in Studioanwenden.
   Weitere Informationen finden Sie unter Apply remote changes .

Signaturtool-Argumente

Erfahren Sie mehr über die verfügbaren Argumente für das Signaturtool.

Befehlszeilenargumente

Argument	Erforderlich	Beschreibung
-d	Ja	Stammverzeichnis des zu signierenden Projekts. Sollte das Projektverzeichnis (zufällig 32 alphanumerisch), die Datei sn_source_control.properties und eine enthalten<project_name> .iml-Datei
-f	Ja	Der Dateipfad des Schlüsselspeichers
-a	Nein	Alias, der für den Zugriff auf einen bestimmten Eintrag im Schlüsselspeicher verwendet wird.
-c	Nein	Verketten Sie Datensatzsignaturen in einer Datei.
-k	Nein	Passwort für den Zugriff auf den im Schlüsselspeicher gespeicherten Schlüssel. Sie können dieses Passwort auch eingeben, wenn Sie dazu aufgefordert werden, anstatt innerhalb des Arguments.
-o	Nein	Signieren Sie mit einem neuen Zertifikat anstelle vorhandener sys_cert-Dateien.
-p	Nein	Passwort für den Zugriff auf den Schlüsselspeicher, wenn dieser über ein Passwort verfügt. Sie können dieses Passwort auch eingeben, wenn Sie dazu aufgefordert werden, anstatt innerhalb des Arguments.
-w	Nein	Löschen Sie alle vorhandenen Signaturdatensatzdateien.
-h	Nein	Diese Hilfemeldung anzeigen und beenden.

Signieren Sie die Datensätze der JDBC-Datenquelle in der Produktionsinstanz

Verwenden Sie Update Sets, um die JDBC-Datenquellen zu signieren und zu validieren, indem Sie die Codesignatur in Produktionsinstanzen und vertrauenswürdigen Nicht-Produktionsinstanzen aktivieren.

- Richten Sie Circle of Trust zwischen der Produktions- und vertrauenswürdigen Instanz ein.
- Erforderliche Rolle: security_admin

Hinweis:

- MID-Server verarbeitet die Dateidatenquellen nicht und daher sind diese Datenquellen nicht mit Code signiert.
- LDAP-Datenquellen können nicht mit Codesignatur signiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Signieren Sie vorhandene Datenquellen vom Typ JDBC

Verwenden Sie Update Sets, um Massensignaturaufträge für die Produktionsinstanz bereitzustellen.

Prozedur

1. Konfigurieren Sie in der vertrauenswürdigen Instanz den KMF-Signierauftrag zum Signieren der Datenquellen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Massensignaturdatensätze aus**.
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie **Datenquelle aus**.

   d. Klicken Sie **auf Codesignaturauftrag in Produktion exportieren**.
   Eine Bestätigungsmeldung wird angezeigt, dass das Update Set signiert ist.

   e. Exportieren Sie das generierte Update Set in eine XML-Datei.

2. Importieren und bestätigen Sie das Update Set in der Produktionsinstanz, um die signierten Massenaufträge von der vertrauenswürdigen Instanz abzurufen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

   b. Öffnen Sie das Update Set, das aus der vertrauenswürdigen Instanz exportiert wurde.

   c. Klicken Sie auf **Start**.
   Eine Bestätigungsmeldung wird angezeigt, dass die Datensätze signiert sind.

Signieren Sie neue Datenquellen vom Typ JDBC

Verwenden Sie Update Sets, um das signierte Update Set auf die Produktionsinstanz zu übertragen.

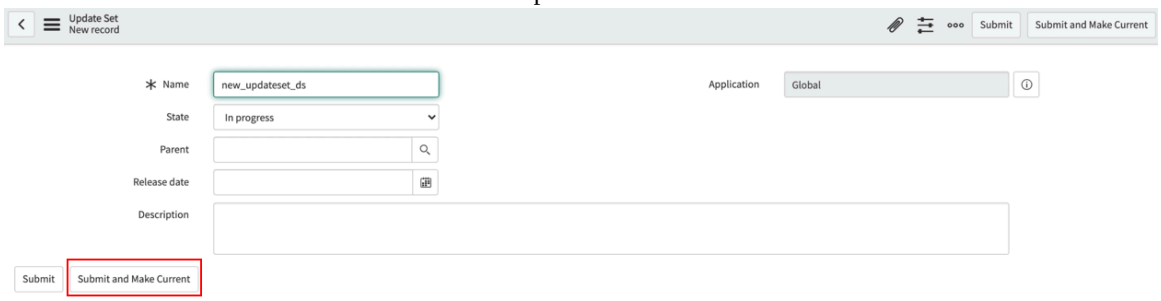
Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

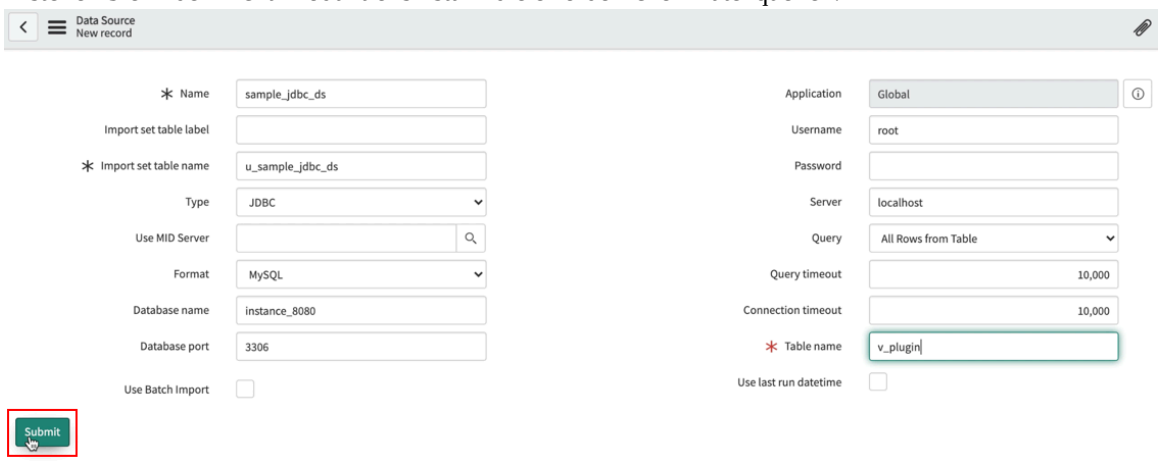
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Starten Sie in der Nicht-Produktionsinstanz ein Update Set.

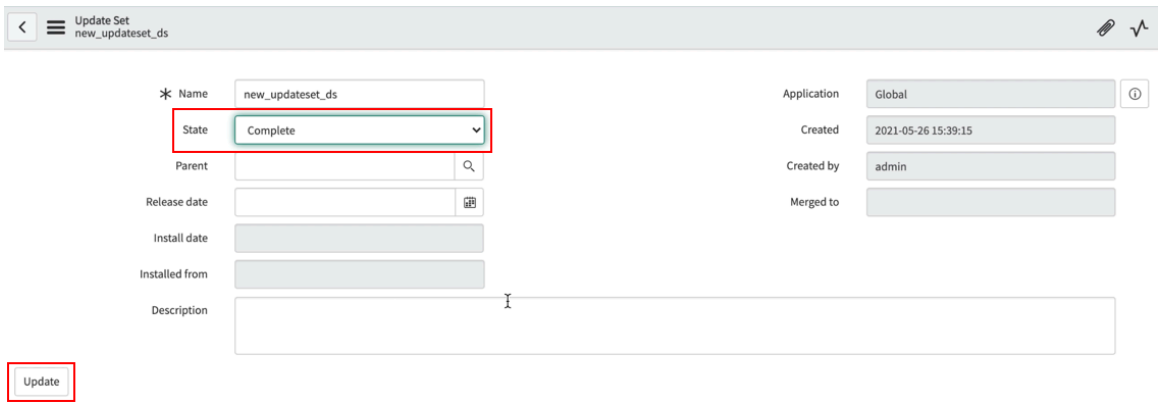


2. Erstellen Sie in der Nicht-Produktionsinstanz die erforderlichen Datenquellen.



Die Datenquellen werden dem Update Set hinzugefügt.

3. Ändern Sie in der Nicht-Produktionsinstanz den Status des Update Set in **Abgeschlossen** und klicken Sie auf **Aktualisieren**.



4. Signieren Sie in der Nicht-Produktionsinstanz das Update Set, indem Sie einen Verschlüsselungsauftrag erstellen.

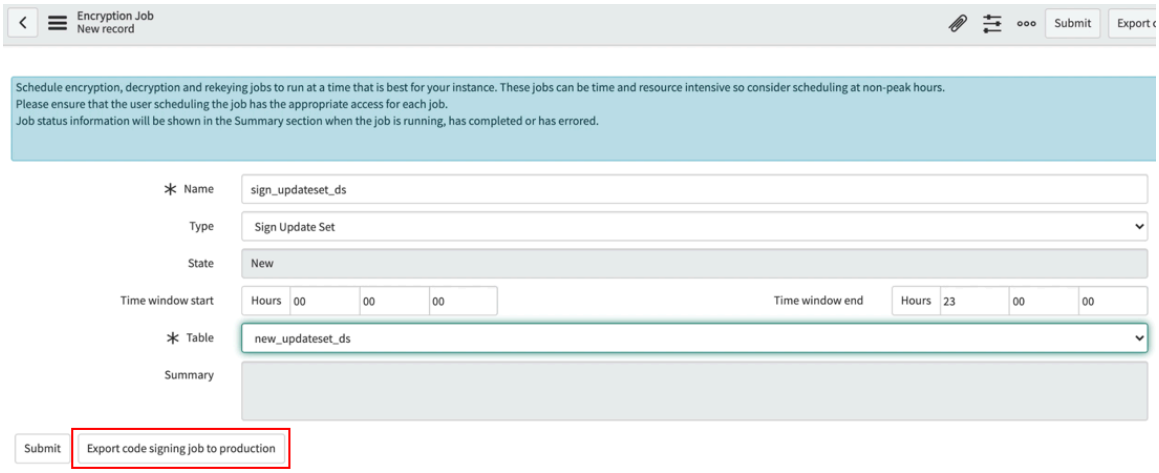
   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

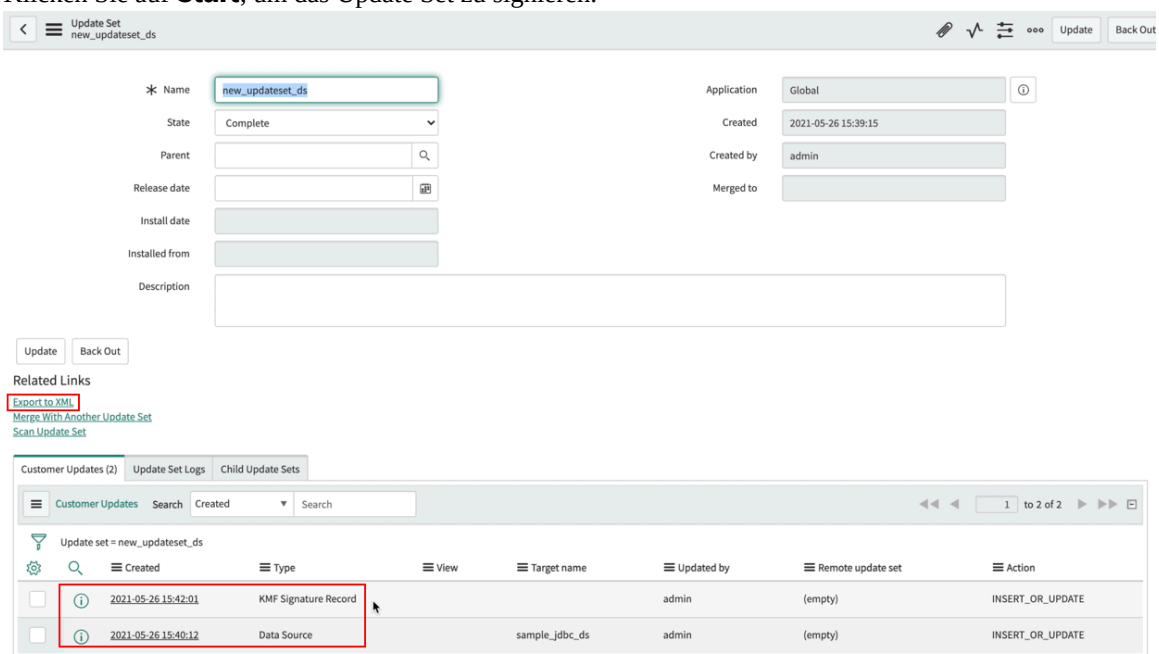
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Update Set signieren aus**.
Tabelle	Update Set, aus dem die Datensätze signiert werden sollen.



d. Klicken Sie auf **Absenden**.

e. Klicken Sie auf **Start**, um das Update Set zu signieren.



- Die**Zusammenfassung** wird aktualisiert, sobald die Datensätze signiert sind.
- Das Update Set wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der Nicht-Produktionsinstanz den signierten Update Set-Datensatz, und exportieren Sie ihn in eine XML-Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Importieren Sie das signierte Update Set in der Produktionsinstanz.

   a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

   b. Klicken Sie auf den zugehörigen Link **Update Set aus XML** importieren, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
   Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen.
   Das Update Set wurde erfolgreich bestätigt.

Signieren Sie die REST- und SOAP-Nachrichten in der Produktionsinstanz

Verwenden Sie Update Sets, um die REST- und SOAP-Nachrichten zu signieren und zu validieren, indem Sie die Codesignatur in Produktions- und Nicht-Produktionsinstanzen aktivieren.

- Richten Sie Circle of Trust zwischen Produktions- und Nicht-Produktionsinstanzen ein.
- Erforderliche Rolle: security_admin

Signieren Sie die vorhandenen REST- und SOAP-Nachrichten

Signieren und validieren Sie die vorhandenen REST- und SOAP-Nachrichten, indem Sie die Codesignatur in Produktionsinstanzen und vertrauenswürdigen Nicht-Produktionsinstanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Konfigurieren Sie in der vertrauenswürdigen Instanz den KMF-Signierauftrag zum Signieren der UI-Aktionen.

   a. Navigieren Sie zu KMF-Signaturkonfiguration.

   b. Füllen Sie diese Werte im Formular aus.

Formular „KMF-Signaturkonfiguration“

Feld	Beschreibung
Tabellenname	Glide-Tabellenname. Wählen Sie beispielsweise **UI-Aktionen [sys_ui_action] aus**.
KMF-Signatur-Zweck	Zweck des Signierens der Datensätze. Wählen Sie **ECC-Warteschlange aus**.
Signaturerzeugungsfelder	Felder in der Datenquelle, die Sie signieren möchten. Wenn Änderungen an den Werten in einem oder mehreren dieser Felder vorgenommen werden, wird die zuvor generierte Signatur ungültig. Wählen Sie **Name** und **Skript aus**.
Signaturerzeugungsfilter	Filterkriterien, die zum Signieren der Datensätze erfüllt sein müssen.
Anhang signieren	Option zum Signieren des Anhangs im Glide-Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Instanzschlüssel	Option zur Verwendung des Instanzschlüssels.

c. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.

2. Signieren Sie in der vertrauenswürdigen Instanz die erforderlichen Datensätze.

a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

b. Klicken Sie auf **Neu**.

c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Massensignaturdatensätze aus**.
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie **UI-Aktion aus**.

d. Klicken Sie **auf Codesignaturauftrag in Produktion exportieren**.
Zwei lokal signierte Update Sets werden erstellt.

- Ein Update Set für die Konfiguration der UI-Aktion.
- Ein weiteres Update Set aus dem Verschlüsselungsauftrag, um den Codesignaturauftrag zu exportieren.

3. Exportieren Sie in der vertrauenswürdigen Instanz das lokale Update Set in eine XML-Datei.

a. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**.

b. Öffnen Sie das Update Set, das Sie für die Massensignierung der Datensätze erstellt haben.

c. Klicken Sie **auf den zugehörigen Link In XML** exportieren, und speichern Sie die XML-Datei.

4. Importieren Sie die Update Sets in der Produktionsinstanz.

a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML** importieren, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen.
Das Update Set wurde erfolgreich bestätigt.

5. Führen Sie in der Produktionsinstanz den Verschlüsselungsauftrag aus, den Sie zuvor in der vertrauenswürdigen Instanz erstellt haben, indem Sie **Start**auswählen.
Eine Bestätigungsmeldung mit der Bestätigung, dass die Datensätze signiert sind, wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Signieren Sie neue REST- und SOAP-Nachrichten

Signieren und validieren Sie die neuen REST- und SOAP-Nachrichten der vertrauenswürdigen Instanz, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

Prozedur

1. Starten Sie in der Nicht-Produktionsinstanz ein Update Set.
2. Erstellen Sie in der Nicht-Produktionsinstanz die erforderlichen REST- oder SOAP-Nachrichten.
   Die Nachrichten werden dem Update Set hinzugefügt.
3. Ändern Sie in der Nicht-Produktionsinstanz den Status des Update Set in **Abgeschlossen** und klicken Sie auf **Aktualisieren**.
4. Signieren Sie in der Nicht-Produktionsinstanz das Update Set, indem Sie einen Verschlüsselungsauftrag erstellen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Update Set signieren aus**.
Tabelle	Update Set, aus dem die Datensätze signiert werden sollen. Wählen Sie **Neues REST V2-Update Set signieren – 1 aus**.

   d. Klicken Sie auf **Absenden**.

   e. Klicken Sie auf **Start**, um das Update Set zu signieren.
      - Die**Zusammenfassung** wird aktualisiert, sobald die Datensätze signiert sind.
      - Das Update Set wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der Nicht-Produktionsinstanz den signierten Update Set-Datensatz, und exportieren Sie ihn in eine XML-Datei.
6. Importieren Sie das Update Set in der Produktionsinstanz.

   a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

   b. Klicken Sie auf den zugehörigen Link **Update Set aus XML** importieren, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
   Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen.
   Das Update Set wurde erfolgreich bestätigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Signieren Sie die Flows, Subflows und Aktionen in der Produktionsinstanz

Verwenden Sie Update Sets, um die Flows, Subflows und Aktionen zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

Vorbereitungen

- Richten Sie Circle of Trust zwischen der Produktions- und vertrauenswürdigen Instanz ein.
- Erforderliche Rolle: security_admin

Signieren Sie den vorhandenen Flow, die Subflows und die Aktionen

Signieren und validieren Sie den vorhandenen Flow, die Subflows und die Aktionen, indem Sie die Codesignatur in Produktions- und vertrauenswürdigen Nicht-Produktionsinstanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Signieren Sie in der vertrauenswürdigen Instanz die Datensätze in der Schrittinstanztabelle.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Massensignaturdatensätze aus**.
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie **Schrittinstanz aus**.

   d. Klicken Sie **auf Codesignaturauftrag in Produktion exportieren**.
   Zwei lokal signierte Update Sets werden erstellt.
   - Ein Update Set für die KMF-Signatur.
   - Ein weiteres Update Set aus dem Verschlüsselungsauftrag, um den Codesignaturauftrag zu exportieren.

2. Exportieren Sie in der vertrauenswürdigen Instanz das lokale Update Set in eine XML-Datei.

   a. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**.

   b. Öffnen Sie das Update Set, das Sie für die Massensignierung der Datensätze erstellt haben.

   c. Klicken Sie **auf den zugehörigen Link In XML** exportieren, und speichern Sie die XML-Datei.

3. Importieren Sie die XML-Datei in der Produktionsinstanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML** importieren, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen.
Das Update Set wurde erfolgreich bestätigt.

4. Führen Sie in der Produktionsinstanz den Verschlüsselungsauftrag aus, den Sie zuvor in der vertrauenswürdigen Instanz erstellt haben.

a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

b. Öffnen Sie den Verschlüsselungsauftrag, den Sie zuvor in der vertrauenswürdigen Instanz erstellt haben.

c. Klicken Sie auf **Starten**, um die Aufgabe zu starten.
Eine Bestätigungsmeldung mit der Bestätigung, dass die Datensätze signiert sind, wird angezeigt.

Signieren Sie neue Flows, Subflows und Aktionen

Signieren und validieren Sie neue Flows, Subflows und Aktionen, indem Sie die Codesignatur in Produktions- und vertrauenswürdigen Nicht-Produktionsinstanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Starten Sie in der vertrauenswürdigen Instanz ein Update Set.
2. Erstellen Sie in der vertrauenswürdigen Instanz die erforderlichen Flows, Subflows oder Aktionen, und veröffentlichen Sie sie.
Die Flows, Subflows oder Aktionen werden dem Update Set hinzugefügt.
3. Ändern Sie in der vertrauenswürdigen Instanz den Status des Update Set in **Abgeschlossen**, und klicken Sie auf **Aktualisieren**.
4. Signieren Sie in der vertrauenswürdigen Instanz das Update Set, indem Sie einen Verschlüsselungsauftrag erstellen.

a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**.

b. Klicken Sie auf **Neu**.

c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Update Set signieren aus**.
Tabelle	Update Set, aus dem die Datensätze signiert werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Klicken Sie auf **Absenden**.

e. Klicken Sie auf **Start**, um das Update Set zu signieren.

- Die**Zusammenfassung** wird aktualisiert, sobald die Datensätze signiert sind.
- Das Update Set wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der vertrauenswürdigen Instanz den signierten Update Set-Datensatz, und exportieren Sie ihn in eine XML-Datei.

6. Importieren Sie das signierte Update Set in der Produktionsinstanz.

a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

b. Wählen Sie den zugehörigen Link **Update Set aus XML** importieren aus, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen.
Das Update Set wurde erfolgreich bestätigt.

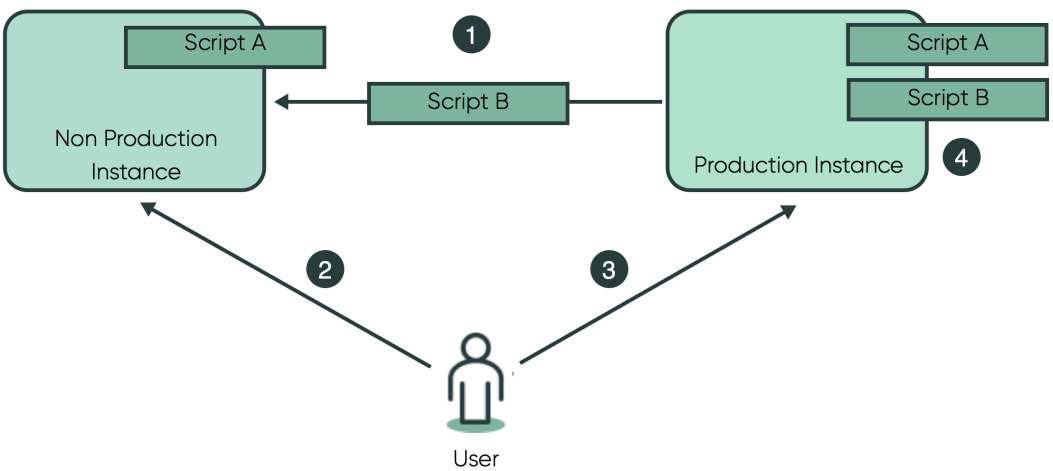
Signieren Sie bestimmte Datensätze oder Anhänge

Erstellen Sie eine Sicherheitsaufgabe, um bestimmte Datensätze oder Anhänge und nicht alle Datensätze oder Anhänge in einer Tabelle zu signieren.

Ab Release Vancouver können Sicherheitsadministratoren Sicherheitsaufträge verwenden, um bestimmte Datensätze in einer Tabelle anstatt aller Datensätze in einer Tabelle zu signieren. Signieren Sie bestimmte Datensätze, um ein versehentliches Signieren von nicht überprüftem Code zu vermeiden.

Diese Aufträge enthalten eine angehängte Protokolldatei, die am Ende des Signierauftrags generiert wird. Diese Protokolldatei enthält Informationen zu signierten Datensätzen und der verwendeten Signaturkonfiguration.

Signiervorgang



Dieses Diagramm zeigt ein Beispiel für die Verwendung des Signaturvorgangs. In diesem Beispiel ist ein Skript mit der Bezeichnung Skript B nur in der Produktionsinstanz vorhanden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und muss zum Signieren in eine vertrauenswürdige Instanz importiert werden. Skript A ist bereits in beiden Instanzen vorhanden und muss nicht signiert werden. Sie wurde entweder bereits überprüft und signiert oder wurde noch nicht überprüft und sollte nicht signiert werden.

1. Importieren Sie den Datensatz in Ihre vertrauenswürdige Umgebung.
2. Erstellen Sie in der vertrauenswürdigen Instanz einen Signierauftrag, um den Datensatz zu signieren. Dieser Prozess wird in Erstellen Sie eine Aufgabe, um bestimmte Datensätze oder Anhänge in einer vertrauenswürdigen Instanz zu signierenbeschrieben.
3. Importieren Sie den signierten Signierauftrag mithilfe eines Update Sets in Ihre Produktionsinstanz.
4. Führen Sie in der Produktionsinstanz den importierten Signierauftrag aus.

Erstellen Sie eine Aufgabe, um bestimmte Datensätze oder Anhänge in einer vertrauenswürdigen Instanz zu signieren

Signieren Sie einen bestimmten Datensatz oder eine Gruppe von Datensätzen, die Sie in einer vertrauenswürdigen Nicht-Produktionsinstanz definieren.

Vorbereitungen

Erforderliche Rolle: security_admin oder sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen**.
2. Im **Feld Welche Art von Sicherheitsauftrag möchten Sie erstellen?** Eingabeaufforderung, wählen Sie **Signierauftrag**aus.
   Ein neuer **Signaturauftragsdatensatz** wird angezeigt.
3. Füllen Sie im Formular die Felder nach Bedarf aus:

Signierauftragsfelder

Feld	Beschreibung
Name	Beschreibender Name für diesen Auftrag.
Typ	Typ des Sicherheitsauftrags. Um bestimmte **Datensätze** zu signieren, wählen Sie die Option Bestimmte Datensätze signieren aus. Um bestimmte Anhänge zu signieren, wählen Sie **Spezifische Anhänge**signieren aus.
Status	Status dieses Auftrags. Dieses Feld beginnt mit dem Wert **New**. Dieses Feld ist schreibgeschützt.
Tabelle	Tabelle mit den Datensätzen oder Anhängen, die Sie signieren möchten. Wenn Sie Anhänge signieren, wählen Sie die Tabelle mit den Datensätzen aus, der die Anhänge zugeordnet sind, und nicht die Tabelle „Anhang“ [sys_attachment].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

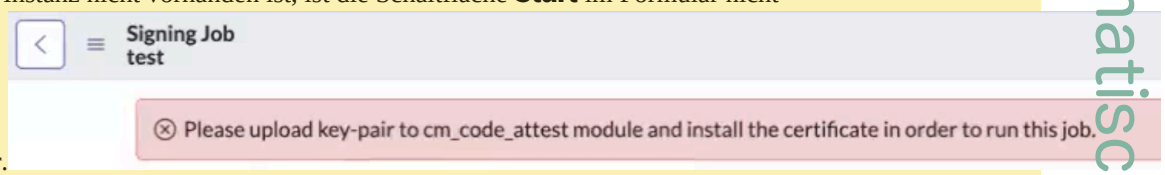
Feld	Beschreibung
	Tipp: Überprüfen Sie die Tabelle „KMF-Signaturdatensatz“ [sn_kmf_record_signature], um sicherzustellen, dass für die ausgewählte Tabelle noch keine Signaturen vorhanden sind.
Datensätze filtern	Filterbedingungen, die verwendet werden, um zu begrenzen, welche Datensätze in der Tabelle **„Datensätze zum Signieren auswählen“ angezeigt** werden.
Datensätze zum Signieren auswählen	Liste der Datensätze in der im Feld „Tabelle“ ausgewählten **Tabelle**, eingeschränkt durch den im Feld „Datensätze filtern“ erstellten **Filter**. Verschieben Sie Datensätze aus dem Fenster **„Verfügbar** “ in das Fenster „ **Ausgewählt** “, um sie in den Signierauftrag aufzunehmen.
Zeitfensterstart	Der Beginn des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird nach der in diesem Feld eingegebenen Zeit ausgeführt. Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.
Zeitfensterende	Das Ende des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird vor der in diesem Feld eingegebenen Zeit ausgeführt. Wenn die Aufgabe noch nicht abgeschlossen ist, wird die Aufgabe angehalten und beim nächsten Start des Zeitfensters fortgesetzt. Die Endzeit muss nach der Startzeit liegen. Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.
Zusammenfassung	Zusammenfassung der Ausführung dieses Auftrags. Dieses Feld ist schreibgeschützt.

4. Klicken Sie mit der rechten Maustaste auf die Formularkopfzeile, und wählen **Sie Speichern**aus.
5. Wählen Sie am unteren Rand des Formulars Codesignaturauftrag **in Produktion exportieren aus**.
   Mit dieser Aktion wird der Signierauftrag signiert, und er ist bereit für den Export.
6. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**
7. Suchen und öffnen Sie das Update Set für Ihren Signierauftrag.
   Auf der Registerkarte „Kunden-Updates“ können Sie sehen, dass dieses Update Set die Signieraufgabe und den Signaturdatensatz enthält.
8. Wählen Sie **In XML exportieren aus**.
   Mit dieser Aktion wird eine XML-Datei erstellt, die Ihr Update Set auf Ihrem lokalen Gerät enthält.
9. Navigieren Sie in Ihrer Produktionsinstanz zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze** > **.**
10. Wählen Sie unten auf der Seite **Update Set aus XML importieren aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

11. Klicken Sie auf die Schaltfläche **Datei** wählen, und wählen Sie die XML-Datei aus, die in den vorherigen Schritten erstellt wurde.
12. Wählen Sie **Hochladen** aus.
    Ihr Update Set wird geladen und in der Liste **Retrieved Update Sets** (Abgerufene Update Sets) angezeigt.
13. Öffnen Sie in der Liste **„Abgerufene Update Sets“** den Datensatz für das importierte Update Set.
14. Klicken Sie auf die Schaltfläche **Preview Update Set** (Vorschau auf Update Set).
    Nachdem die Vorschau erfolgreich abgeschlossen wurde, wird die Schaltfläche **Update Set** festlegen angezeigt.
15. Wählen Sie **Update Set festlegen aus**.
16. **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**.
17. Öffnen Sie Ihren Signierauftrag.
18. Wählen Sie **Starten** aus, um den Signierauftrag auszuführen.

⚠ Warnung:
Wenn das Schlüsselpaar nicht in Ihre Produktionsinstanz hochgeladen wurde, wird oben im Datensatzformular eine Warnung angezeigt. Wenn dieses Schlüsselpaar in Ihrer Instanz nicht vorhanden ist, ist die Schaltfläche **Start** im Formular nicht sichtbar.



Nächste Maßnahme
Nach Abschluss werden im Feld **Zusammenfassung** die Ergebnisse der Aufgabe angezeigt. An Ihren Signaturauftragsdatensatz ist auch eine Protokolldatei mit dem Namen „Mass_Sign_Records-“ angehängt.<sys_id> “. Überprüfen Sie diesen Datensatz auf Details zum Auftrag und eine Liste der sys_ids für jeden signierten Datensatz.

Signieren Sie bestimmte Datensätze oder Anhänge in einer Produktionsinstanz

Signieren Sie einen bestimmten Datensatz oder eine Gruppe von Datensätzen, die Sie in einer Produktionsinstanz definieren.

Vorbereitungen
Erforderliche Rolle: security_admin oder sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie keine Vertrauensstellung zwischen Ihrer Produktion und vertrauenswürdigen Instanzen eingerichtet haben, können Sie Ihre Datensätze oder Anhänge mit den folgenden Schritten direkt in Ihrer Produktionsinstanz signieren. Informationen zum Erstellen dieser Beziehung zwischen Ihren Instanzen finden Sie unter Laden Sie die erforderlichen Schlüsselpaare und Zertifikate für die Codesignatur.

Prozedur
1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen**.
2. Im **Feld Welche Art von Sicherheitsauftrag möchten Sie erstellen?** Eingabeaufforderung **Signierauftrag**auswählen.
   Ein neuer **Signaturauftragsdatensatz** wird angezeigt.
3. Füllen Sie im Formular die Felder nach Bedarf aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Signierauftragsfelder

Feld	Beschreibung
Name	Beschreibender Name für diesen Auftrag.
Typ	Typ des Sicherheitsauftrags. Um bestimmte **Datensätze** zu signieren, wählen Sie die Option Bestimmte Datensätze signieren aus. Um bestimmte Anhänge zu signieren, wählen Sie **Spezifische Anhänge**signieren aus.
Status	Status dieses Auftrags. Dieses Feld beginnt mit dem Wert **New**. Dieses Feld ist schreibgeschützt.
Tabelle	Tabelle mit den Datensätzen oder Anhängen, die Sie signieren möchten. Wenn Sie Anhänge signieren, wählen Sie die Tabelle mit den Datensätzen aus, der die Anhänge zugeordnet sind, und nicht die Tabelle „Anhang“ [sys_attachment]. **Tipp:** Überprüfen Sie die Tabelle „KMF-Signaturdatensatz“ [sn_kmf_record_signature], um sicherzustellen, dass für die ausgewählte Tabelle noch keine Signaturen vorhanden sind.
Datensätze filtern	Filterbedingungen, die verwendet werden, um zu begrenzen, welche Datensätze in der Tabelle **„Datensätze zum Signieren auswählen“ angezeigt** werden.
Datensätze zum Signieren auswählen	Liste der Datensätze in der im Feld Tabelle ausgewählten **Tabelle**, begrenzt durch den im Feld Datensätze filtern erstellten **Filter**. Verschieben Sie Datensätze aus dem Fenster **„Verfügbar** “ in das Fenster „ **Ausgewählt** “, um sie in den Signierauftrag aufzunehmen.
Zeitfensterstart	Der Beginn des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird nach der in diesem Feld eingegebenen Zeit ausgeführt. Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.
Zeitfensterende	Das Ende des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird vor der in diesem Feld eingegebenen Zeit ausgeführt. Wenn die Aufgabe noch nicht abgeschlossen ist, wird die Aufgabe angehalten und beim nächsten Start des Zeitfensters fortgesetzt. Die Endzeit muss nach der Startzeit liegen. Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusammenfassung	Zusammenfassung der Ausführung dieses Auftrags. Dieses Feld ist schreibgeschützt.

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Der Sicherheitsauftrag wird zwischen den in den Feldern **Zeitfensterstart** und **Zeitfensterende** angegebenen Zeiten ausgeführt, oder wenn Sie auf die Schaltfläche **Ausführen** klicken. Nach Abschluss werden im Feld **Zusammenfassung** die Ergebnisse der Aufgabe angezeigt. An Ihren Signaturauftragsdatensatz ist auch eine Protokolldatei mit dem Namen „Mass_Sign_Records-“ angehängt.<sys_id> “. Überprüfen Sie diesen Datensatz auf Details zum Auftrag und eine Liste der sys_ids für jeden signierten Datensatz.

Codesignaturreferenz

Referenzthemen enthalten zusätzliche Informationen zur Verwaltung und Problembehandlung der Codesignatur.

Mit Codesignatur installierte Eigenschaften

Codesignatur fügt die folgenden Eigenschaften hinzu.

Problembehandlung und Zugriff auf -Protokolle

Greifen Sie auf verschiedene Protokolle zu, um Fehler zu beheben und die Fehlerursachen zu identifizieren.

Mit Codesignatur installierte Eigenschaften

Codesignatur fügt die folgenden Eigenschaften hinzu.

Eigenschaft	Typ	Beschreibung
com.glide.codesigning.expanded.tracking.enabled	Wahr|Falsch	Bei „true“ wird die Validierungslänge für den Metastapel für ecc_queue-Themen erhöht, die in der Eigenschaft **com.glide.codesigning.expanded_tracking.topic.list** aufgeführt sind. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.expanded.tracking.length	Ganzzahl	Ebenen der Codesignaturvalidierung, die auftreten sollen, wenn Codesignatur aktiviert ist. Der Standardwert ist 3. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.expanded_tracking.topic.list	Zeichenfolge	Kommagetrennte Liste von Themen, die einer erhöhten Metastapelnachverfolgung unterliegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Typ	Beschreibung
		Wichtig: Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.tracking.agent.validation.exclusion_list	Zeichenfolge	Kommagetrennte Liste von ecc_queue-Agents, für die die Codesignatur übersprungen werden soll
com.glide.codesigning.tracking.debug	Wahr|Falsch	Bei „true“ ist die Debug-Protokollierung für den Codesignatur-Tracker aktiviert.
com.glide.codesigning.tracking.enabled	Wahr|Falsch	Bei „wahr“ wird die Nachverfolgung von Codesignatur-Anrufern aktiviert. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.tracking.logging.enabled	Wahr|Falsch	Bei „wahr“ wird die Protokollierung für die Nachverfolgung der Codesignatur aktiviert.
com.glide.codesigning.tracking.unsupported_scripts_tracking.enabled	Wahr|Falsch	Bei „wahr“ werden ecc_queue-Datensätze, die über nicht unterstützte Skripts eingefügt wurden (sofern erkannt), nicht notariell beglaubigt. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.tracking.validation.fail_smart	Wahr|Falsch	Bei „wahr“ schlägt die Überprüfung der Codesignatur beim ersten Fehler bei der Skriptvalidierung fehl, anstatt alle Skripts zu überprüfen. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.event_handler.code_signing.tracking	Zeichenfolge	Definiert den Event Handler, der dafür sorgt, dass Kunden, die die Codesignatur neu aktivieren, so sicher wie möglich konfiguriert werden. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.web_service_outbound.impl.codesigning.tracking	Wahr|Falsch	Bei „wahr“ wird die Nachverfolgung der SOAPMessageV2-Codesignatur aktiviert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Typ	Beschreibung
		Wichtig: Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.snc.csf.servicenow_root_of_trust.disabled	Wahr|Falsch	Gibt an, ob die Funktion „Root of Trust“ aktiv ist. Der Standardwert ist `false`, was bedeutet, dass ServiceNow Build-Zertifikate vertrauenswürdig sind. **Wichtig:** Diese Eigenschaft kann nur mithilfe einer signierten geplanten Aufgabe von einem Benutzer mit den Rollen „Administrator“, „Sicherheitsadministrator“ und „KMF-Manager“ geändert werden. Weitere Informationen zum Ändern Ihres Root of Trust finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.
com.snc.kmf.signature.validation.optin	Wahr|Falsch	Bei „true“ wird Codesignatur in Ihrer Instanz aktiviert. **Wichtig:** Diese Eigenschaft kann nur über eine Anforderung an Kundenservice und Supportgeändert werden. Weitere Informationen finden Sie unter KB1205749
glide.jdbcprobeloader.tracking	Wahr|Falsch	Schaltet die Codesignatur für JDBC-Datenquellen ein oder aus. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
glide.rest.codesigning.tracking	Wahr|Falsch	Bei „wahr“ wird die Nachverfolgung der RESTMessageV2-Codesignatur aktiviert. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.

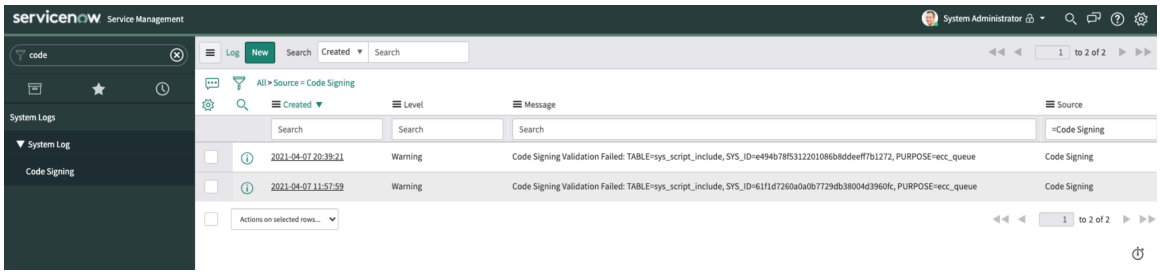
Problembehandlung und Zugriff auf -Protokolle

Greifen Sie auf verschiedene Protokolle zu, um Fehler zu beheben und die Fehlerursachen zu identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignaturprotokolle

Wenn einer der ECC-Warteschlangendatensätze nicht von der Code Signing Tracker-API signiert ist, werden die nicht signierten Nachrichten und die erforderlichen Details im Codesignaturmodul angezeigt. Navigieren zu **Systemprotokolle** > **Systemprotokoll** > **Codesignatur** , um auf die Liste der nicht vertrauenswürdigen Datensätze zuzugreifen.

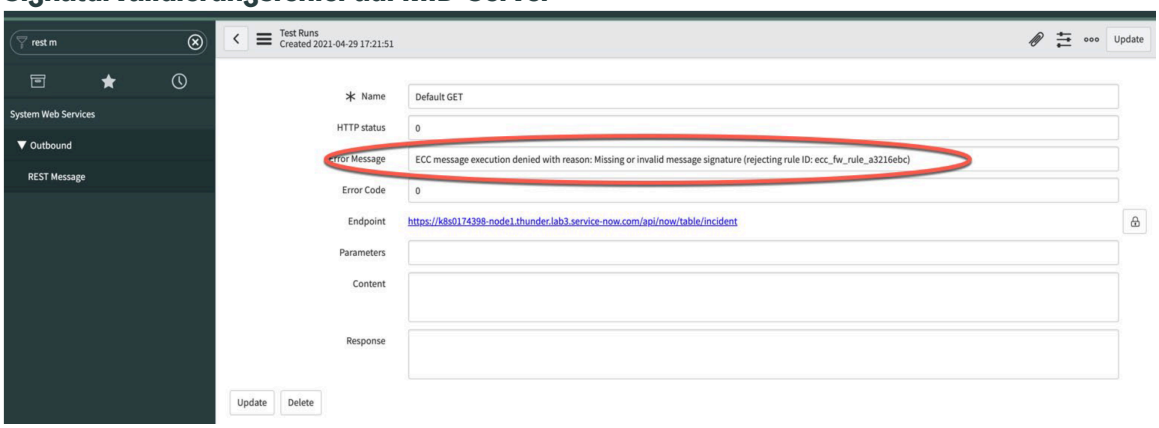


Aktivieren Sie für zusätzliche Debug-Knoten-Protokolle *com.glide.codesigning.tracking.debug*, und legen Sie den Wert auf truefest.

Fehler bei der Validierung der REST-Nachrichtensignatur am MID-Server

Greifen Sie auf die Fehlermeldung bezüglich des Signaturvalidierungsfehlers zu, indem Sie zu navigieren **System-Webservices** > **Ausgehend** > **REST-Nachricht** und Öffnen des erforderlichen REST-Nachrichtendatensatzes.

Signaturvalidierungsfehler auf MID-Server

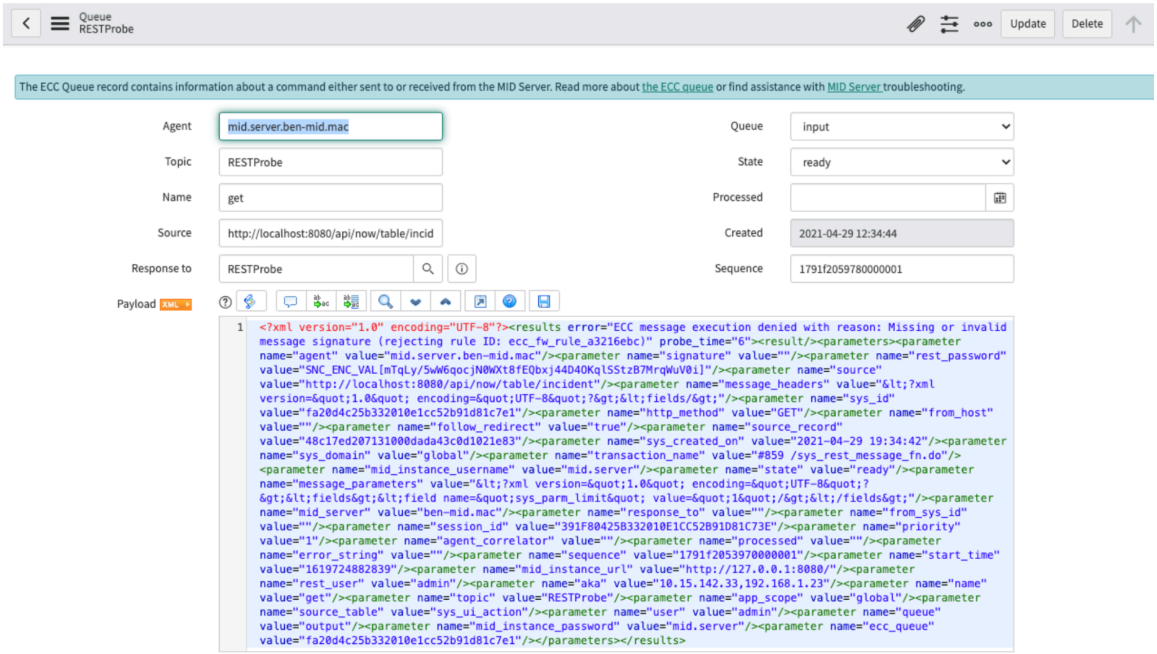


Hinweis:

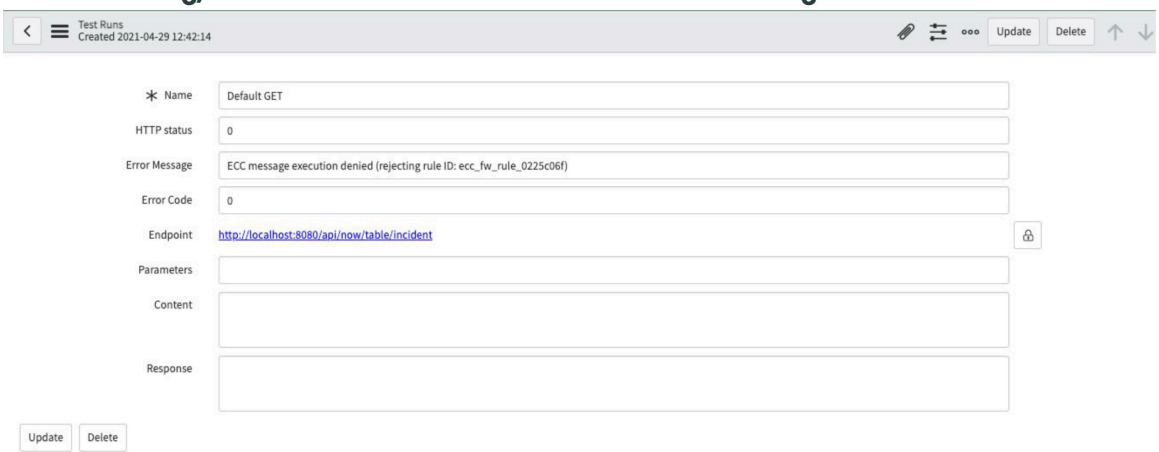
Fehlermeldungen im Zusammenhang mit den ECC-Firewall-Ablehnungen beginnen mit ECC-Nachrichtenausführung verweigert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ECC-Warteschlange, wenn die Signaturvalidierung auf fehlschlägt MID-Server



Fehlermeldung, wenn die ECC-Nachricht durch die Benutzerregel blockiert wird



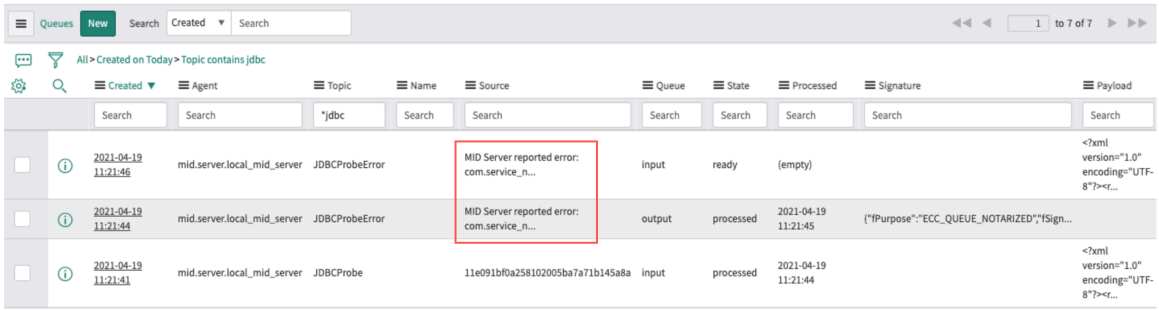
JDBC-Probe

Wenn eine JDBC-Datenquelle mit einer ungültigen oder fehlenden Signatur auf einem MID-Serverausgeführt wird, wird eine Fehlermeldung mit den erforderlichen Details angezeigt.

Quelle zeigt auch die Details der Fehlermeldung an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



MID-Server Protokolle

Um die detaillierte ECC-Firewallprotokollierung zu aktivieren, erhöhen Sie die Protokollebene, indem Sie den Wert des MID Server -Konfigurationsparameters `mid.log.level` auf TRACE festlegen. Die detaillierten Protokolle enthalten Informationen zu:

- Regeln, die MID-Server aus der Startkonfigurationsdatei geladen hat.
- Granulare Ausführungsnachverfolgung von Regeln.
- Spezifische Regel, aufgrund derer eine ECC-Nachricht akzeptiert oder abgelehnt werden soll.

Hinweis:
Wenn „boot-config.xml“ ungültig ist, kann MID-Server nicht gestartet werden, und die Fehlerdetails werden in den MID Agent-Protokollen protokolliert.

Sicherheitsrollen

Sicherheitsrollen bieten zusätzliche Sicherheit. Jeder Benutzer muss mindestens eine Rolle haben, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Erkunden Sie explizite Rollen

Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von expliziten Rollen kennen.

Erkunden Sie erweiterte Berechtigungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie, wie die Rolle mit erhöhten Berechtigungen sitzungsbasierte Berechtigungen aktiviert.

Explizite Rollen

Sie können internen Benutzern und externen Benutzern Zugriff auf Ihre Instanz gewähren. Möglicherweise möchten Sie jedoch nicht, dass beide Benutzertypen dieselben Zugriffsrechte haben. Um die Sicherheit zu erhöhen, muss jeder Benutzer mindestens eine Rolle besitzen, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Ab Release Paris können Benutzer nicht mehr beide expliziten Rollen (snc_internal und snc_external) haben. Auch durch Gruppen- und Rolleneinschluss dürfen nicht beide Rollen enthalten sein, da dies dazu führen würde, dass jedes Gruppenmitglied oder jeder Benutzer, der einer solchen Gruppe oder Rolle zugeordnet ist, automatisch beide Rollen hätte. Now Platform bricht jeden Vorgang ab, der ein solches Szenario hervorrufen würde.

Externe Benutzer müssen mindestens die Rolle snc_external erhalten. Die Rolle snc_external gibt an, dass es sich gegenüber Ihrer Organisation um einen externen Benutzer handelt. Sie sollten keinen Zugriff auf Ressourcen haben, es sei denn, dies wird ausdrücklich erlaubt durch ACLs für die Rolle snc_external oder zusätzliche Rollen, die die Rolle snc_external erben. Standardmäßig haben Benutzer mit der Rolle snc_external keinen Zugriff auf:

- Scripted REST API-Ressourcen, die nicht als extern markiert sind
- Tabellen ohne die Rolle, die die Rolle snc_external oder public erbt
- Ressourcen, die keine Datensatztypen sind, z. B. Prozessoren und UI-Seiten, ohne Zugriff auf die Rolle „snc_external“ oder eine Rolle, die die Rolle „snc_external“ erbt.
- Now Intelligence-Dashboards.

Markieren Sie die Rolle snc_internal nicht als erweitert. Andernfalls können interne Benutzer nicht auf die Instanz zugreifen.

Plugin „Explicit Roles“

Wenn das „Explicit Roles“-Plugin aktiviert ist, gilt Folgendes:

- Alle -Benutzer müssen über die Rolle snc_internal für den Zugriff auf interne Ressourcen oder die Rolle snc_external für den Zugriff auf externe Ressourcen verfügen. Benutzer ohne eine dieser expliziten Rollen können nur auf öffentliche Ressourcen zugreifen.
- Allen vorhandenen Benutzern wird automatisch die Rolle snc_internal zugewiesen. Durch diese Rolle werden die vorhandenen Zugriffsebenen und das Systemverhalten nicht geändert. Stattdessen stellt sie eine Kategorie bereit, um interne Benutzer von externen Benutzern zu unterscheiden. Alle internen Benutzer behalten dieselbe Zugriffsebene bei wie vor der Aktivierung des Plugins.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp:
Um Änderungen an vorhandenen Funktionen für Benutzer zu verhindern, wird durch die Aktivierung des Plugins „Explicit Roles“ die Benutzerrolle snc_internal allen vorhandenen Benutzern in der Instanz zugewiesen. Dies schließt alle externen Benutzer ein, die hinzugefügt wurden, bevor das Plugin „Explicit Roles“ aktiviert wurde. Nachdem das Plugin „Explicit Roles“ aktiviert wurde, gehen Sie für alle externen Benutzer, die vor Aktivierung des Plugins „Explicit Roles“ hinzugefügt wurden, wie folgt vor:

- Entfernen Sie die Rolle snc_internal.
- Fügen Sie die Rolle snc_external hinzu.

Durch die vorstehenden Maßnahmen können Sie sicherstellen, dass externe Benutzer, die vor der Aktivierung des Plugins „Explicit Roles“ hinzugefügt wurden, keinen Zugriff auf interne Ressourcen haben, die nur internen Benutzern zur Verfügung stehen sollten.

- Neu erstellten Benutzern wird automatisch die Rolle snc_internal zugewiesen, wenn sie erstmalig versuchen, sich bei der Instanz anzumelden, es sei denn, ihnen wurde explizit die Rolle snc_external zugewiesen. Sie können die Rolle snc_external einem neuen Benutzer hinzufügen, bevor er sich zum ersten Mal bei der Instanz anmeldet, um externe Benutzerrechte bereitzustellen.

Wichtig:

Aktivieren Sie dieses Plugin während eines Wartungsfensters oder wenn nur wenige Benutzer angemeldet sind. Benutzern, die derzeit bei der Aktivierung des Plugins angemeldet sind, wird die Rolle snc_internal nicht dynamisch zugewiesen. Stattdessen müssen sich Benutzer abmelden und wieder anmelden, um die Rolle snc_internal zu erhalten. Sobald das Plugin aktiviert ist, können Sie die Rollen snc_internal und snc_external jederzeit hinzufügen oder entfernen, um Benutzerrechte zu ändern.

Nach der Aktivierung des Plugins erhält der Benutzer bei jeder Anmeldung die Rolle snc_internal, sofern das Konto diese Rolle noch nicht hatte, oder die Rolle snc_external. Dies schließt per Identitätswechsel angemeldete Benutzer ein.

- Allen vorhandenen ACLs ohne Rollenanforderung wird automatisch die Rolle snc_internal zugewiesen. Da sowohl vorhandenen ACLs als auch Benutzern die Rolle „snc_internal“ zugewiesen ist, ändern sich die vorhandenen Zugriffsebenen nicht.
- Neu erstellten ACLs ohne Rollenanforderung wird automatisch die Rolle snc_internal zugewiesen. Diese Rollenzuweisung gilt nicht für neu erstellte ACLs mit zugewiesener Rolle.
- Für alle vorhandenen Prozessor-Datensätze [sys_processor] oder neu erstellte Prozessor-Datensätze [sys_processor] mit **Typ = Skript** wird die Rolle snc_internal automatisch zum Feld **Rollen** hinzugefügt, wenn das Feld leer ist.
- Um den Zugriff auf UI-Seiten auf interne Benutzer zu beschränken, weist das Plugin automatisch die Rolle snc_internal der * ACL mit dem **Typ ui_page** zu.
- Um den Zugriff auf Prozessoren auf interne Benutzer zu beschränken, weist das Plugin automatisch die Rolle snc_internal der * ACL mit dem **Typ processor** zu.
- Externe Benutzer müssen mindestens die Rolle snc_external erhalten, um auf die Instanz zuzugreifen. Diese Rolle muss externen Benutzern manuell erteilt werden. Der Zugriff auf Datensätze wird über ACLs gewährt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschieben Sie keine System-Update Sets zwischen Instanzen, unabhängig davon, ob das Plugin „Explicit Roles“ aktiviert oder deaktiviert ist. Weitere Informationen finden Sie unter System-Update Sets .

Hinweis:
Dieses Plugin erfordert auch das Plugin Contextual Security Manager.

Externen Benutzer Zugriff auf Tabellen gewähren

Sie können externen Benutzern Zugriff auf eine Tabelle gewähren, indem Sie der Tabelle eine Rolle hinzufügen, die die Rolle snc_external erbt. Weitere Informationen finden Sie unter Provide external users access to a table .

Die hasRoles()-Methode

Die Methode `hasRoles()` ist zwar noch verfügbar, wird aber im Geneva-Release abgeschafft. Verwenden Sie stattdessen die Methode `hasRole(role name)`.

Wenn Sie die Methode `hasRoles()` verwenden, beachten Sie die folgenden Änderungen:

- Diese Methode schließt die snc_internal-Standardrolle automatisch aus, wenn sie nach Rollen sucht. Dies bedeutet, dass die Methode `hasRoles()` immer noch **false** zurückgibt, wenn ein Benutzer nur über die Rolle snc_internal verfügt.
- Wenn der Benutzer die Rolle „snc_external“ hat, gibt die Methode **false** zurück, da die Instanz externe Benutzer als ohne Rolle betrachtet.

Gegenseitiger Ausschluss: snc_external und snc_internal

Die Now Platform verhindert, dass Benutzer gleichzeitig über beide Rollen snc_external und snc_internal verfügen. Die Now Platform wendet diesen gegenseitigen Ausschluss überall im System an und schreibt Fehlermeldungen für jeden Konflikt in die Protokolle.

Hinweis:
ACLs können beide Rollen haben, wenn die ACL-Ressourcen für alle Benutzer zugänglich sein sollen.

Beispiel: Einem Benutzer beide expliziten Rollen hinzufügen (direkte Kollision):

1. Weisen Sie Benutzer Abel Tuter die Rolle snc_internal zu.
2. Weisen Sie Benutzer Abel Tuter die Rolle snc_external zu.

Ergebnis: Das Hinzufügen der Rolle snc_external schlägt fehl, da Abel Tuter die Rolle snc_internal hat.

Beispiel: Einer Gruppe beide expliziten Rollen hinzufügen (direkte Kollision):

1. Stellen Sie sich eine Gruppe namens Testgruppe vor, der derzeit keine expliziten Rollen zugewiesen sind.
2. Fügen Sie Abel Tuter der Testgruppe hinzu.
3. Fügen Sie die Rolle snc_external der Testgruppe hinzu.

Ergebnis: Das Hinzufügen der Rolle snc_external schlägt fehl, da Abel Tuter die Rolle snc_internal hat und nicht beide Rollen haben kann.

Beispiel: Eine explizite Rolle einer Gruppe zuweisen, in der ein Gruppenmitglied die explizite Rolle hat, die einen Konflikt verursacht (indirekte Kollision):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Weisen Sie Benutzer Abel Tuter die Rolle snc_internal zu.
2. Stellen Sie sich eine Gruppe namens Testgruppe vor, der derzeit keine expliziten Rollen zugewiesen sind.
3. Fügen Sie Abel Tuter der Testgruppe hinzu.
4. Fügen Sie die Rolle snc_external der Testgruppe hinzu.

Ergebnis: Das Hinzufügen der Rolle snc_external zur Gruppe schlägt fehl, da Abel Tuter die Rolle snc_external durch seine Zugehörigkeit zur Gruppe erben würde. Beide expliziten Rollen würden demselben Benutzer zugewiesen, was nicht zulässig ist.

Weitere Beispiele finden Sie in der folgenden Tabelle:

Rolle	Versuchte Aktion	Ergebnis
Direkte Kollision		
Der Benutzer hat die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Der Benutzer hat die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Der Benutzer hat keine explizite Rolle.	Fügt die Rolle snc_internal oder snc_external hinzu.	Die Rolle wird hinzugefügt.
Der Benutzer hat beide explizite Rollen (vorhandene Kollision).	Fügen Sie den Benutzer einer Gruppe ohne Rollen hinzu.	Die Aktion wird abgebrochen.
Eine Rolle, die keinem Benutzer zugeordnet ist, enthält die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Eine Rolle, die keinem Benutzer zugeordnet ist, enthält die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Der Rolle enthält beide explizite Rollen (vorhandene Kollision).	Fügen Sie die Rolle einem Benutzer, einer Rolle oder einer Gruppe hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat keine Rollen.	Fügt die Rolle snc_internal oder snc_external hinzu.	Die Rolle wird hinzugefügt.
Indirekte Kollision		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Versuchte Aktion	Ergebnis
Rolleneinschluss mit Kollision	1. Gewähren Sie einem Benutzer mit der Rolle snc_internal die Testrolle. 2. Fügen Sie der Testrolle die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Rolleneinschluss ohne Kollision	1. Gewähren Sie einem Benutzer ohne Rolle die Testrolle. 2. Fügen Sie der Testrolle die Rolle snc_external hinzu.	Die Rolle wird sowohl dem Benutzer als auch der Testrolle hinzugefügt.
Gruppeneinschluss mit Kollision	1. Fügen Sie einen Benutzer mit der Rolle snc_internal der „Testgruppe 2“ (untergeordnete Gruppe von Testgruppe 1) hinzu. 2. Fügen Sie Testgruppe 2 die Rolle snc_external hinzu. 3. Fügen Sie die Rolle snc_external der übergeordneten Gruppe „Testgruppe 1“ (übergeordnete Gruppe von Testgruppe 2) hinzu.	Die Aktion wird abgebrochen.
Gruppeneinschluss ohne Kollision	1. Fügen Sie einen Benutzer ohne Rolle der Gruppe „Testgruppe 2“ (untergeordnete Gruppe von Testgruppe 1) hinzu. 2. Fügen Sie die Rolle snc_external oder snc_internal der „Testgruppe 1“ (übergeordnete Gruppe der Testgruppe 2) hinzu.	Die Rolle wird der übergeordneten Gruppe, der untergeordneten Gruppe und dem Benutzer hinzugefügt.
Gruppeneinschluss plus Rolleneinschluss mit Kollision	Fügen Sie contains_external der Testgruppe 1, der übergeordneten Gruppe von Testgruppe 2, hinzu.	Testgruppe 1 und Testgruppe 2 erhalten beide contains_external, aber sie erhalten nicht explizit die Rolle snc_external.
	Fügen Sie die Rolle snc_internal der Testgruppe 2, der untergeordneten Gruppe von Testgruppe 1, hinzu.	Die Aktion wird abgebrochen.
Änderung der übergeordneten Gruppe plus Gruppeneinschluss	1. Entfernen Sie Testgruppe 1 als übergeordnete Gruppe von Testgruppe 2. 2. Fügen Sie der Testgruppe 1 die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen. Wiederholen Sie diesen Vorgang für bereits geschachtelte Gruppen, erwarten Sie derselbe Ergebnis.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Versuchte Aktion	Ergebnis
	3. Fügen Sie Testgruppe 2 die Rolle snc_external hinzu. **4.** Legen Sie in Testgruppe 2 die Testgruppe 1 als übergeordnete Gruppe fest, und speichern Sie.	

Die Ursache einer abgebrochenen Aktion wird in der Fehlermeldung angezeigt und muss behoben werden, bevor ein erneuter Versuch erfolgreich verlaufen kann.

Für direkte Fälle, z. B. Hinzufügen einer expliziten Rolle zu einem einzelnen Benutzer, überprüfen Sie, welche explizite Rolle der Benutzer haben soll. Wenn der Benutzer über die falsche explizite Rolle verfügt, muss diese zuerst entfernt und dann die richtige explizite Rolle hinzugefügt werden.

Für indirekte Fälle, z. B. Hinzufügen einer expliziten Rolle zu einer Gruppe (sodass einem Gruppenmitglied beide expliziten Rollen zugewiesen werden), überlegen Sie, ob dieser Benutzer in der Gruppe sein soll. Bestimmen Sie auch, ob die explizite Rolle der Gruppe zugewiesen werden soll. Dies schließt auch Fälle ein, in denen die Rolle durch die Gruppenhierarchie und durch Rolleneinschluss geerbt wird.

Beachten Sie, dass die Now Platform nur die erste mögliche Kollision meldet. Wenn nach Aufhebung der Kollision erneute Versuche wieder fehlschlagen, wobei eine andere Ursache vorliegt, sollten Sie die relevanten gegenseitigen Abhängigkeiten von Benutzern/Gruppen/Rollen umfassender analysieren. Dabei sollten Sie gegebenenfalls überdenken, wie Gruppen- und Rolleneinschlüsse aufgebaut sind.

Fordern Sie explizite Rollen an

Aktivieren Sie explizite Rollen, indem Sie das Plugin „Explicit Roles“ (com.glide.explicit_roles) über den Now Support Service Catalog anfordern.

Vorbereitungen

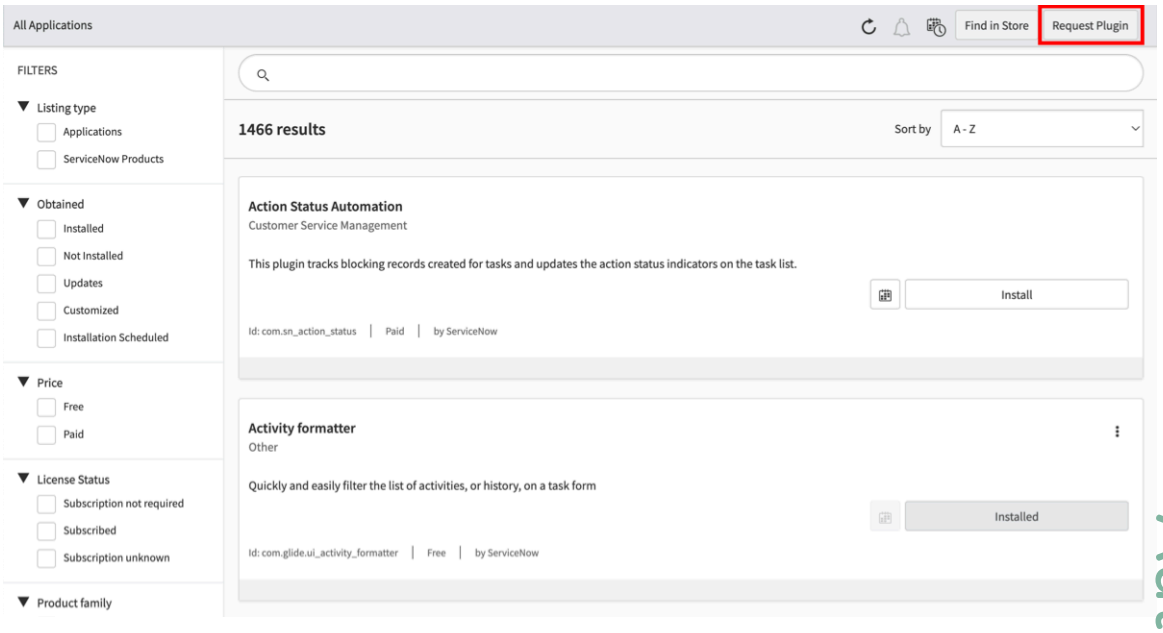
Erforderliche Rolle: admin

Wichtig:
Aktivieren Sie dieses Plugin während eines Wartungsfensters oder wenn nur wenige Benutzer angemeldet sind. Benutzern, die derzeit bei der Aktivierung des Plugins angemeldet sind, wird die Rolle snc_internal nicht dynamisch zugewiesen. Stattdessen müssen sich Benutzer abmelden und wieder anmelden, um die Rolle snc_internal zu erhalten. Sobald das Plugin aktiviert ist, können Sie die Rollen snc_internal und snc_external jederzeit hinzufügen oder entfernen, um Benutzerrechte zu ändern.

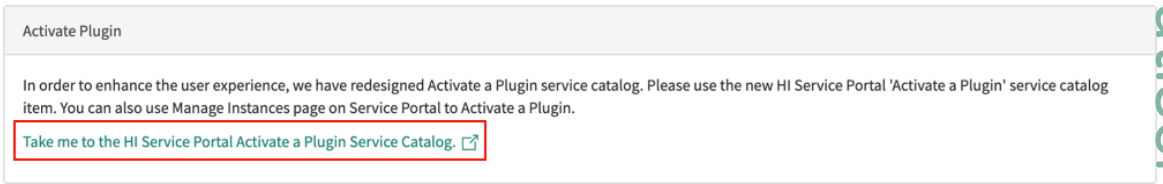
Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.

5. Wählen Sie **Aktionen > Plugin aktivieren** aus.

6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
	Datum und Uhrzeit zum Aktivieren des Plugins.

Automatische Übersetzung

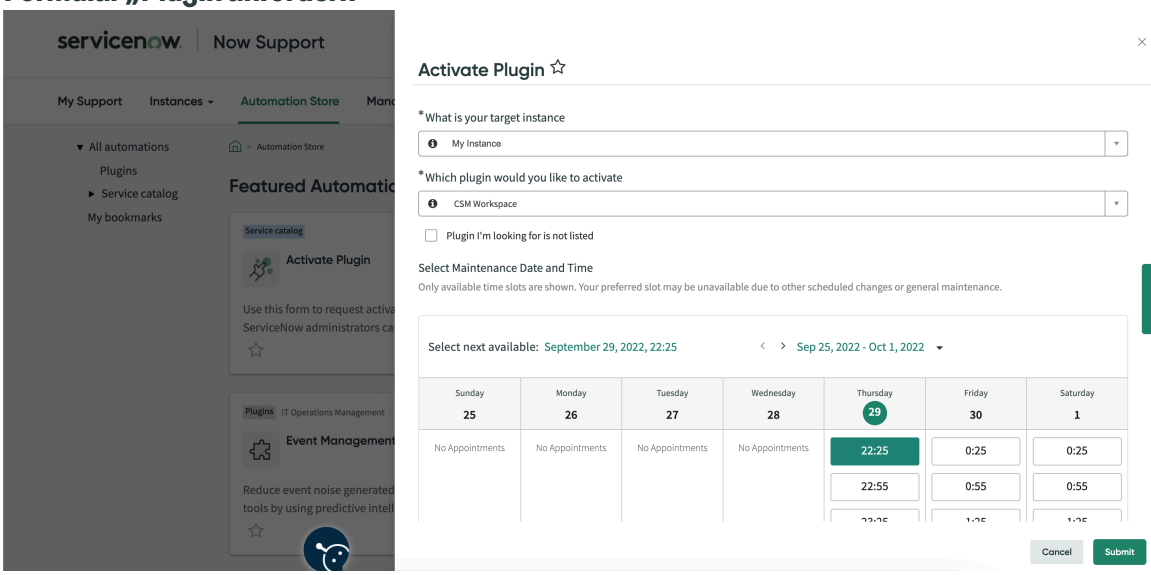
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	**Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Plugins aus dem Servicekatalog anfordern [KB0751715] im Now Support Knowledge Base.

Rollen mit erhöhten Berechtigungen

Für Rollen mit erhöhten Berechtigungen müssen Sie die Verantwortung für die Verwendung der Rolle manuell übernehmen, bevor Sie auf die Funktionen der Rolle zugreifen können.

Standardmäßig verfügen Sie bei der Anmeldung nicht über Rollen mit erhöhten Berechtigungen. Sie müssen manuell eine Erhöhung auf die Berechtigung der Rolle durchführen. Eine Rolle mit erhöhten Berechtigungen ist nur für die Dauer Ihrer Benutzersitzung gültig. Bei Sitzungszeitüberschreitung oder Abmeldung wird die Rolle entfernt.

Sie können jede Rolle als Rolle mit erhöhten Berechtigungen festlegen und diese Rolle dann einem oder mehreren Benutzern zuweisen. Führen Sie dies aus, wenn Sie verhindern möchten, dass Benutzer unmittelbar nach der Anmeldung Zugriff auf die Rechte haben, die die Rolle bietet. Sie können die Berechtigungsrolle im Formular „Rolle“ festlegen. Anweisungen finden Sie unter Rollen erstellen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine erhöhte Rolle zu verwenden, müssen Sie die folgenden Bedingungen erfüllen:

- Die erhöhte Rolle muss Ihnen zugewiesen werden.
- Sie müssen manuell eine Erhöhung auf eine bestimmte erhöhte Rolle durchführen, um deren Berechtigungen zu erhalten, auch wenn Sie bereits auf eine zweite erhöhte Rolle hochgestuft wurden, die die erste erhöhte Rolle enthält.

  Beispiel: Wenn die erhöhte Rolle A die erhöhte Rolle B enthält, müssen Sie auch nach einer Erhöhung auf Rolle A eine Erhöhung auf Rolle B durchführen, um deren Berechtigungen zu erhalten.

Die Administratorrolle

Um einem Benutzer die Administratorrolle zuzuweisen, muss der gewährende Benutzer auch über die Administratorrolle verfügen. Beispielsweise kann ein Benutzer, der nur über die Rolle „user_admin“ verfügt, anderen Benutzern die Rolle „admin“ nicht gewähren.

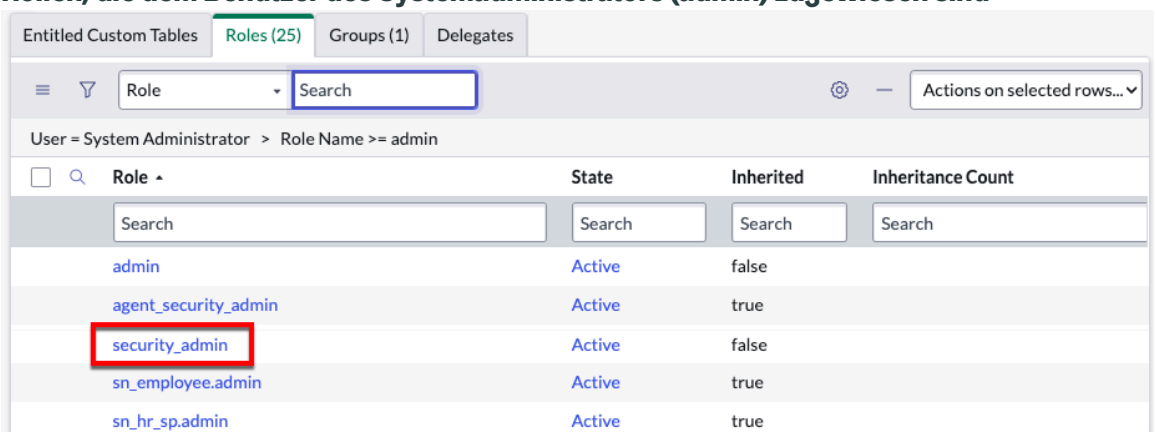
- Nicht-Administratoren können einen Benutzer nicht zu einer Gruppe hinzufügen, die die Administratorrolle enthält.
- Um einem Benutzer die Rolle „security_admin“ zuzuweisen, muss der gewährende Benutzer auch die Rolle „admin“ haben und auf die Rolle „security_admin“ hochstufen, bevor er anderen Benutzern die Rolle „security_admin“ gewährt. Ein Benutzer, der nur über die Administratorrolle verfügt, kann anderen Benutzern die Rolle security_admin nicht gewähren.
- Ein Benutzer ohne die Rolle „security_admin“ kann keinen Benutzer zu einer Gruppe hinzufügen, die die Rolle „security_admin“ enthält.

⚠ Warnung:
Die Verwendung erhöhter Berechtigungen für die Administratorrolle wird nicht unterstützt und kann zu unerwartetem Verhalten führen. Informationen dazu, wie Administratoren eine manuelle Erhöhung erfordern, finden Sie unter Erzwingen, dass Administratoren eine manuelle Erhöhung durchführen.

Die Rolle security_admin

Im Basissystem ist die Rolle security_admin die einzige Rolle mit erhöhten Berechtigungen. Diese Rolle wird automatisch dem Benutzer zugewiesen, der der Standardbenutzer des Systemadministrators (admin) ist. Bietet Zugriff auf ACLs und strenge Sicherheitseinstellungen.

Rollen, die dem Benutzer des Systemadministrators (admin) zugewiesen sind



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Um diese Rolle anzuzeigen, müssen Sie zuerst eine Erhöhung auf die Rolle security_admin durchführen. Wenn Sie nur als Systemadministrator (admin) angemeldet sind, wird der Datensatz security_admin in der Liste der Rollen nicht angezeigt.

Rolle „Security_admin".

Die Rolle „security_admin" ist eine Rolle mit erhöhten Berechtigungen, die mit „Strenge Sicherheitseinstellungen" bereitgestellt wird und es Benutzern ermöglicht, Zugriffskontrollen zu erstellen und zu ändern und „Strenge Sicherheitseinstellungen" zu ändern.

Im Basissystem verfügt nur der Standardbenutzer des Systemadministrators (admin) über die Rolle security_admin. Da die Berechtigungen erhöht werden müssen, verfügt der Administratorbenutzer bei der Anmeldung nicht über diese Rolle. Nach der Erhöhung der Berechtigungen verfügt der Administratorbenutzer für die Dauer der Benutzersitzung über die Rolle security_admin. Weitere Informationen finden Sie unter Führen Sie eine Erhöhung auf eine privilegierte Rolle durch.

Um eine hohe Sicherheit zu gewährleisten, erfordert die Rolle „security_admin" eine Erhöhung der Berechtigungen. Begrenzen Sie die Benutzer und Gruppen, denen Sie diese Rolle zuweisen.

Führen Sie eine Erhöhung auf eine privilegierte Rolle durch

Der Basissystemadministrator kann eine privilegierte Rolle annehmen, um Zugriff auf die Funktionen von Strenge Sicherheitseinstellungen zu erhalten.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis:
Wenn Sie weiteren Benutzern die Administratorrolle gewähren, können sie nicht auf eine privilegierte Rolle hochgestuft werden. Nur der Basissystemadministrator kann eine Erhöhung durchführen.

Prozedur

1. Klicken Sie im Bannerframe auf Ihr Bild oder klicken Sie auf Ihre Initialen, wenn Sie kein Bild hochgeladen haben.
2. Wählen Sie **Rollen erweitern aus**.
   Ein Dialogfeld mit verfügbaren Rollen für die Erhöhung wird angezeigt.
3. Wählen Sie die erhöhten Rollen aus, die zugewiesen werden sollen, und klicken Sie auf **OK**.
   Diese Rolle gewährt dem Benutzer für den Rest der Sitzung erweiterte Berechtigungen für alle Ressourcen, die von der Rolle gesteuert werden. Wenn sich der Benutzer abmeldet, werden die erhöhten Berechtigungen mit der Sitzung beendet, können jedoch bei der nächsten Anmeldung wiederhergestellt werden.
4. Beenden Sie die Erhöhung der Rolle, indem Sie zum Dialogfeld in Schritt 2 zurückkehren und die Auswahl der Rolle aufheben.

Erzwingen, dass Administratoren eine manuelle Erhöhung durchführen

Eine Eigenschaft ist verfügbar, um alle Benutzer mit der Administratorrolle zu zwingen, die Rolle, auf die sie hochstufen möchten, manuell auszuwählen.

Vorbereitungen

Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich als Administrator an.
2. Erhöhen Sie Ihre Rolle auf security_admin.
3. Navigieren Sie zu **sys_properties.list**.
4. Suchen Sie nach der Eigenschaft `glide.security.strict_elevate_privilege`, und wählen Sie sie aus.
5. Legen Sie das Feld Wert auf **true** fest, und klicken Sie auf **Absenden**.

Ergebnisse

Wenn sich der Benutzer anmeldet, wird ihm ein Dialogfenster angezeigt, in dem er die Rolle auswählen kann, auf die er hochstufen kann.

Security Center

ServiceNow Security Center ist eine Anwendung, die aus einer Reihe von Tools besteht, die Ihr Unternehmen dabei unterstützen sollen, die Sicherheit Ihrer ServiceNow-Bereitstellungen zu gewährleisten. Mit Security Center können Sie die Sicherheitslage verbessern und die Compliance-Stufen mit einer nahtlosen Benutzer-Experience stärken.

Security Center ist eine kostenlose Anwendung, die Systemadministratoren aus dem ServiceNow Store herunterladen können. Sie wird ab dem Vancouver-Release standardmäßig installiert.

Hinweis:
Das Instanz-Sicherheitszentrum (ISC) erreicht das Verkaufsende im September 2024. SSC ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration von Instance Security Center zu ServiceNow Security Center ..

Homepage	Sicherheitshärtung	Sicherheitsscanner
	Erfahren Sie, inwieweit Härtungskonfigurationen den Sicherheitsempfehlungen von ServiceNow entsprechen	Scannen Sie anhand einer Reihe von Sicherheitsprüfungen, um Fehlkonfigurationen und unsicheres Verhalten zu identifizieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Ihre Härtungs-Compliance-Punktzahl als Prozentsatz an, analysieren Sie die häufigsten nicht konformen Härtungseinstellungen, die korrigiert werden müssen, und sehen Sie sich die Ergebnisse Ihrer Sicherheitsscans an.		

Sicherheitsmetriken	Virenschutz	Sicherheitslernen
Überwachen Sie über 50 verschiedene Metriken, die bei der Identifizierung potenzieller Sicherheitsbedrohungen helfen.	Zeigt den Trend an, wenn Events in potenziell infizierten Dateien auftreten.	Ein zentrales Repository für Sicherheitsressourcen, das Zugriff auf Sicherheits- und Compliance-Dokumente von ServiceNow bietet.

Benutzerrollen

Um Security Center zu verwenden, benötigen Sie die Rolle „admin“ oder „security_dashboard_user“.

Erforderliche Rolle	Benutzer	Vorteile
Administrator	Sicherheitspersonal in Ihrer Organisation, das sicherheitsbezogene Informationen für eine Instanz überwacht und berechtigt ist, die Einstellungen für Sicherheitshärtung zu ändern. Sie sollten jederzeit zum Security Center zurückkehren können, um Einstellungen anzupassen und die allgemeine Sicherheitsintegrität einer Instanz zu verwalten.	Überwachen und verwalten Sie die Compliance der Instanzsicherheit kontinuierlich.
sn_vsc.security_center_viewer	Sicherheitspersonal in Ihrer Organisation, das sicherheitsbezogene Informationen für eine Instanz überwacht,	Überwachen Sie kontinuierlich die Compliance der Instanzsicherheit, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle	Benutzer	Vorteile
	aber nicht berechtigt ist, die Einstellungen für die Härtung der Sicherheit zu ändern. Beispielsweise kann ein Sicherheitsanalyst mit dieser Rolle Instanzsicherheitsinformationen anzeigen. Ein anderer Benutzer mit einer Administratorrolle muss jedoch die tatsächlichen Sicherheitseinstellungen aktualisieren.	

Erste Schritte

- Security Center ist in allen Familien-Releases ab Vancouver enthalten.
- Lesen Sie die Produktdokumentation, beginnend mit Homepage.

Homepage

Verschaffen Sie sich auf der Homepage einen schnellen Überblick über die Sicherheitslage Ihrer Instanz. Zeigen Sie Ihre Härtungs-Compliance-Punktzahl als Prozentsatz an, erkennen Sie grafische Trends Ihrer Compliance-Punktzahl, analysieren Sie die häufigsten nicht konformen Härtungseinstellungen, die korrigiert werden müssen, und sehen Sie sich die Ergebnisse Ihrer Sicherheitsscans an.

Die Compliance-Punktzahl für Härtung ist ein Prozentsatz, der angibt, wie eng Ihre Sicherheitseinstellungen mit den empfohlenen Einstellungen übereinstimmen. Die Zusammenfassung der Compliance-Punktzahl für Härtung zeigt diesen Prozentsatz und Daten im Zusammenhang mit den letzten Änderungen der Punktzahl an. Verwenden Sie das Trenddiagramm der Compliance-Punktzahl für Härtung, um zu sehen, wie sich Ihre Compliance-Punktzahl im Laufe der Zeit verändert hat.

Verbessern Sie Ihre Compliance-Bewertung, indem Sie die häufigsten nicht konformen Härtungseinstellungen verwenden. Diese Liste zeigt die 10 Sicherheitshärtungseinstellungen, die sich am negativsten auf Ihre Härtungs-Compliance-Punktzahl auswirken. Diese Transparenz hilft Ihnen, die zu korrigierenden Härtungseinstellungen zu priorisieren.

Im Abschnitt „Zusammenfassung des Sicherheitsscans“ werden Balkendiagramme angezeigt, die die Anzahl der Funde für jeden Ihrer Sicherheitsscans im Laufe der Zeit widerspiegeln.

1. Greifen Sie über die Homepage auf das Trenddiagramm der Compliance-Punktzahl für Härtung zu, oder navigieren Sie zu **Härtung** > **Punktzahltrend**.
2. Wählen Sie **Punktzahltrend überprüfen** aus, um den Zeitraum anzupassen und Punkte auf der Trendlinie zur Analyse auszuwählen.
3. Wählen Sie im Zusammenfassungsabschnitt des Sicherheitsscans eine Leiste aus, um zur Scan-Ergebnisseite für diese Scan-Suite zu navigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitshärtung

Verwenden Sie das Härtungstool des Sicherheitscenters, um Ihre Härtungs-Compliance-Punktzahl anzuzeigen, sie mit vorherigen Punktzahlen zu vergleichen und die Einstellungen zu ändern, um Ihre Compliance-Punktzahl und Sicherheitslage zu verbessern.

Die Härtungseinstellungen geben empfohlene Werte für die sicherheitsbezogenen Eigenschaften und Plugins in der Now Platform an. Das Härtungstool berechnet die Compliance-Punktzahl der Härtungseinstellung als Prozentsatz. Diese Zahl gibt an, wie konform Ihre Instanz mit den Härtungseinstellungen von Security Center ist.

Formel für die Berechnung der Compliance-Bewertung für Härtung:

- Jede Härtungseinstellung hat eine Risikopunktzahl zwischen 0 und 10.
- Die Punktzahl entspricht der Summe aller konformen Risikopunktzahlen geteilt durch die Summe aller Risikopunktzahlen.

Beispiel: Wenn die Summe aller konformen Risikopunktzahlen 25,4 beträgt und die Summe für alle Risikopunktzahlen 34,9 beträgt, lautet die Compliance-Punktzahl (25,4 /34,9) x 100, was 72,7 entspricht. Diese Dezimalzahl wird auf die nächste ganze Zahl aufgerundet und ergibt daher 73.

Vergleich der Härtungspunktzahl

Verschaffen Sie sich einen Überblick über die Integrität Ihrer Härtungseinstellungen, und verwenden Sie diese Daten, um die Sicherheitslage Ihrer Instanz zu verbessern.

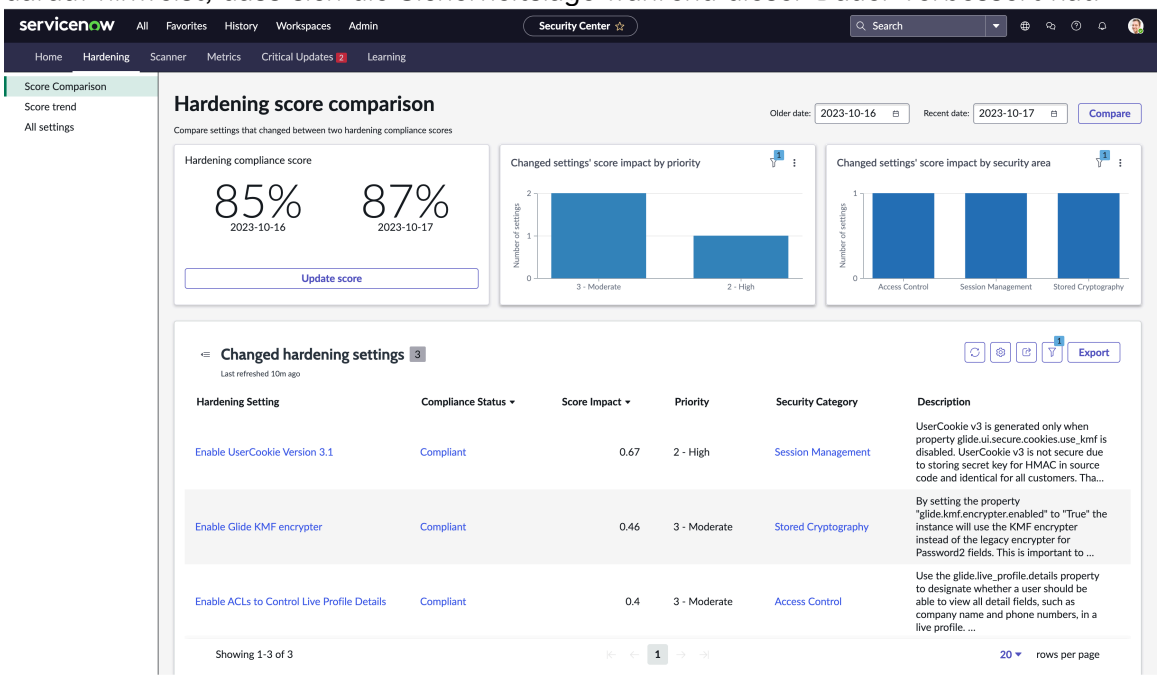
Auf der Vergleichsseite der Härtungspunktzahl werden alle Härtungseinstellungen angezeigt, bei denen sich der Compliance-Status zwischen dem ersten und zweiten Datum geändert hat, und es wird angegeben, wie sie sich auf die Härtungs-Compliance-Punktzahl ausgewirkt haben. Wenn sich beispielsweise eine Einstellung von „Konform“ in „Nicht konform“ geändert hat, wäre die Punktzahl gesunken.

Um die Ergebnisse dieser Änderungen anzuzeigen, geben Sie in der Datumsauswahl oben rechts auf der Seite ein älteres Datum und ein aktuelles Datum ein, und wählen Sie dann Vergleichen aus. Im Folgenden finden Sie eine Erklärung der einzelnen Karten:

- Compliance-Punktzahl für Härtung: Zeigt die Compliance-Punktzahl Ihrer Instanz als Prozentsatz für das erste und zweite Datum an, das Sie ausgewählt haben.
- Auswirkung auf die Punktzahl der geänderten Einstellungen nach Priorität: Zeigt die Anzahl der Härtungseinstellungen an, deren Compliance-Status zwischen den beiden Daten geändert wurde, geordnet nach Prioritätswert.
- Auswirkung der Punktzahl der geänderten Einstellungen nach Sicherheitsbereich: Zeigt die Anzahl der Härtungseinstellungen an, deren Compliance-Status zwischen den beiden Daten geändert wurde, organisiert nach Sicherheitsbereich.
- Härtungseinstellungen geändert: Zeigt die Liste der Härtungseinstellungen an, deren Compliance-Status zwischen den beiden Daten geändert wurde. Sie können Einstellungen, die nicht konform wurden und Ihre Härtungsvergleichspunktzahl verringert haben, auf Möglichkeiten überprüfen, sie konform zu machen, um Ihre Punktzahl zu erhöhen. Weitere Informationen finden Sie unter Compliance-Bewertung für Härtung erhöhen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im folgenden Screenshot ist beispielsweise die Compliance-Punktzahl gestiegen, was darauf hinweist, dass sich die Sicherheitslage während dieser Dauer verbessert hat.



Compliance-Punktzahltrend für Härtung

Zeigen Sie die Trends der Compliance-Bewertung für Härtung über einen Zeitraum in einem Diagramm oder einer Tabelle an.

Zeigen Sie Trends in Ihrer Compliance-Bewertung über einen bestimmten Zeitraum an. Verwenden Sie die Datumsauswahl, um einen Zeitraum für die Analyse auszuwählen, und gewinnen Sie dann tiefere Einblicke in die Daten, indem Sie Performance Analytics-Funktionen wie Ziele, Schwellenwerte und KPIs anwenden.

Diagrammoptionen: Wählen Sie **Diagrammoptionen** aus, um Analysen durchzuführen, Zeitreihen anzuzeigen und die Daten in verschiedenen Diagrammtypen anzuzeigen.

Analyse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ziel: Ziele, die Ihre Organisation erreichen möchte. Weitere Informationen finden Sie unter Performance Analytics targets .
- Schwellenwert: Definiert einen normalen Punktzahlbereich für einen Indikator und benachrichtigt Sie, wenn bestimmte Ereignisse auftreten. Weitere Informationen finden Sie unter Performance Analytics thresholds .
- Prognose: Beschreibt die Fähigkeit, zukünftige Punktzahlen basierend auf vergangenem Verhalten vorherzusagen. Weitere Informationen finden Sie unter Performance Analytics scores forecasts .
- Trend: Zeigt an, wie sich der Wert eines oder mehrerer Elemente im Laufe der Zeit ändert.
- Kommentare: Zeigt Anmerkungen zu einzelnen Datenpunkten an.
- Bezeichnungen: Zeigt Punktzahlen im Zusammenhang mit Visualisierungen an.
- Statistiken: Zeigt Statistiken zu Ihrer Compliance-Bewertung an.

Zeitreihen

- Punktzahl: Punktzahl für den KPI.
- Change: Änderung der Punktzahl für diesen Indikator.
- Change-Prozentsatz: Change-Prozentsatz der Punktzahlen.

Diagrammtypen: Siehe Time series visualization type use cases .

Tabelle „Alle Datensätze“.

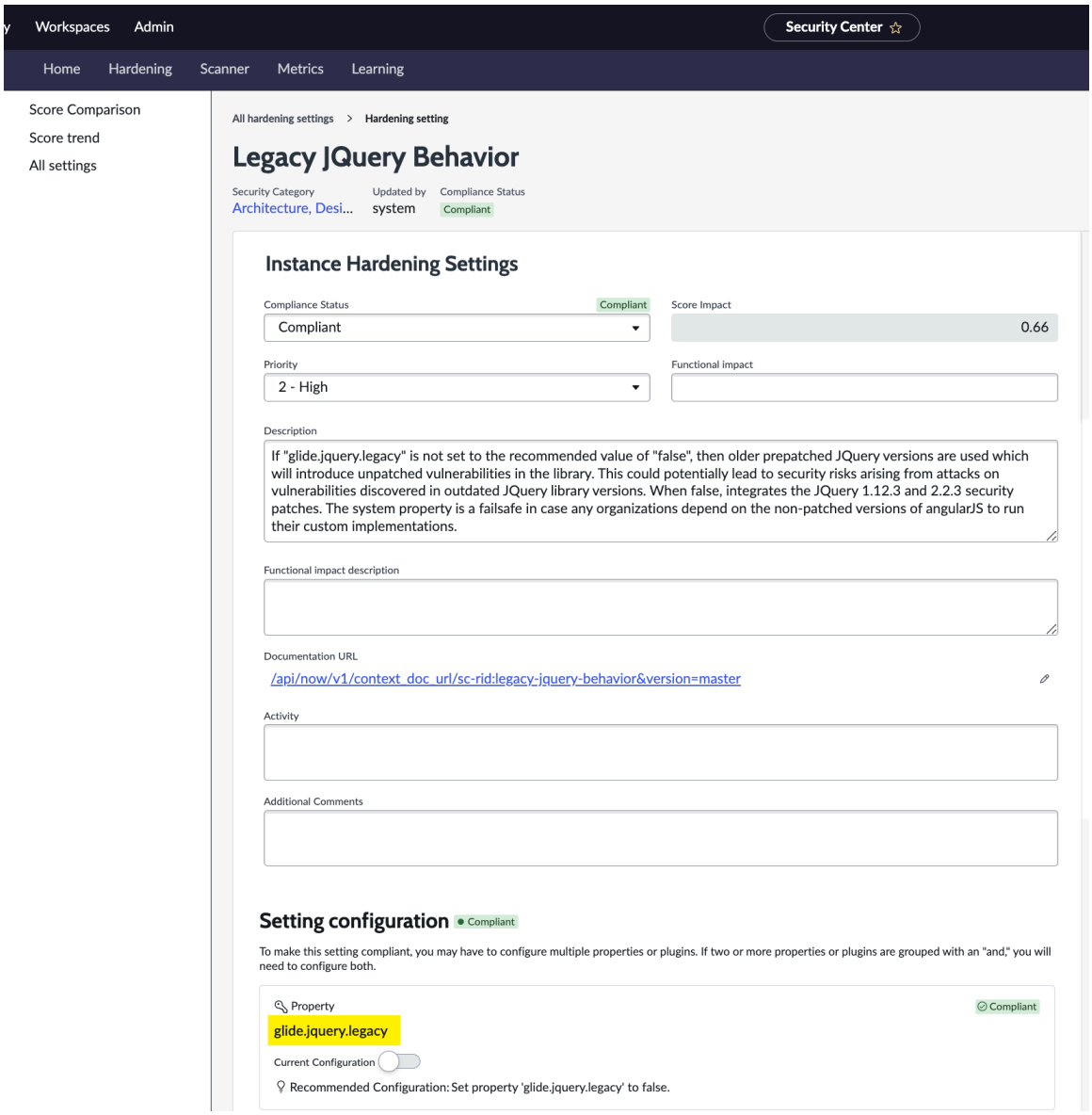
Die Tabelle „Alle Datensätze“ zeigt das Datum an, an dem die Compliance-Punktzahlen erfasst wurden, die Prozentsätze der Punktzahlen und die Anzahl der nicht konformen Einstellungen. Sie können diese Tabelle als weitere Option verwenden, um den Sicherheitsstatus Ihrer Instanz im Zeitverlauf zu analysieren.

Details zu Härtungseinstellungen

Analysieren Sie die Details einer Härtungseinstellung, indem Sie in der Security Center-App auf den entsprechenden Link klicken.

Navigieren zu **Härtung** > **Alle Einstellungen**, und wählen Sie dann eine Härtungseinstellung aus, die auf eine Seite im Härtungseinstellungstool umgeleitet werden soll, auf der die sicherheitsbezogenen Informationen angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Konfigurationsdetails der Härtungseinstellungen

Konfigurationsattribut	Beschreibung
Compliance-Status	Gibt an, ob die Härtungseinstellung konform ist oder nicht.
Auswirkung auf die Punktzahl	Ein Prozentsatz, der angibt, inwieweit sich diese Härtungseinstellung auf Ihre Sicherheitslage auswirkt.
Priorität	Eine Zahl im Bereich von 1 bis 4, wobei 1 die höchste Gewichtung hat, die angibt, wie stark sich diese Härtungseinstellung auf Ihre Sicherheitslage auswirkt.
Funktionale Auswirkung	Die Auswirkungen dieser Härtungseinstellung auf den Betrieb Ihrer Instanz.
Beschreibung	Allgemeine Übersicht über die Härtungseinstellung.
Dokumentations-URL	Link zur Dokumentation für die Härtungseinstellung.
Aktivität	Benachrichtigungen über Aktualisierungen im Zusammenhang mit der Härtungseinstellung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdetails der Härtungseinstellungen (Fortsetzung)

Konfigurationsattribut	Beschreibung
Einstellungskonfiguration	Details zum Compliance-Status Ihrer Härtungseinstellung zusammen mit Anweisungen, wie Sie sie konform machen können. **Hinweis:** Für einige Härtungseinstellungen müssen Sie möglicherweise mehrere Eigenschaften und Plugins konfigurieren, um sie konform zu machen.

Compliance-Bewertung für Härtung erhöhen

Erhöhen Sie Ihre Compliance-Punktzahl für Härtung, indem Sie sicherstellen, dass die Härtungseinstellungen den Empfehlungen des Systems entsprechen.

Vorbereitungen

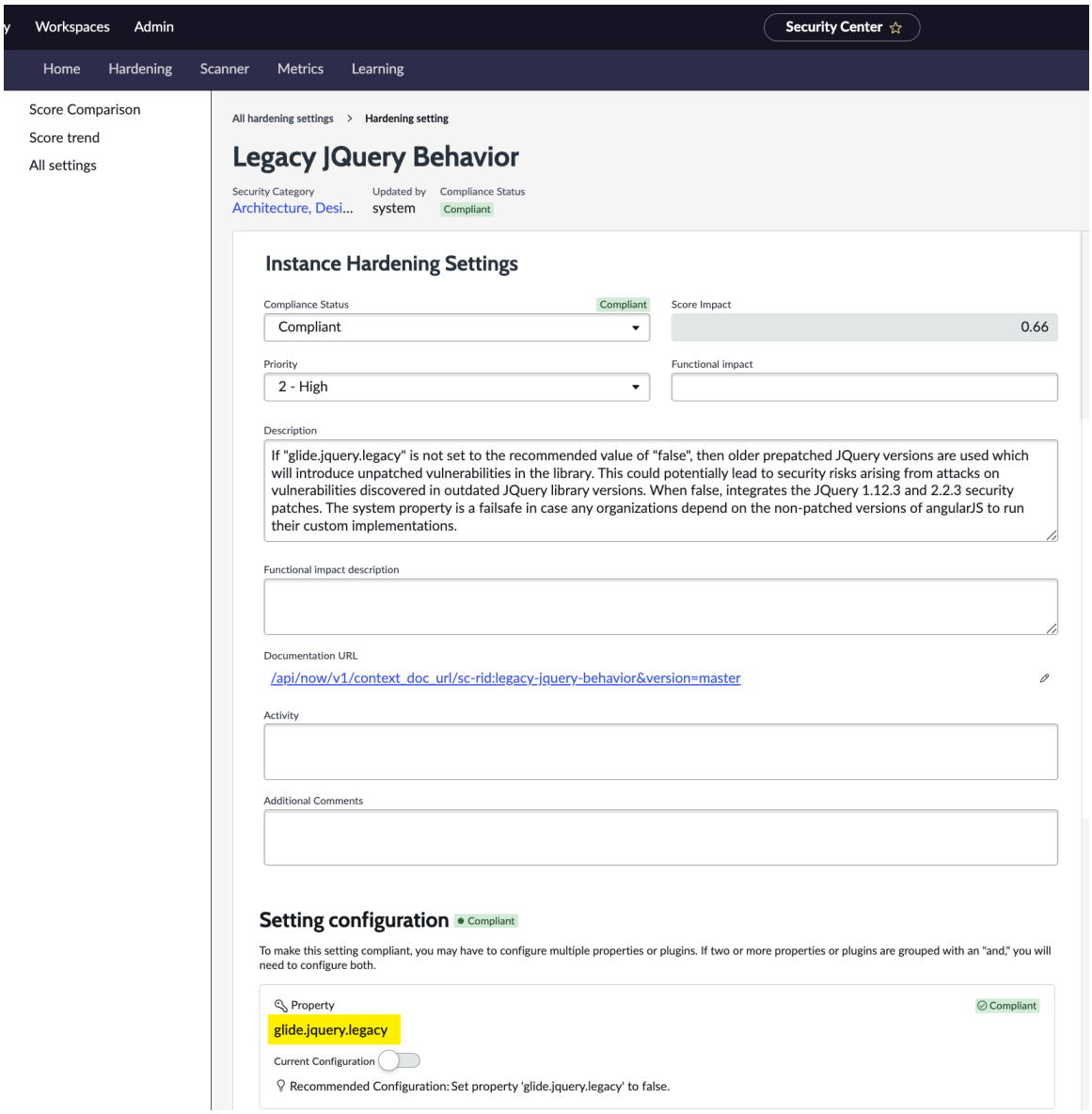
Erforderliche Rolle: admin

Identifizieren Sie nicht konforme Härtungseinstellungen mit der höchsten Auswirkung auf Ihre Instanz. Überprüfen Sie sie, um festzustellen, ob Sie die Systemempfehlungen einhalten können, damit Sie Ihre allgemeine Compliance-Punktzahl erhöhen können.

Prozedur

1. Navigieren zu **Härtung** > **Alle Einstellungen**.
2. Spalte „Compliance-Status filtern“, um nur nicht konforme Härtungseinstellungen anzuzeigen.
3. Wählen Sie **Punktzahlauswirkung** aus, um vom größten zum kleinsten zu sortieren.
4. Wählen Sie Einstellungen aus, und überprüfen Sie die Einstellungsdetails, um zu entscheiden, ob Sie den Empfehlungen entsprechen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Machen Sie die Härtungseinstellung konform.
6. Wenn Sie eine nicht konforme Härtungspunktzahl aktualisieren, um sie konform zu machen, rufen Sie die Homepage auf und wählen **Punktzahl** aktualisieren, um die aktuelle Punktzahl anzuzeigen.
   Die Härtungspunktzahl wird aufgerundet. Eine Punktzahl von 86,75 % wird auf 87 aufgerundet.

Alle Einstellungen

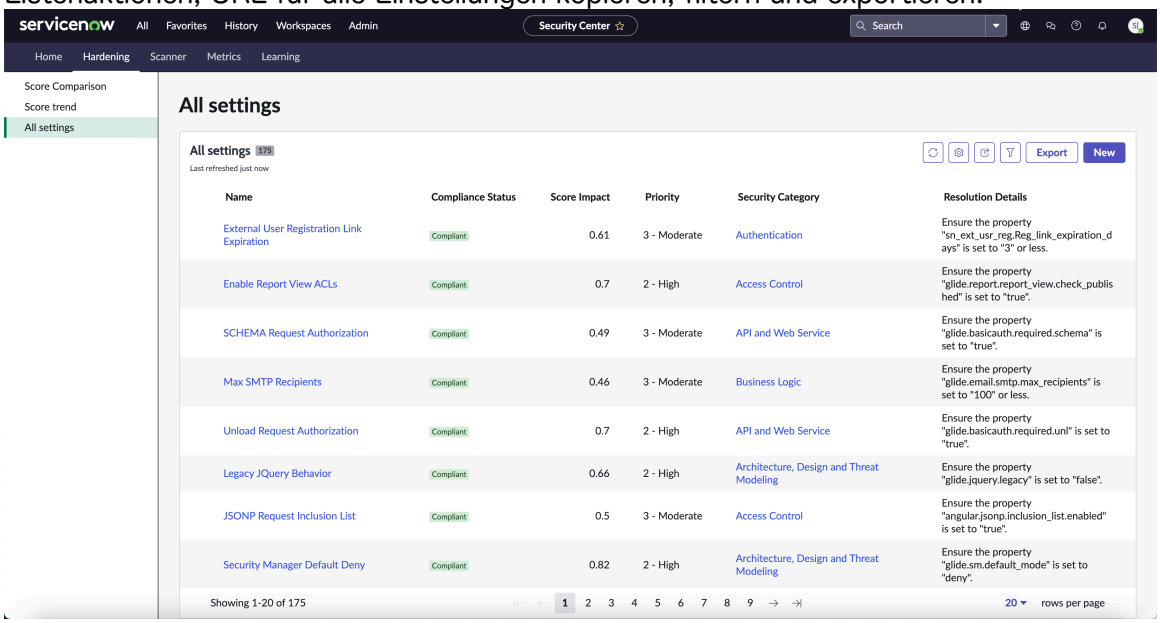
Zeigen Sie alle in Ihrer Instanz verfügbaren Härtungseinstellungen auf einer einzigen Seite an.

Eine Tabelle, die alle in Ihrer Instanz verfügbaren Härtungseinstellungen anzeigt. Sie können die allgemeinen Vorgänge für eine Tabelle anwenden, indem Sie rechts oben in der Tabelle auf Symbole klicken: Liste aktualisieren,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listenaktionen, URL für alle Einstellungen kopieren, filtern und exportieren.



- **Name**: Der Name der Eigenschaft Härtungseinstellung.
- **Compliance-Status**: **„Konform“** gibt an, dass die Härtungseinstellung ordnungsgemäß konfiguriert ist. **Nicht konform** gibt an, dass die Härtungseinstellung für Eigenschaften nicht gemäß der Systemempfehlung konfiguriert ist.
- **Punktzahlauswirkung**: Ein Prozentwert der Auswirkung dieser Härtungseinstellung auf Ihre Sicherheitslage. Die Summe aller Punktzahlauswirkungen ergibt 100 %.
- **Priorität**: Ein Wert, der die Relevanz der Einstellung darstellt: „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“. Die Beziehung zwischen Punktzahlauswirkung und Priorität besteht darin, dass eine höhere Punktzahlauswirkung eine höhere Relevanz anzeigt.
- **Sicherheitskategorie**: Die Sicherheitskategorie der Eigenschaft.
- **Auflösungsdetails**: Schritte, die Sie ausführen sollten, um die Sicherheitsschwachstelle der Härtungseinstellung zu beheben.

Informationen zum Konfigurieren einer Eigenschaftshärtung finden Sie unter Compliance-Bewertung für Härtung erhöhen.

Baseline der Härtungseinstellungen

Erkunden Sie, wie unterschiedliche Baselineversionen für Härtungseinstellungen mit verschiedenen Familien- und Store-Releases übereinstimmen.

Security Center funktioniert, indem eine Teilmenge von Systemeigenschaften aus einer Instanz erfasst und ihre Konfigurationsdetails zusammen mit den Sicherheitsauswirkungen der Nichteinhaltung innerhalb der App angezeigt werden. Die Baseline dient als Referenzpunkt für die Systemeigenschaften, die mit jedem Release der Security Center-App erfasst werden.

Übersicht über die Baseline der Härtungseinstellungen

Security Center-Version	Baselineversion der Härtungseinstellung	Unterstützte Familien	Store-Releasedatum	Wird standardmäßig mit installiert
SSC v1.1	Baseline v1.0	Utah, Vancouver	Mai 2023	Familie Vancouver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über die Baseline der Härtungseinstellungen (Fortsetzung)

Security Center-Version	Baselineversion der Härtungseinstellung	Unterstützte Familien	Store-Releasedatum	Wird standardmäßig mit installiert
SSC v1.2	Baseline v1.0	Utah, Vancouver	August 2023	Nur speichern
SSC v1.3	Baseline v2.0	Vancouver, Washington	November 2023	Familie Washington
SSC v1.4	Baseline v4.0	Washington, Xanadu	Mai 2024	Xanadu

Sicherheitsscanner

Verwenden Sie das Scanner-Tool, um Ihre Instanz anhand einer Reihe von Sicherheitsprüfungen zu scannen, um Fehlkonfigurationen zu identifizieren. Das Tool vereinfacht den Prozess der Erstellung verschiedener Prüfsuites für verschiedene Anwendungsfälle, sodass Sie die Ergebnisse im Laufe der Zeit analysieren können.

Das Sicherheitsscannen ist eine Methode, um Ihre Instanz auf Konfigurationen zu untersuchen, die auf Sicherheitsintegritätsprobleme hinweisen. Auf diese Weise können Sie Möglichkeiten zur Implementierung von Sicherheitsempfehlungen für Ihre Organisation identifizieren.

Beim Zugriff auf das Scanner-Tool ist kein Vergleich verfügbar, bis Sie die zu vergleichende Suite mit mindestens zwei Scan-Ergebnissen der Suite auswählen. Sie können die Standard-Suite und -Prüfungen verwenden oder eigene benutzerdefinierte Prüfungen und Suiten erstellen.

Vergleich der Härtungspunktzahl

Verschaffen Sie sich einen Überblick über die Integrität Ihrer Härtungseinstellungen, und verwenden Sie diese Daten, um Sicherheitsbedrohungen zu beheben und die Sicherheitslage Ihrer Instanz zu verbessern.

Auf der Vergleichsseite der Härtungspunktzahl werden die Sicherheitsänderungen in Ihren Härtungseinstellungen zwischen dem ersten und zweiten Datum angezeigt. Um Visualisierungen dieser Änderungen anzuzeigen, geben Sie in der **Datumsauswahl** oben rechts auf der Seite ein **älteres Datum** und ein aktuelles Datum ein, und klicken Sie dann auf **Vergleichen**. Nachfolgend finden Sie eine Erklärung der einzelnen Karten:

- **Compliance-Punktzahl für Härtung**: Zeigt die Compliance-Punktzahl Ihrer Instanz als Prozentsatz am ersten und zweiten Datum an.
- **Auswirkung auf die Punktzahl der geänderten Einstellungen nach Priorität**: Zeigt die Anzahl der Einstellungen an, deren Prioritäten geändert wurden.
- **Auswirkung der Punktzahl geänderter Einstellungen nach Sicherheitsbereich**: Zeigt die Anzahl der Einstellungen an, deren Kategorien geändert wurden. Beispiel: Wechsel von **Zugriffskontrolle** zu **Datenschutz**.
- **Geänderte Härtungseinstellungen**: Zeigt eine konsolidierte Ansicht der Einstellungen an, die zusammen mit ihren zugehörigen Sicherheitsdaten in der Liste geändert wurden. Darüber hinaus kann allgemeine Funktionen anwenden, die mit Listen verknüpft sind, z. B. Aktualisieren, Listen-UI-Aktionen, URL kopieren, Filter und Export.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im folgenden Screenshot hat sich die Compliance-Punktzahl beispielsweise von 71 % in 73 % geändert, was darauf hinweist, dass die Sicherheitslage in diesem Zeitraum verbessert wurde.

Die Anzahl der Einstellungen, deren Priorität geändert wurde, beträgt insgesamt vier: zwei hoch und zwei mittel. Darüber hinaus beträgt die Anzahl der Einstellungen, die die Sicherheit geändert haben, insgesamt vier: zwei Zugriffskontrolle, eine Authentifizierung und eine Geschäftslogik. Die Sicherheitsdetails dieser vier Einstellungen werden auch in der Liste Härtungseinstellungen geändert angezeigt. Sie können die nicht konformen Einstellungen anzeigen und korrigieren, wodurch die Compliance-Bewertung für Härtung neu berechnet wird.

Scanprüfungen

Prüfungen sind Regeln, die Konfigurationen oder Aktivitäten angeben, die nicht den Sicherheitspraktiken entsprechen. Prüfungen können für Tabellen, Datensätze oder Metadaten ausgeführt werden.

Folgende Arten von Prüfungen können erstellt werden:

- Tabellenüberprüfung
- Überprüfung des Spaltentyps
- Nur Skriptüberprüfung
- Linter-Überprüfung

Weitere Informationen zu -Prüfungen finden Sie unter Getting started with checks .

Wenn Sie bereit sind, eine Prüfung zu erstellen, klicken Sie auf **Neu**.

Erstellen Sie eine neue Suite

Erstellen und planen Sie eine benutzerdefinierte Suite, damit Sie die Sicherheit Ihrer Instanz für Ihre Organisation analysieren können.

Vorbereitungen

Erforderliche Rolle: admin

Eine Suite ist eine Sammlung von Prüfungen, die für einen Scan verwendet werden können. Zeigen Sie eine Liste der in Ihrer Instanz verfügbaren Scan-Suites an, die in einer Tabelle organisiert sind, indem Sie zu navigieren **Scanner** > **Suites**. Sie haben die Möglichkeit, eigene Suiten zu erstellen oder die Standardsuite Auditor zu verwenden: Dies ist eine vordefinierte Standardsuite, die Prüfungen für bewährte Sicherheitspraktiken enthält. Diese Prüfungen bestehen aus Systemeigenschaften, Plugins und Tabellen, die sich auf die Sicherheitslage Ihrer Instanz auswirken können. Die folgenden Schritte zeigen, wie Sie eine Suite erstellen, zusammen mit den verschiedenen Optionen, die für ihre Konfiguration verfügbar sind.

Prozedur

1. Navigieren zu **Suites** > **Neu**.
2. Geben Sie einen **Namen** und eine **Beschreibung**für die Suite ein, und wählen **Sie Speichern**aus.
3. **Prüfungen**
   Hier fügen Sie Ihrer Suite Prüfungen hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie **Bearbeiten** aus.

b. Wählen Sie die Prüfungen aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um sie in Ihrer Suite zu platzieren.

c. Speichern.

4. **Untergeordnete Suites**
   Hier fügen Sie untergeordnete Suiten oder Suiten hinzu, die unter den übergeordneten Suiten platziert sind.

   a. Wählen Sie **Bearbeiten** aus.

   b. Wählen Sie die untergeordneten Suiten aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um sie in Ihrer untergeordneten Suite zu platzieren.

   c. Speichern.

5. **Übergeordnete Suites**
   Hier fügen Sie übergeordnete Suiten hinzu. Alle untergeordneten Suiten werden ausgeführt, wenn eine übergeordnete Suite in einem Scan verwendet wird.

   a. Wählen Sie **Bearbeiten** aus.

   b. Wählen Sie die untergeordneten Suiten aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um sie in Ihrer übergeordneten Suite zu platzieren.

   c. Speichern.

6. **Zeitplan**
   Legen Sie einen Zeitpunkt für die Ausführung Ihrer Suite fest.

   a. Wählen Sie **Neu**.

   b. Geben Sie die Details des geplanten Scans ein.
   Die Zeitfelder haben das folgende Format: Stunde:Minuten:Sekunden.

   c. Speichern.

Scanfunde

Ein Ergebnis ist ein Verweis auf einen Datensatz, der gegen eine Regel einer Prüfung in der Instanz verstoßen hat. Sie können den Quelldatensatz und die Anzahl der durch den Datensatz ausgelösten Regeln einer bestimmten Prüfung ermitteln.

Navigieren Sie zu **Ergebnisse**, um eine Liste der Scan-Ergebnisse in Ihrer Instanz anzuzeigen. Wählen Sie einen Link unter der Spalte **Erstellt** aus, um Detailinformationen zu einem Ergebnis anzuzeigen:

- **Prüfung**: Liste der Prüfungen, die dem Scan zugeordnet sind.
- **Kategorie**: Die dem Scan zugeordnete Sicherheitskategorie. Zum Beispiel Zugriffskontrolle oder schädlicher Code.
- Anzahl: Die Häufigkeit, mit der der Datensatz gegen**Prüfregeln**verstoßen hat.
- **Priorität**: Der Schweregrad des Sicherheitsrisikos: 1 ist die höchste Priorität, während 4 die niedrigste Priorität ist.
- **Ergebnis**: Status und Typ des Scans.
- **Prüfungsversion**: Die Change-Version der Prüfung.
- **Quelltabelle**: Der Datensatz, der gegen eine Regel der Prüfung verstoßen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Stummschaltgrund**: Der Grund für das Stummschalten des Ergebnisses.
- **Quelle**: Das Datum, an dem das Ergebnis erstellt wurde.
- **Aufgabe**: Wird verwendet, um Aufgabenzuweisungen aus der Suche nach einem Datensatz zu erleichtern.
- **Domäne**: Definiert, auf was Sie zugreifen können und auf was nicht.
- **Kurzbeschreibung**: Eine kurze Erklärung des Scans.
- **Auflösungsdetails**: Anweisungen zur Lösung der Scan-Probleme.

Sicherheitsmetriken

Verwenden Sie das Metrics-Tool, um über 50 verschiedene Sicherheitsmetriken zu überwachen, um potenzielle Sicherheitsbedrohungen oder unsicheres Verhalten zu identifizieren. Sie können Schwellenwerte für E-Mail-Benachrichtigungen festlegen, die Daten auf verschiedene Arten visualisieren und analysieren, die Daten exportieren oder Dashboards mit den Metriken erstellen, die für Ihre Organisation am wichtigsten sind.

Metriken werden als Analytics Hub-Visualisierungen implementiert, die eine Vielzahl von Funktionen ermöglichen, darunter das Senden von E-Mail-Warnungen bei Überschreitung von Schwellenwerten, die Visualisierung von Zielen sowie das Anzeigen und Filtern von zugrunde liegenden Events.

Dashboard mit eigenen Security-Metriken

Zeigen Sie die Sicherheitsmetriken in Ihrer Instanz über ein einziges Dashboard an.

Um zur Seite „Metriken“ zu navigieren, wählen Sie **Meine Metriken**aus. Auf dieser Seite wird das Standard-Dashboard angezeigt. Sie haben jedoch auch die Möglichkeit, ein eigenes Dashboard zu erstellen, indem Sie **Bearbeiten**wählen.

Sie können Ihr eigenes Dashboard anpassen, indem Sie Visualisierungen, Filter, Überschriften, Bilder, Rich-Text und Listen hinzufügen. Weitere Informationen zu den verschiedenen Möglichkeiten, wie Sie Ihr Dashboard anpassen können, finden Sie unter Platform Analytics dashboards .

Alle Sicherheitsmetriken

Navigieren Sie zu **Alle Sicherheitsmetriken**, um eine Tabelle mit den Daten anzuzeigen, die sich auf die Sicherheitsmetriken Ihrer Instanz beziehen.

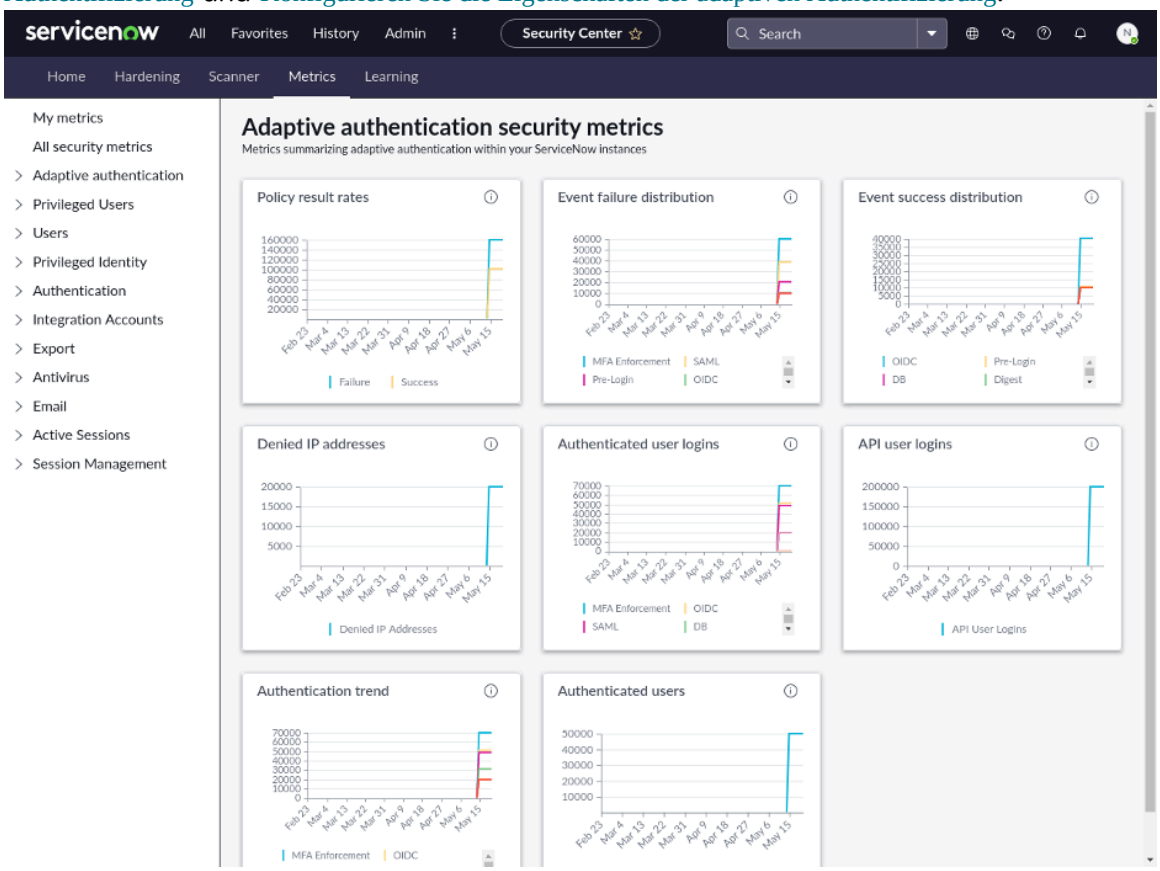
Sicherheitsmetriken der adaptiven Authentifizierung

Verwenden Sie Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten und den Zugriff auf Ihre Instanz basierend auf den angegebenen Richtlinienbedingungen zu verweigern oder zuzulassen.

Mit Metriken der adaptiven Authentifizierung können Sie überwachen, wie die adaptive Authentifizierung in Ihrer Instanz verwendet wird. Sie haben die Möglichkeit, eine Zusammenfassung aller Ihrer Metriken zur adaptiven Authentifizierung anzuzeigen, oder Sie können Detailinformationen anzeigen und einzelne Metriken anzeigen, z. B. Richtlinienergebnisraten oder abgelehnte IP-Adressen. Für diese Seite muss das Plugin „Adaptive Authentifizierung“ (`com.snc.adaptive_authentication`) für die adaptive Authentifizierung in Ihrer Instanz verfügbar sein. Sie müssen auch die Authentifizierungsrichtlinie aktivieren, um die Metriken anzuzeigen. Weitere Informationen finden Sie unter Aktivieren Sie die adaptive

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierung und Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.



Hinweis:
Diese Funktion wurde mit Version 1.2 veröffentlicht.

- Richtlinienergebnisraten: Alle erfolgreichen und fehlgeschlagenen Ereignisse der adaptiven Authentifizierung.
- Event-Fehlerverteilung: Alle fehlgeschlagenen Events für jeden Event-Typ.
- Event-Erfolgsverteilung: Die erfolgreichen Events, die jedem Event-Typ zugeordnet sind.
- Abgelehnte IP-Adressen: Die Anzahl der von der Instanz blockierten IP-Adressen zusammen mit den zugehörigen Daten.
- Authentifizierte Benutzeranmeldungen: Die Anzahl der Events, die für jeden Event-Typ gezählt werden, mit Ausnahme des Events vor der Anmeldung.
- API-Benutzeranmeldungen: Die Anzahl der Events, die API-Authentifizierungsrichtlinien für jeden Event-Typ zugeordnet sind.
- Authentifizierungstrend: Die Gesamtzahl der aufgezeichneten Events.
- Authentifizierte Benutzer: Die Anzahl der Benutzer, die für jeden Ereignistyp gezählt werden, mit Ausnahme des Ereignisses vor der Anmeldung.

Privilegierte Benutzer

Zeigen Sie die Trendlinie für die privilegierten Benutzer (aktiv und inaktiv) und ihre Aktivität im Now Platformanzeigen.

Im Übersichtsbereich für privilegierte Benutzer wird die Trendlinie für die privilegierten Benutzer (aktiv und inaktiv) und ihre Aktivität auf dem Now Platformangezeigt. Privilegierte Benutzer sind Benutzer, denen von Administratoren zusätzliche Rollen für den Zugriff auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen zugewiesen wurden, z. B. „Strenge Sicherheitseinstellungen“, „Import“ und „Portalbenutzer“.

Nachfolgend finden Sie eine Erklärung der privilegierten Benutzer:

- Benutzer gesamt: Gesamtanzahl der Benutzer in Ihrer Instanz.
- Aktive Benutzer: Gesamtzahl der Benutzer, die Sitzungen in Ihrer Instanz initiiert haben.
- Inaktive Benutzer: Benutzer, die sich kürzlich nicht bei Ihrer Instanz angemeldet haben.
- Inaktive Benutzer, die nicht ausgesperrt sind: Benutzer, die sich nicht zuletzt angemeldet haben, aber dennoch Zugriff auf ihren Account haben.
- Ausgesperrte Benutzer: Benutzer, die sich nicht bei ihrem Konto authentifizieren dürfen.
- Neue Benutzer: Benutzer, die Ihrer Instanz kürzlich hinzugefügt wurden.
- Erfolgreiche Anmeldungen: Benutzer, die sich erfolgreich angemeldet haben.
- Fehlgeschlagene Anmeldungen: Nicht erfolgreiche Anmeldeversuche.
- Lokale Anmeldungen, die nicht durch MFA geschützt sind: Benutzer, die sich ohne MFA angemeldet haben.
- Anwender, die sich nie angemeldet haben: Benutzer, die sich noch nie bei Ihrer Instanz angemeldet haben.
- Anwender, die sich seit dem letzten Monat nicht angemeldet haben: Anwender, die sich in den letzten 30 Tagen nicht angemeldet haben.
- Benutzer, die sich in den letzten 6 Monaten nicht angemeldet haben: Benutzer, die sich in den letzten 6 Monaten nicht angemeldet haben.
- Benutzer, die sich im letzten Jahr nicht angemeldet haben: Benutzer, die sich im letzten Jahr nicht angemeldet haben.
- Passwort zurücksetzen erforderlich: Benutzer, die ihr Passwort zurücksetzen müssen.
- Passwortzurücksetzungsfehler der Benutzer: Anzahl der Passwortfehler pro Benutzer.

Benutzer

Zeigen Sie die Trendlinie für die Gesamtzahl der Benutzer (aktiv und inaktiv) und ihre Aktivität im Now Platformanan.

Im Abschnitt „Benutzerübersicht“ wird die Trendlinie für die Gesamtzahl der Benutzer (aktiv und inaktiv) und ihre Aktivität im Now Platformangezeigt.

Nachfolgend finden Sie eine Erklärung des Benutzertyps:

- Benutzer gesamt: Gesamtanzahl der Benutzer in Ihrer Instanz.
- Aktive Benutzer: Gesamtzahl der Benutzer, die Sitzungen in Ihrer Instanz initiiert haben.
- Inaktive Benutzer: Benutzer, die sich kürzlich nicht bei Ihrer Instanz angemeldet haben.
- Inaktive Benutzer, die nicht ausgesperrt sind: Benutzer, die sich nicht zuletzt angemeldet haben, aber dennoch Zugriff auf ihren Account haben.
- Neue Benutzer: Benutzer, die Ihrer Instanz kürzlich hinzugefügt wurden.
- Erfolgreiche Anmeldungen: Benutzer, die sich erfolgreich angemeldet haben.
- Fehlgeschlagene Anmeldungen: Nicht erfolgreiche Anmeldeversuche.
- Externe Anmeldungen: Authentifizierungen, bei denen eine Drittpartei verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Lokale Anmeldungen, die nicht durch MFA geschützt sind: Anmeldungen, die keine MFA verwenden.
- Anwender, die sich seit dem letzten Monat nicht angemeldet haben: Anwender, die sich in den letzten 30 Tagen nicht angemeldet haben.
- Benutzer, die sich in den letzten 6 Monaten nicht angemeldet haben: Benutzer, die sich in den letzten 6 Monaten nicht angemeldet haben.
- Benutzer, die sich im letzten Jahr nicht angemeldet haben: Benutzer, die sich im letzten Jahr nicht angemeldet haben.
- Passwort zurücksetzen erforderlich: Benutzer, die ihr Passwort zurücksetzen müssen.
- Passwortzurücksetzungsfehler der Benutzer: Anzahl der Passwortfehler pro Benutzer.

Privilegierte Identität

Analysieren von Daten im Zusammenhang mit Metriken für Benutzer mit privilegierter Identität.

Dieses Dashboard zeigt Daten zu privilegierten Identitätsbenutzern und deren Aktivität in Ihrer Instanz an.

- Administratoranmeldungen: Gesamtanzahl der Anmeldungen mit Benutzern der Administratorrolle.
- Identitätswechsel: Gesamtanzahl der Identitätswechsel, die von Benutzern mit der Rolle „Identitätswechsler“ durchgeführt wurden.
- Erhöhung: Gesamtanzahl der Sicherheitserhöhungen, die von Benutzern mit der Rolle „security_admin“ durchgeführt wurden.
- ServiceNow-Anmeldungen: Gesamtanzahl der Anmeldungen von ServiceNow-Mitarbeitern.
- Hinzugefügte Admin-Benutzer: Gesamtzahl der Benutzer mit der Administratorrolle.

Authentifizierungsmetriken

Zeigen Sie Metriken im Zusammenhang mit der Authentifizierung in Ihrer Instanz über ein Dashboard an.

Zeigt Daten für Metriken an, die sich auf Authentifizierungsschemas beziehen, z. B. MFA-Nutzung, Webservicekonten und Nutzung biometrischer Scanner.

- Für MFA registrierte Benutzer: Gesamtanzahl der für die Verwendung von MFA registrierten Benutzer.
- Benutzer mit MFA-Umgehung: Gesamtanzahl der Benutzer, die die Multifaktor-Authentifizierung umgehen.
- Nicht-MFA-Benutzer mit hohen Berechtigungen: Gesamtanzahl der Benutzer mit hohen Berechtigungen, die keine MFA verwenden.
- Aktive MFA-Benutzer: Gesamtanzahl der MFA-Benutzer, die in Ihrer Instanz aktiv sind.
- Ausgesperrte MFA-Benutzer: Gesamtanzahl der MFA-Benutzer, die in Ihrer Instanz ausgesperrt sind.
- Webservice-Account-Benutzer: Gesamtanzahl der Benutzer, die nur über einen Webservice-Account verfügen.
- Ablaufende X509-Zertifikate: Gesamtanzahl der X509-Zertifikate, die in den nächsten 30 Tagen ablaufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrations-Accounts

Zeigen Sie die Trends zu den Integrationskonten an, die im Now Platformerstellt wurden.

Das Dashboard für Integrationskonten zeigt Trends zu den Integrationskonten an, die im Now Platformerstellt wurden.

Nachfolgend finden Sie Erklärungen zu den Metriken der Integrationskonten:

- Integrationsaccounts insgesamt: Trends im Zusammenhang mit Integrationsaccounts in Ihrer Instanz.
- Aktive Integrationskonten: Trends im Zusammenhang mit aktiven Integrationskonten in Ihrer Instanz.
- Inaktive Integrationskonten: Trends für die Gesamtanzahl der Integrationskonten, die in Ihrer Instanz inaktiv sind.

Exportieren

Erkennen Sie die Daten, die häufig exportiert werden, und welche Benutzer den Export durchführen.

- Exporte gesamt: Gesamtanzahl der vom Benutzer exportierten Tabellendatensätze.
- Klassifizierte Exporte: Gesamtanzahl der exportierten Tabellendatensätze, zusammengefasst nach der ihnen zugewiesenen Datenklassifizierung.

Virenschutz

Zeigt den Trend an, wenn Events in potenziell infizierten Dateien auftreten. Sehen Sie, wann sie erkannt, unter Quarantäne gestellt, wiederhergestellt oder gelöscht werden.

- Dateien in Quarantäne: Die Anzahl der Dateien, die potenziell Malware enthalten.
- Heruntergeladene Dateien: Die Anzahl der heruntergeladenen Dateien.
- Wiederhergestellte Dateien: Die Anzahl der wiederhergestellten Dateien.
- Gelöschte Dateien: Die Anzahl der gelöschten Dateien.

E-Mail

Zeigt Daten im Zusammenhang mit Spam-E-Mails an, die extern empfangen werden.

Spam-E-Mails stellen die Anzahl der pro Tag empfangenen Junk-Mails dar.

Aktive Sitzungen

Zeigen Sie die Trendlinie der aktiven Benutzer im Now Platformanan.

Die Trendlinie kann für die folgenden Metriken angezeigt werden:

- Benutzersitzungen: Metriken im Zusammenhang mit aktiven Benutzersitzungen in Ihrer Instanz.
- Privilegierte Benutzersitzungen: Metriken im Zusammenhang mit privilegierten Benutzern oder Benutzern, denen zusätzliche Rollen zugewiesen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sitzungsverwaltung

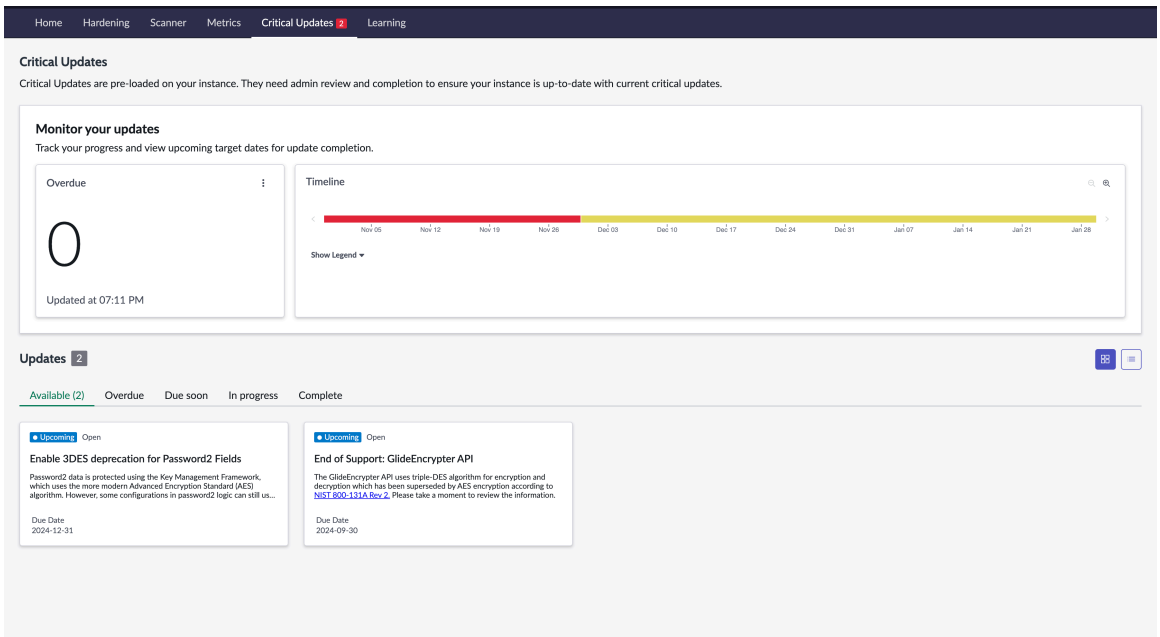
Zeigen Sie Metriken im Zusammenhang mit Benutzersitzungen und die Häufigkeit der Sperrungen der Sitzungen an.

Kritische Updates

Erhöhen Sie die Sicherheitslage Ihrer Instanz, indem Sie sicherstellen, dass die vom System empfohlenen kritischen Updates rechtzeitig implementiert werden.

„Kritische Updates“ ist ein Tool, das Administratoren bei der Implementierung wichtiger Sicherheitsupdates basierend auf ihrer Instanz und der Konfiguration von Plugins hilft. Ein kritisches Update ist eine empfohlene Änderung an einer Instanz, die darauf abzielt, Ihnen zu helfen, die Bedeutung sicherheitsbezogener Änderungen zu verstehen. Kritische Updates unterstützt Sie bei der Implementierung der Schritte zum Scannen, Aktualisieren und Testen der Sicherheitsupdates in Ihrer Instanz. Implementieren Sie ein kritisches Update, um zu verhindern, dass die Anpassung Ihrer Instanz beeinträchtigt wird. Manuell implementierte kritische Updates unterscheiden sich von den automatischen Updates, die in Ihrer Instanz für ServiceNow-Code oder -Funktionalität mit Familien-Releases oder -Patches gerendert werden.

Auf der Homepage für kritische Updates sehen Sie die Zeitleiste der kritischen Updates, sodass Sie priorisieren können, wann die Schritte implementiert werden sollen. Die Zeitleiste im Screenshot zeigt die überfälligen und bald fälligen kritischen Updates. Darüber hinaus können Sie den Fortschritt Ihrer kritischen Updates unter der Bezeichnung Updates nachverfolgen. Wählen Sie die Registerkarten aus, damit Sie die verfügbaren, überfälligen, bald fälligen, in Bearbeitung oder abgeschlossenen kritischen Updates sehen können.



Erste Schritte:

- Greifen Sie auf dieses Tool zu, indem Sie in Security Center zu **Kritische Updates** navigieren.
- Kritische Updates sind ab Washington DC in der Security Center-App enthalten.

Implementieren Sie Schritte für kritische Updates

Erfahren Sie, wie Sie kritische Updates für Ihre Instanz implementieren, um die Sicherheitslage zu verbessern.

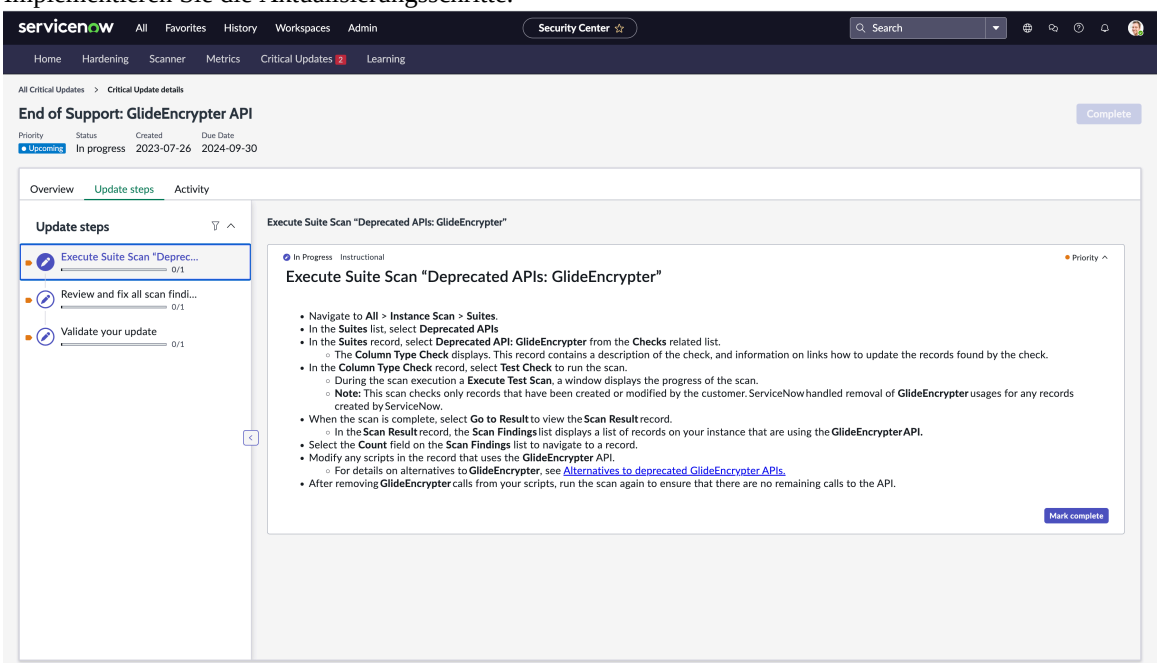
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Kritische Updates (CU) enthält Schrittanweisungen, wie Sie die Änderungen in Ihrer Instanz implementieren, um Ihre Sicherheitslage zu verbessern. CU ruft relevante Inhalte aus der Produktdokumentation ab, um Sie durch die einzelnen Schritte des Implementierungsprozesses zu führen. Führen Sie die folgenden Schritte aus, um zu erfahren, wie Sie ein kritisches Update implementieren.

Prozedur

1. Navigieren Sie zur App „ **Kritische Updates**“ .
2. Klicken Sie auf, um ein kritisches Update zu implementieren.
   Unter dem Abschnitt **Updates** werden auf der Registerkarte Verfügbar alle kritischen Updates für Ihre Instanz aufgelistet. Klicken Sie auf dieser Registerkarte auf ein kritisches Update, um die Anweisungen anzuzeigen.
3. Lesen Sie die Übersicht, um zu erfahren, warum das kritische Update erforderlich ist, und um sich auf die Implementierung der Schritte vorzubereiten.
   Klicken Sie auf **Zum nächsten Schritt** wechseln, um zu den Implementierungsdetails zu gelangen.
4. Implementieren Sie die Aktualisierungsschritte.



   a. Lesen Sie jede Gruppe von Anweisungen, und implementieren Sie sie in Ihrer Instanz.
   b. Klicken Sie auf Als **abgeschlossen** markieren, wenn Sie mit einer Reihe von Anweisungen fertig sind.
   c. Wiederholen Sie die Schritte ab, bis Sie alle Aktualisierungsschritte abgeschlossen haben.
   d. Klicken Sie auf **Abschließen**.
   Das kritische Update sollte im Abschnitt „Updates“ der Homepage „Kritische Updates“ nicht mehr verfügbar sein.

Zeigen Sie die Aktivität kritischer Updates an

Hier finden Sie Details zu allen Aktivitäten im Zusammenhang mit Ihren kritischen Updates.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

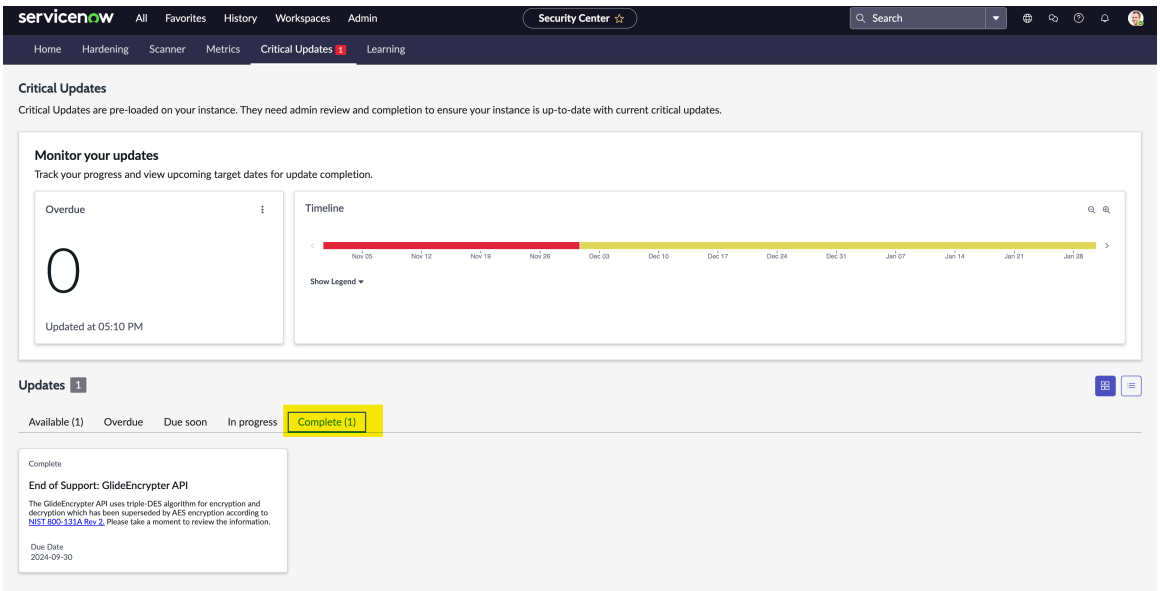
Warum und wann dieser Vorgang ausgeführt wird

Die Aktivitäten werden von neu nach alt aufgelistet, sodass Sie die letzte Aktivität zuerst analysieren können. Jede Aktualisierung einer Aktivität wird mit einem Zeitstempel versehen, und Sie können mithilfe von Suche und Filter nach bestimmten Informationen suchen.

Prozedur

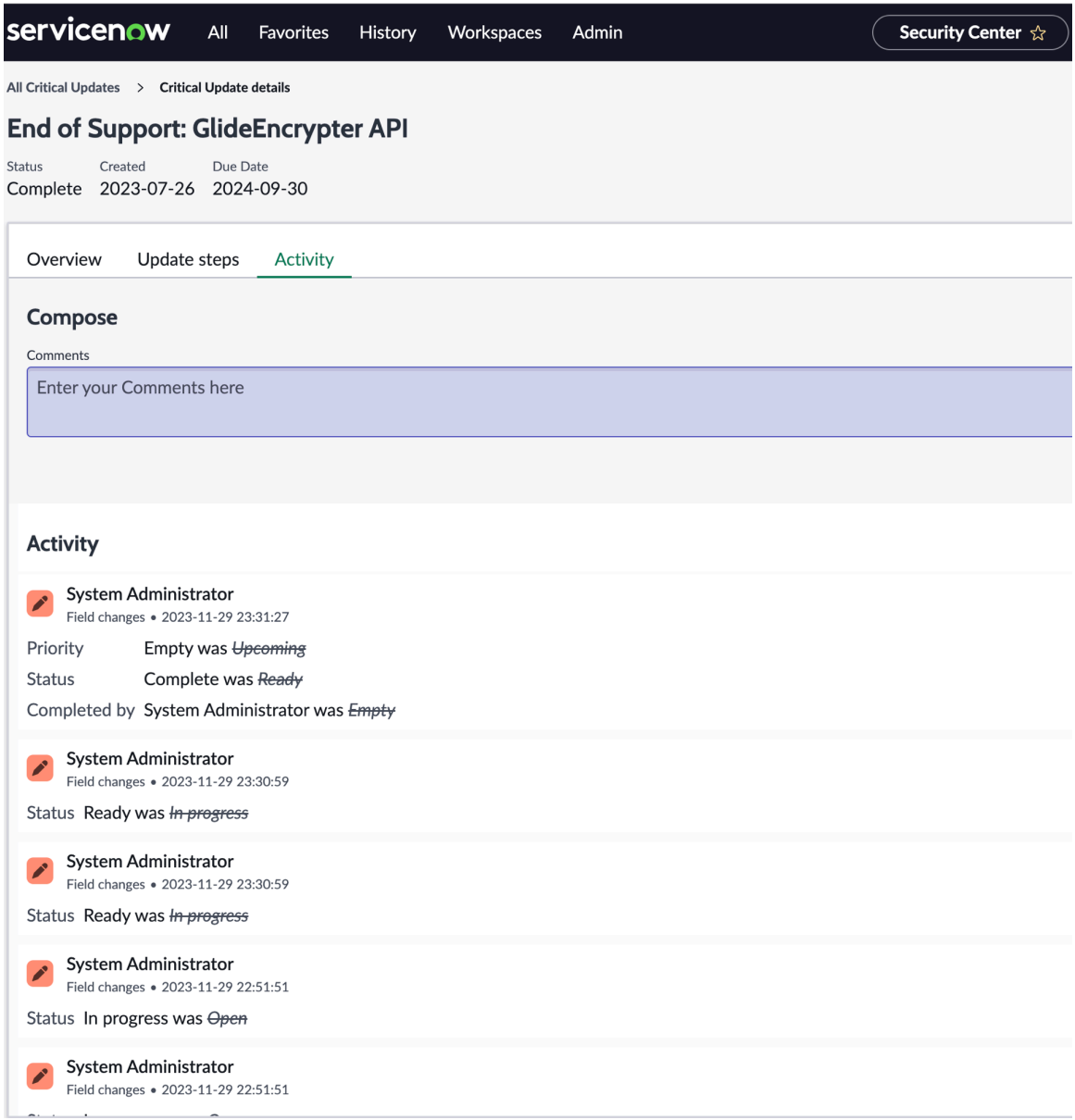
1. Navigieren Sie in Security Center zur App **Kritische Updates**.
2. Navigieren Sie zur **Aktualisierungsbezeichnung** von Kritische Updates.
3. Klicken Sie auf einen Status, und wählen Sie dann eine kritische Aktualisierung aus diesem Status aus.

   Im folgenden Beispiel wird der Status **Abgeschlossen** und dann das kritische Update für **Ende des Supports: GlideEncrypter-API** ausgewählt.



4. Zeigen Sie die Aktivität Ihres kritischen Updates an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Alle Aktivitäten im Zusammenhang mit einem kritischen Update werden automatisch aufgezeichnet. Darüber hinaus haben Sie die Möglichkeit, Aktivitäten zusätzliche Kommentare hinzuzufügen.

Sicherheitslernen

Greifen Sie von einer einzigen Seite aus auf Sicherheits-Lernmaterialien zu.

Lesen Sie Sicherheits-Whitepaper, E-Books, Knowledge Base-Artikel, Produktdokumentation und Community-Diskussionen aus einer konsolidierten Ansicht, indem Sie zu **Lernen**navigieren. Der Inhalt ist nach Überschriften und beschreibenden UI-Karten organisiert, damit Sie die richtige Ressource schnell finden.

Instanz-Sicherheitszentrum

Überwachen Sie die Compliance-Stufe der Instanzsicherheitskontrollen, zeigen Sie Metriken zur Überwachung von Sicherheitsereignissen an, und konfigurieren und verwalten Sie Instanzsicherheitseinstellungen – alles im Instanz-Sicherheitszentrum. Das Instance Security Center konsolidiert mehrere wichtige

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitskomponenten in einer einzigen Steuerungskonsole, mit der Sie instanzbasierte Sicherheits-Ereignisse erkennen, schützen und darauf reagieren können.

Übersicht über das Instanz-Sicherheitszentrum

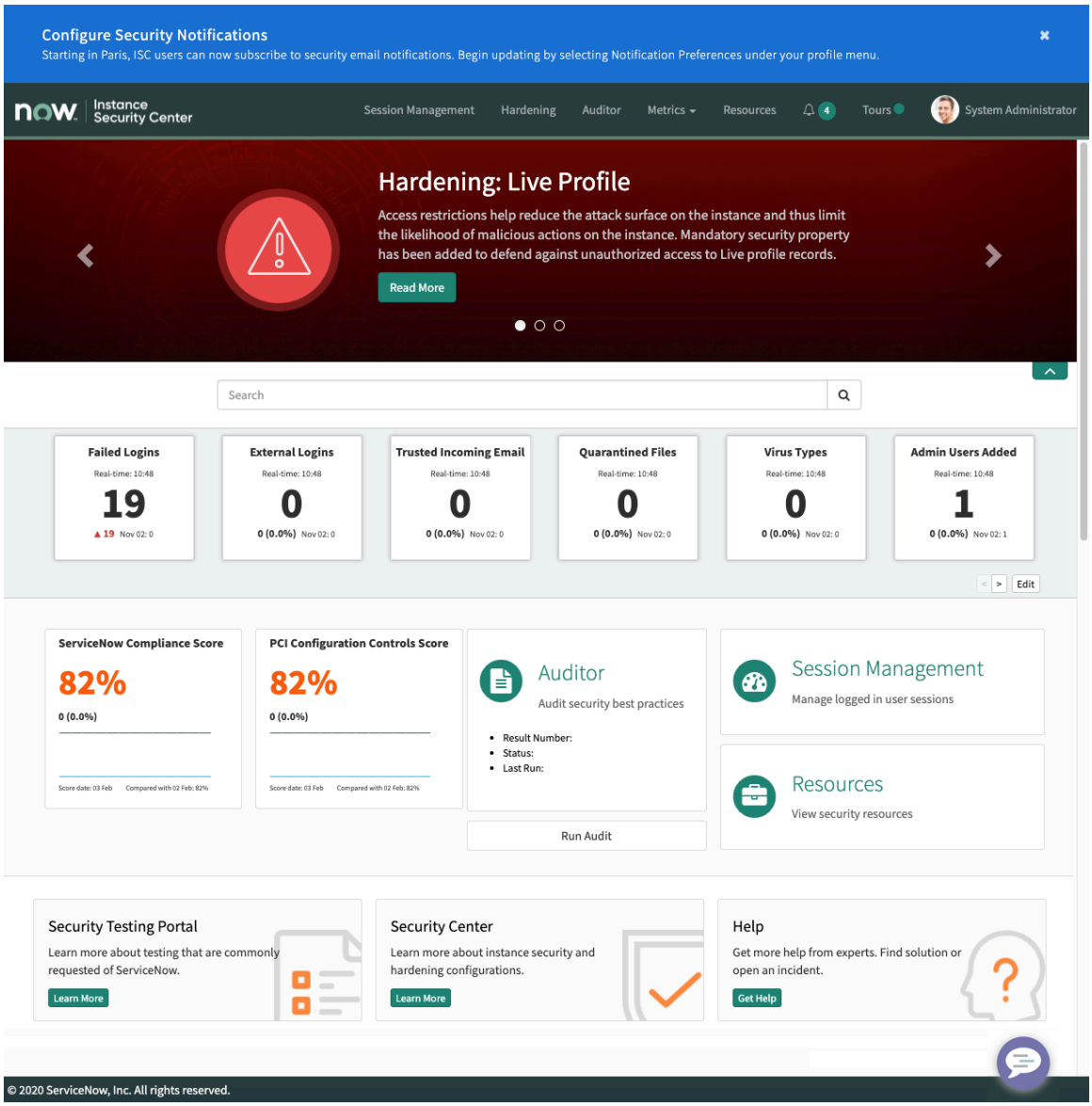
Hinweis:

Das Instanz-Sicherheitszentrum wird auf die zukünftige Einstellung vorbereitet. Es wird ausgeblendet und in neuen Instanzen nicht mehr aktiviert, aber weiterhin unterstützt. ServiceNow Security Center bietet die neueste Experience für diese Funktionalität.

Weitere Informationen finden Sie im Artikel Deprecation Process (Veraltungsprozess) in der Knowledge Base des Now Support.

Komponenten des Instanz-Sicherheitszentrums

Um auf das Instanz-Sicherheitszentrum zuzugreifen, navigieren Sie zu **Systemsicherheit** > **Instanz-Sicherheitszentrum** oder auf der Systemadministrations-Homepage.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Homepage des Instanz-Sicherheitszentrums enthält die folgenden Sicherheitskomponenten:

- Administratornachrichten
- Rotierendes Sicherheitsbanner
- Suchen
- Sicherheits-Event-Menüband
- Tägliche Compliance-Punktzahl
- Punktzahl der PCI-Konfigurationssteuerungen
- Management von Benutzersitzungen
- Härtung
- Auditor
- Metriken (Benutzer, E-Mail und Antivirus)
- Ressourcen
- Sicherheitsbenachrichtigungen
- Touren
- Sicherheitstestportal
- Sicherheitscenter
- Hilfe
- Virtual Agent-Zugriff

Auf der Homepage des Instanz-Sicherheitszentrums können Sie die Sicherheits-Compliance-Punktzahl für Ihre Instanz anzeigen und die allgemeine Sicherheitsintegrität überwachen. Sie können dann Systemeigenschaften konfigurieren oder aktualisieren, die sich auf die Sicherheit Ihrer Instanz beziehen, damit sie den Sicherheitsanforderungen entsprechen.

Hinweis:
Das Instanz-Sicherheitszentrum unterstützt keine Domänentrennung.

Benutzerrollen

Um das Instanz-Sicherheitszentrum zu verwenden, benötigen Sie die Rolle „admin“ oder „security_dashboard_user“.

Weitere Informationen zum Verwalten von Pro-Benutzer-Abonnements finden Sie unter Managing per-user subscriptions in Subscription Management. Wenden Sie sich an Ihren Kundenbetreuer.

Rollen

Erforderliche Rolle	Benutzer	Vorteile
Administrator	Diese Rolle hat Zugriff auf alle Systemfeatures, -funktionen und -daten, da Administratoren die Regeln der Zugriffssteuerungsliste (ACL) überschreiben und alle Rollenprüfungen bestehen können. Vermeiden Sie es, Benutzern diese	Nutzen Sie die Tools von Security Center, um den Sicherheitsstatus der Instanz zu verbessern und sicherheitsbezogenes Verhalten zu überwachen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen (Fortsetzung)

Erforderliche Rolle	Benutzer	Vorteile
	Rolle zuzuweisen, wenn gezieltere Rollen verfügbar sind.	
sn_vsc.security_center_viewer	Mit dieser Rolle können Benutzer, die keine Administratoren sind, die Informationen in Security Center anzeigen, aber keine Änderungen an den Tools Security Center vornehmen oder Instanzkonfigurationen mithilfe der Tools Security Center ändern. Beispielsweise möchten oder müssen Plattformbesitzer, Analysten für Sicherheitsvorgänge oder Compliance-Stakeholder möglicherweise einige der in Security Centerverfügbaren Sicherheits-KPIs, Sicherheitseinblicke und Sicherheitslernmaterialien anzeigen.	Verschaffen Sie sich einen Überblick über die Tools von Security Center, um den Sicherheitsstatus von Instanzen und das Sicherheitsverhalten zu überwachen.

Warnung:
Um sicherzustellen, dass das Instanz-Sicherheitszentrum bei jedem Upgrade aktuelle Sicherheitsinformationen erhält, passen Sie dieses Modul nicht an. Wenn Sie Sicherheitseinstellungen in Ihrer Instanz ändern, stellen Sie sicher, dass Sie sie zuerst in einer Nicht-Produktionsumgebung testen.

Administratornachrichten

Nachrichten und Erinnerungen, die hauptsächlich für Administratoren gedacht sind, werden über dem rotierenden Sicherheitsbanner angezeigt.

Beispielsweise wird eine Nachricht zum Konfigurieren von Sicherheitsbenachrichtigungen angezeigt, um Administratoren daran zu erinnern, Einstellungen für Sicherheitsbenachrichtigungen zu konfigurieren, falls dies noch nicht geschehen ist. Sie verweist sie auch auf die richtige Seite, um dies zu tun.

Hinweis:
Das Administratornachrichtenbanner wird nicht für Nicht-Admin-Benutzer angezeigt, oder wenn keine umsetzbaren Elemente für Admin-Benutzer vorhanden sind.

Rotierendes Sicherheitsbanner

Um Sie bei der Überwachung der Sicherheitsintegrität Ihrer Instanz zu unterstützen, werden im rotierenden Banner kritische Instanzsicherheitsmeldungen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zwei bis drei Sicherheitsmeldungen rotieren normalerweise in regelmäßigen Abständen.
- Die Punkte am unteren Rand des Banners zeigen die Gesamtzahl der aktuellen Sicherheitsmeldungen an.
- Um durch sie zu navigieren, wählen Sie die Punkte oder die Pfeile, die auf beiden Seiten der Nachrichten angezeigt werden.

Die Hintergrundfarben des Banners geben den relativen Schweregrad der Nachrichten an.

Farbe	Beschreibung
Rot	Kritische Sicherheitssituation, die eine zeitnahe Reaktion erfordert, oder eine Empfehlung zum Schutz oder zur Reaktion auf kritische Sicherheits-Ereignisse.
Dunkelgrau	Nicht kritische Warnmeldung.
Blau	Allgemeine Informationsnachricht.

Um den Textinhalt im Banner zu reduzieren oder zu minimieren, wählen Sie Banner reduzieren . Um den Textinhalt zu maximieren, wählen Sie ihn erneut aus.

- Wenn Sie das Instanz-Sicherheitszentrum erneut verwenden, wird der Textinhalt eingeklappt oder erweitert angezeigt, je nachdem, wie Sie ihn in der vorherigen Sitzung verwendet haben.
- Wenn sich der Textinhalt selbst ändert, wird er für alle Benutzer maximiert angezeigt.

Suchen

Verwenden Sie die Suchleiste, um das gesamte Instanz-Sicherheitszentrum nach Sicherheitsressourcen zu durchsuchen, die Sie beim Verständnis und der Lösung von Sicherheitsproblemen unterstützen. Sie können die folgenden sicherheitsbezogenen Ressourcen durchsuchen:

- Now Support Knowledge Base Artikel
- Seiten des Instanz-Sicherheitszentrums
- Externe Now Support Links
- PA-Sicherheits-Widgets, z. B. „Tägliche Compliance-Punktzahl“ und „Extern eingehende E-Mails“.
- Banner-Inhalt

Event-Menüband

Verwenden Sie das Event-Menüband, um wichtige Sicherheits-Event-Überwachungsmetriken für die aktuelle Instanz anzuzeigen.

- Um manuell durch die Metriken zu scrollen, wählen Sie die rechte oder linke Pfeiltaste.
- Um das Event-Menüband zu konfigurieren, wählen Sie **Bearbeiten**.

Weitere Informationen zum Event-Menüband und seiner Konfiguration finden Sie unter Überwachen Sie Sicherheits-Ereignisse und Konfigurieren Sie das Sicherheits-Event-Menüband.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tägliche Compliance-Punktzahl

Der Abschnitt „Tägliche Compliance-Punktzahl“ enthält die Kacheln „ **Tägliche Compliance-Punktzahl**“, **„Sitzungsmanagement“**, „ **Härtung**“, „ **Auditor**“ und „ **Ressourcen** “.

Sie verwenden die tägliche Compliance-Punktzahl, um zu messen, wie fehlerfrei Ihre Instanz aus sicherheitstechnischer Sicht ist.

Die tägliche Compliance-Punktzahl ist eine prozentuale Punktzahl. Sie basiert darauf, wie konform die aktuellen Einstellungen der Instanzsicherheitseigenschaften mit den im Härtungseinstellungen für die Instanzsicherheitveröffentlichten Compliance-Werten sind.

- Weitere Informationen zu Berechnungen der täglichen Compliance-Punktzahl und zu den Auswirkungen von Härtungseinstellungen finden Sie unter Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften.
- Mit der **Schaltfläche Aktualisieren** kann ein Administrator die tägliche Compliance-Punktzahl sofort neu berechnen. Weitere Informationen finden Sie unter Wie die Punktzahlen, Trends und Diagrammdaten der täglichen Compliance aktualisiert werden.

Härtung

Verwenden Sie diesen Prozess, um die spezifischen Sicherheitskonfigurationseigenschaften anzupassen, die sich auf die tägliche Compliance-Punktzahl auswirken:

1. Um auf die Seite „Härtungs-Compliance-Konfigurationen“ zuzugreifen und eine Härtung der Instanzsicherheit durchzuführen, wählen Sie die Kachel „ **Tägliche Compliance-Punktzahl** “ oder den Link **Härtung**.
2. Geben Sie an, ob Sie alle oder nur empfohlene Sicherheitskontrollen anzeigen möchten. Wählen Sie dann die Kategorie aus, in der Sie arbeiten möchten.
3. Legen Sie jede Sicherheitskonfigurationseigenschaft in der ausgewählten Kategorie fest. Klicken Sie auf **Weitere** Informationen, um detaillierte Informationen für eine Eigenschaft anzuzeigen.

Weitere Informationen zum Sichern und Optimieren von Sicherheitskonfigurationseigenschaften zur weiteren Verbesserung der Compliance finden Sie unter Passen Sie die Sicherheitseinstellungen der Instanz an, um die Compliance zu erhöhen.

Weitere Informationen darüber, wie Trend- und Diagrammdaten aktualisiert werden, finden Sie unter Wie die Punktzahlen, Trends und Diagrammdaten der täglichen Compliance aktualisiert werden.

Auditor

Führen Sie den Auditor aus, um Ihre Instanz zu scannen und falsche Sicherheitsdefinitionen zu finden. Sie enthält Ergebnisse, die Sie korrigieren können, um die Sicherheitslage Ihrer Instanz zu verbessern.

Um auf die Seite „Auditor“ zuzugreifen, wählen Sie die Kachel „ **Auditor** “ oder den Link „ **Auditor** “ aus. Weitere Informationen finden Sie unter Suchen Sie nach falschen Sicherheitsdefinitionen.

Sitzungsverwaltung

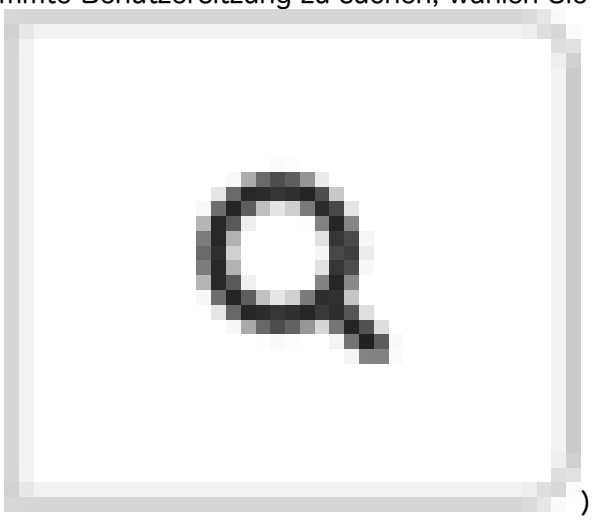
Verwenden Sie Session Management für Folgendes:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Benutzeranmeldungssitzungen anzeigen und verwalten.
- Zeigen Sie die Benutzeranmeldungssitzung des aktuellen Knotens an, mit dem Sie verbunden sind.
- Zeigen Sie detaillierte Informationen zu jeder Sitzung an, z. B. Benutzername und IP-Adresse.
- Isolieren und sperren Sie bestimmte Benutzersitzungen, die Sicherheitsrisiken darstellen.

Um auf die Seite „Sitzungsverwaltung“ zuzugreifen, wählen Sie die Kachel **Sitzungsverwaltung** oder den Link aus.

Feld	Beschreibung
Benutzer	Name des Benutzers, der dieser Anmeldesitzung zugeordnet ist. • Um eine bestimmte Benutzersitzung zu suchen, wählen Sie das Spotlight-Suchsymbol () aus, um nach Benutzer, Benutzer-Agent-Stichwort oder IP-Adresse zu suchen. Wenn Sie beispielsweise alle aktuellen Anmeldungen von einem bestimmten Browsertyp suchen möchten, geben Sie den Browsernamen als Stichwort in das Feld **Benutzeragent** ein. • Klicken Sie auf einen Benutzernamen, um auf den Benutzerprofildatensatz zuzugreifen. Sie können das Benutzerprofil nur ändern, wenn Ihnen eine Administratorrolle zugewiesen wurde. **Hinweis:** Weitere Informationen zu Benutzerprofilen finden Sie unter Benutzer erstellen .
MFA	Kontrollkästchen, das angibt, ob die Multifaktor-Authentifizierung (MFA) für den angemeldeten Benutzer aktiviert ist. Weitere Informationen zu MFA finden Sie unter Multifaktor-Authentifizierung (MFA).
Aktiv	Checkbox, die angibt, ob der angemeldete Benutzer aktiv oder inaktiv ist.
Benutzeragent	Typ des Browsers und Betriebssystem des Geräts für die Benutzeranmeldungssitzung.
IP-Adresse	IP-Adresse des angemeldeten Benutzers.
Letzter Zugriff	Datum und Uhrzeit des letzten Zugriffs dieser Benutzersitzung auf die Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Um detaillierte Informationen für eine bestimmte Anmeldesitzung anzuzeigen oder die Sitzung selbst zu sperren, wählen Sie die Felder **Benutzeragent**, **IP-Adresse**oder **Zuletzt aufgerufen** aus.

Metriken

Zeigen Sie Details für die folgenden Metriktypen an:

Typ der Metrik	Beschreibung
Benutzer	Sicherheitsmetriken, die der Benutzeraktivität in der Instanz zugeordnet sind. Um auf die Seite „Benutzermetriken“ zuzugreifen, klicken Sie auf den Link **Metriken** und dann auf **Benutzermetriken**.
Exportieren	Sicherheitsmetriken, die den aus der Instanz exportierten Daten zugeordnet sind. Um auf die Seite „Metriken exportieren“ zuzugreifen, klicken Sie auf den Link **Metriken** und dann auf **Metriken exportieren**.
Authentifizierung	Sicherheitsmetriken, die der Authentifizierung zugeordnet sind, z. B. selten verwendete IP-Adressen, fehlgeschlagene Anmeldungen und Arten von Authentifizierungsschemata, die von Ihren Benutzern verwendet werden. Um auf die Seite „Metriken exportieren“ zuzugreifen, wählen Sie den Link **Metriken** und dann **Authentifizierungsmetriken aus**.
E-Mail	Sicherheitsmetriken, die anomalem Verhalten im Zusammenhang mit eingehenden E-Mails in Ihrer Instanz zugeordnet sind. Um auf die Seite „E-Mail-Metriken“ zuzugreifen, wählen Sie den Link **Metriken** und dann E- **Mail-Metriken**aus.
Virenschutz	Sicherheitsmetriken, die der Antiviren-Event-Aktivität in der Instanz zugeordnet sind Um auf die Seite Antivirus-Metriken zuzugreifen, wählen Sie die **Antivirus** -Kachel oder den Link **Metriken** und dann **Antivirus**aus.

Hinweis:
Weitere Informationen zum Überwachen der einzelnen Metriktypen finden Sie unter Überwachen Sie Instanzmetriken.

Ressourcen

Greifen Sie auf Now Support Knowledge Base Artikel, Ressourcen und Blogs zu, die sich auf die Instanzsicherheit beziehen. Diese Ressourcen umfassen Sicherheitseinstellungen, Codierung, Compliance, Korrekturen und verwandte Themen. So greifen Sie auf die Seite „Ressourcen“ zu:

1. Klicken Sie auf die Kachel oder den Link **Ressourcen**.
2. Wählen Sie auf der Seite „Ressourcen“ eine Kategorie aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Beschreibung
Empfohlene Richtlinien	Zugriff auf empfohlene Sicherheitsrichtlinien, einschließlich der Artikel Härtungseinstellungen für die Instanzsicherheit und Leitfaden für sichere Codierung [KB0623354].
Sicherheitsressourcen	Zugriff auf sicherheitsbezogene Ressourcen in Knowledge Base, einschließlich: ○ Sicherheitstest der Kundeninstanz ○ Cloud Security, Trust, and Compliance Center KB-Artikel

Sicherheitsbenachrichtigungen

Im Instanz-Sicherheitszentrum wird ein Benachrichtigungs-Glockensymbol ( ) mit einer Gesamtanzahl der ungelesenen Sicherheitsbenachrichtigungen angezeigt. Benachrichtigungen bleiben bestehen und werden in dieser Anzahl berücksichtigt, bis Sie sie als gelesen markieren.

1. Klicken Sie auf das Glockensymbol, um die ersten fünf ungelesenen Sicherheitsbenachrichtigungen anzuzeigen.

   Eine Benachrichtigung wird angezeigt, wenn in Ihrer Instanz die Ereignisse „Administratoranmeldung“, „ **Administrator entsperrt**“, „ **FehlgeschlageneAnmeldung**“, „ **Rolle mit hohen Berechtigungen“**, „ **Identitätswechsel“**, „ **Sicherheitserhöhung“**und „ **Wöchentliche Zusammenfassung“** stattfinden. Weitere Informationen zu diesen Sicherheitsereignissen finden Sie unter Überwachen Sie Sicherheits-Ereignisse.

2. Um detaillierte Informationen für ein bestimmtes Sicherheitsereignis anzuzeigen, wählen Sie die Benachrichtigung aus.

   Wenn Sie beispielsweise eine Benachrichtigung für eine Rolle mit hohen Berechtigungen auswählen, können Sie die Tabelle „Rollen“ (sys_user_role) anzeigen. Verwenden Sie diese Tabelle, um anzuzeigen, welchen Benutzern während des Kalendertags privilegierte Rollen zugewiesen wurden. Anhand dieses Verlaufs können Sie feststellen, ob die Rollen ordnungsgemäß zugewiesen wurden.

3. Wenn mehr als fünf ungelesene Benachrichtigungen vorhanden sind, wählen Sie **Alle Benachrichtigungen** anzeigen aus, um auf die Seite Alle Benachrichtigungen mit einer Liste aller ungelesenen Benachrichtigungen zuzugreifen.
   - Um detaillierte Informationen für ein bestimmtes Sicherheitsereignis anzuzeigen, wählen Sie die Benachrichtigung aus.
   - Um alle aufgelisteten Benachrichtigungen als gelesen zu markieren, wählen Sie **Alle als gelesen**markieren aus.

Hinweis:
Als Administrator können Sie auch Einstellungen für das Senden bestimmter Arten von Benachrichtigungen für jeden Typ von Sicherheits-Ereignis konfigurieren. Weitere Informationen finden Sie unter Legen Sie die Einstellungen für Sicherheits-Event-Benachrichtigungen fest.

Touren

Klicken Sie auf den Link **Touren**, um eine geführte visuelle Tour durch das Instanz-Sicherheitszentrum anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Guided Tour enthält nur die Sicherheitsüberwachungsfunktionen, die auf der Homepage aufgeführt sind.
- Sie enthält nicht die Sicherheitsfunktionen, auf die Sie zugreifen, wenn Sie die Kacheln oder Links auf der Homepage auswählen.

Sicherheitstestportal, Sicherheitscenter und Hilfe

Now Support Serviceportal ist eine zentrale Ressource, die Sie zum Verwalten von Instanzen, Aufgaben und Konten verwenden. Sie können auch auf nützliche Ressourcen zugreifen, mit denen Sie Sicherheits- und technische Probleme in Ihrer Instanz diagnostizieren und beheben können.

Um auf diese Ressourcen zuzugreifen, wählen Sie in den folgenden Kacheln **„Weitere Informationen“** oder **„Hilfe** erhalten“ aus:

Kachel	Beschreibung
Portal für Sicherheitstests	Zugriff auf das Sicherheits-Dashboard im Now Support Security Testing Portal.
Sicherheitscenter	Zugriff auf Security Compliance im Now Support Sicherheitsportal.
Hilfe	Zugriff auf die folgenden Hilferessourcen im Sicherheitsportal Now Support : • Bitten Sie einen Experten, Antworten auf häufig gestellte Fragen zu finden. • Melden Sie dem globalen technischen Support von ServiceNow ein Problem oder einen Ausfall, indem Sie einen Fall öffnen. • Selfservice-Supportressourcen, einschließlich: ◦ Videos ◦ Dokumentation ◦ ServiceNow Community ◦ Knowledge Base ◦ Known Error-Portal ◦ Sicherheits-RFX-Datenbank • ServiceNow Community Fragen, die für Ihre Verwendung empfohlen werden.

Virtual Agent-Zugriff

Virtual Agent ist eine Plattform für die Bereitstellung von Benutzerhilfe durch Konversationen innerhalb einer Messaging-Schnittstelle.

Wenn die zugehörigen Plugins installiert sind, können Administratoren auf die Funktionen Virtual Agent und Natural Language Understanding (NLU) zugreifen, indem sie das Virtual Agent-Symbol auswählen:

Sie können damit die folgenden Aufgaben ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicherheitsbezogene Fragen, und erhalten Sie dann kurze Antworten und Referenzlinks, um mehr zu erfahren.
- Erhalten Sie Antworten im Zusammenhang mit Prozessen wie:
  - Instanz-Sicherheitszentrum
  - Platform-Sicherheit
  - ServiceNow -Sicherheitsrichtlinien
  - Vertrauen, Governance und Risiko
- Suchen Sie nach sicherheitsbezogenen Ressourcen, z. B. Knowledge Base -Themen im Now Support -Sicherheitsportal.

Hinweis:
Weitere Informationen zur Verwendung und Aktivierung von Virtual Agentfinden Sie unter:

- Virtual Agent
- Aktivieren Sie die ISC-Schnittstelle Virtual Agent .

Migration von Instance Security Center zu ServiceNow Security Center .

Lernen Sie die wichtigsten Unterschiede bei der Migration von Instance Security Center (ISC) zu ServiceNow Security Center (SSC) kennen.

ServiceNow Security Center (SSC) ist eine neue Sicherheitsanwendung, die aus einer Reihe von speziell entwickelten Tools besteht, die Unternehmen dabei unterstützen, die Sicherheit ihrer ServiceNow-Bereitstellungen zu gewährleisten. Mit Security Center können Unternehmen ihre Sicherheitslage verbessern und ihre Compliance-Stufen durch eine nahtlose Benutzer-Experience stärken. Instance Security Center (ISC) ist das Legacy-Produkt. ServiceNow beendet den Support für ISC mit dem Now Platform Xanadu-Release, das für September 2024 geplant ist. Daher ist SSC die empfohlene Lösung für die Zukunft.

Aktualisierung der Härtungseinstellung für SSC

Erfahren Sie mehr über die Aktualisierungen der Härtungseinstellungen in ServiceNow Security Center (SSC).

Funktionsverbesserungen	ISC vs. SSC
Erweiterte Härtungseinstellungen für Sicherheit	SSC enthält eine viel größere Anzahl von Härtungseinstellungen im Vergleich zu früheren Versionen von ISC. Zukünftige SSC-Versionen werden die Anzahl der Einstellungen weiter erhöhen.

Vereinfachte Bewertung von Härtungseinstellungen	• ISC verwendet eine Formel, die eine bestimmte prozentuale Auswirkung für hohe, mittlere und niedrige Einstellungen sicherstellt.
	• SSC verwendet eine andere Formel:
	  ○ Jede Einstellung hat eine eigene Punktzahlgewichtung.
	  ○ Die Compliance-Bewertung für Härtung wird berechnet, indem der Zähler

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsverbesserungen	ISC vs. SSC
	(Summe aller konformen Einstellungen) durch den Nenner (Summe der Auswirkungsgewichtungen für alle Einstellungen) geteilt wird.
Verbesserte Benutzer-Experience für die Auswertung von Daten	• Compliance-Bewertungen für zwei verschiedene Daten vergleichen. • Visualisieren Sie Compliance-Punktzahlen in einem Liniendiagramm, und analysieren Sie Daten mit Analytics Hub.

Führen Sie allgemeine Sicherheitshärtungsaufgaben in SSC durch

Im Folgenden finden Sie Anweisungen zum Ausführen allgemeiner Aufgaben zur Erhöhung der Sicherheit in SSC.

Überprüfen Sie die neueste Punktzahl	Navigieren Sie zu einem der folgenden Elemente: • **Startseite** Weitere Informationen finden Sie unter Homepage. • **Härtung > Punktzahl** Weitere Informationen finden Sie unter Compliance-Punktzahltrend für Härtung.
Aktualisieren Sie die neueste Punktzahl	Wählen Sie auf der SSC-Homepage **Punktzahl aktualisieren**aus.
Ändern Sie die Konfiguration der Einstellung	Wählen Sie einen Einstellungsnamen auf einer der folgenden Seiten aus, um die Detailseiten der Einstellungen anzuzeigen, auf denen Sie die Konfiguration ändern, vorherige Aktivitäten anzeigen und Notizen hinzufügen können: • Startseite • Härtung > Alle Einstellungen • Härtung > Punktzahlvergleich Siehe Compliance-Bewertung für Härtung erhöhen
Legen Sie einen Zeitplan für die Neuberechnung Ihrer Compliance-Punktzahl fest	So planen Sie, wann das System eine Aktualisierung Ihrer Compliance-Bewertung auslöst: • Filtern Sie in der Tabelle `sysauto_script` nach `SC - Compliance monatlich berechnen`. • Ändern Sie den Datensatz, um den bevorzugten Zeitplan anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisierungen von Sicherheits-KPIs und -Metriken für SSC

Erfahren Sie mehr über die Aktualisierungen an Sicherheits-KPIs und -Metriken in ServiceNow Security Center (SSC).

Funktionsverbesserungen	ISC vs. SSC
Verbesserungen an KPIs	In SSC können Sie: • Zeigen Sie den Trend der Punktzahl im Zeitverlauf an. • Überwachen Sie alle KPIs und Metriken mithilfe derselben Schnittstelle und derselben Analysefunktionen.
Verbesserungen an Metriken	In SSC wurden die folgenden Erweiterungen vorgenommen: • Über 50 neue Metriken wurden hinzugefügt. • Sie können KPIs und Metriken über dieselbe Benutzeroberfläche überwachen und analysieren. • Sie können Ziele und Schwellenwerte für Metriken erstellen.

Greifen Sie in SSC auf Sicherheits-KPIs und -Metriken zu

Führen Sie einen der folgenden Schritte aus:

- Navigieren zu **Startseite** > **Metriken**, und wählen Sie dann **Metriken** aus dem linken Navigationsmenü aus.
- Navigieren zu **Startseite** > **Alle Metriken**, und wählen Sie dann Metriken aus der Tabelle aus.

Sicherheitsscanner-Updates in SSC

Erfahren Sie mehr über die Aktualisierungen des Sicherheitsscanners in ServiceNow Security Center (SSC).

Funktionsverbesserungen	ISC vs. SSC
Neue Funktionalität	SSC enthält die folgenden neuen Funktionen: • Führen Sie Scans manuell aus, oder planen Sie sie so, dass sie zu bestimmten Zeiten ausgeführt werden. • Erstellen Sie Ihre eigenen Scan-Prüfungen. • Erstellen Sie Ihre eigene Scan-Suite. • Vergleichen Sie die Ergebnisse von zwei Scans.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsverbesserungen	ISC vs. SSC
Verbesserte E-Mail-Funktionalität	Richten Sie E-Mail-Benachrichtigungen ein, damit Sie über neue Sicherheits-Ereignisse in Ihrer Instanz benachrichtigt werden.

Führen Sie allgemeine Sicherheitsscanner-Aufgaben in SSC aus

Im Folgenden finden Sie Anweisungen zum Ausführen allgemeiner Sicherheitsscanner-Aufgaben in SSC.

Führen Sie den Auditor-Suite-Scan aus	1. Navigieren zu **Scanner** > **Suites**. 2. Wählen Sie die Auditor-Suite aus der Lis–te aus. 3. Wählen Sie **Sicherheitsscan ausführen aus**.
Suite-Scan-Ergebnisse anzeigen	Navigieren zu **Scanner** > **Ergebnisse**.

Neue Sicherheitsfunktionen in SSC

Erfahren Sie mehr über die neuen Sicherheitsfunktionen, die in ServiceNow Security Center (SSC) eingeführt wurden.

Die folgenden neuen Funktionen wurden zu ServiceNow Security Center hinzugefügt.

- Sitzungen überwachen: Sie können die Sitzungsaktivitäten im Zeitverlauf mit dem neuen Metriktool visualisieren.
- Ressourcen finden: Alle Sicherheits-Lernressourcen sind jetzt auf einer einzigen Seite gruppiert.

Verwenden Sie neue Sicherheitsfunktionen in SSC

Überwachen Sie die Sitzungsaktivität	1. Navigieren Sie zu **Metriken**. 2. Wählen Sie in der linken Navigation unter Sitzungsverwaltung die Option **Aktive Sitzung**aus.
Greifen Sie auf Lernressourcen zu	Navigieren Sie zu **Lernen**.

Überwachen Sie Sicherheits-Ereignisse

Analysieren Sie die Event-Metriken in Ihrer Instanz, damit Sie potenzielle Sicherheits-Events erkennen und verhindern können.

Im Event-Menüband auf der Instanzsicherheits-Homepage können Sie diese Metriken und die zugehörigen Details analysieren, um potenzielle Sicherheits-Events in der Instanz zu identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für jede Event-Metrik wird eine einzelne Punktzahl in Echtzeit angezeigt, die angibt, wie oft das Event während des Tages in dieser Instanz aufgetreten ist. Diese Einzel-Punktzahl-Berichte werden automatisch aktualisiert, wenn die entsprechenden Ereignisse stattfinden.
- Jede Event-Metrik enthält auch Compliance-Trend- und Diagramminformationen für einen bestimmten Datumsbereich. Diese Informationen werden täglich aktualisiert, wenn Sie den Performance Analytics-Auftrag ausführen. Weitere Informationen finden Sie im Abschnitt „ **Event-Trenddetails analysieren** “.

Ereignistypen

Sie können mindestens sechs der folgenden Ereignistypen überwachen. Verwenden Sie bei mehr als sechs Events die Pfeile nach links oder rechts unter dem Event-Menüband, um durch sie zu scrollen. Informationen zum Konfigurieren des Event-Menübands finden Sie unter Konfigurieren Sie das Sicherheits-Event-Menüband.

Benachrichtigungseinstellung	Beschreibung
Administratoranmeldungen	Anzahl der Anmeldeversuche in dieser Instanz während des Kalendertags durch Benutzer, denen eine Administratorrolle zugewiesen ist.
Administratorbenutzer hinzugefügt	Anzahl der Benutzer mit einer Administratorrolle, die in dieser Instanz während des Kalendertags hinzugefügt wurden. Beispielsweise kann in Ihrer Instanz ein Sicherheitsproblem auftreten, wenn die Anzahl 10 beträgt, aber 4 Benutzer bekanntermaßen eine zugewiesene Administratorrolle haben.
Externe eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Externe Anmeldungen	Anzahl der Benutzer mit der zugewiesenen Rolle snc_external, die sich während des Kalendertags bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen in der Regel zu Wartungs-, Support-, Beratungs- oder Auditzwecken. Durch die Überwachung dieser Metrik können Sie überprüfen, ob die externen Anmeldeversuche legitim sind und keine potenziellen Sicherheitsprobleme darstellen. Weitere Informationen zum Zuweisen externer Benutzerrollen finden Sie unter Explizite Rollen.
Fehlgeschlagene Anmeldungen	Anzahl der versuchten Anmeldungen, die während des Kalendertags in dieser Instanz fehlgeschlagen sind. Diese Metrik kann darauf hinweisen, dass versucht wird, sich anzumelden und die Sicherheit Ihrer Instanz zu gefährden.
Identitätswechsel	Anzahl der Anmeldungen mit Identitätswechsel in dieser Instanz während des Kalendertags. Weitere Informationen dazu, wie Sie die Identität von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
	Benutzern annehmen, finden Sie unter Identitäten von Benutzern annehmen .
Dateien in Quarantäne	Anzahl der Dateien, die beim Ausführen von Antivirus-Scanning in dieser Instanz während des Kalendertags unter Quarantäne gestellt wurden. Weitere Informationen zu Dateien in Quarantäne und Antivirus-Scanningfinden Sie unter Virenschutzmetriken und Antivirus-Scanning.
Erhöhungen der Sicherheit	Anzahl der Fälle, in denen ein Sicherheitsadministrator die Sicherheit für Standardbenutzer erhöht hat, indem die zugewiesene Benutzerrolle während des Kalendertags in eine Sicherheitsrolle mit hohen Berechtigungen geändert wurde. Zu diesen Sicherheitsrollen mit hohen Berechtigungen gehören oauth_admin, admin, security_admin und impersonator. • Diese Metrik weist darauf hin, dass jemand versucht hat, die Sicherheit eines nicht autorisierten Benutzers zu erhöhen. Verwenden Sie diese Metrik nicht allein, um eine bestimmte Sicherheitsgefährdung zu erkennen. Behandeln Sie diese Metrik stattdessen als Hinweis darauf, dass Sie eine andere Metrik überprüfen sollten, um festzustellen, ob eine Sicherheitskompromittierung aufgetreten ist. • Weitere Informationen zum Erhöhen der Benutzersicherheit finden Sie unter Führen Sie eine Erhöhung auf eine privilegierte Rolle durch und Rollen mit erhöhten Berechtigungen.
SNC-Anmeldungen	Anzahl der Kundenservice und Support Mitarbeiter, die sich während des Kalendertags mithilfe der Hi-Hopping-Technik bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen in der Regel zu Wartungs-, Support-, Beratungs- oder Auditzwecken. Informationen zur Steuerung des Zugriffs von ServiceNow für Unternehmensmitarbeiter finden Sie unter ServiceNow-Zugriffssteuerung.
Spam	Weitere Informationen finden Sie unter E-Mail-Metriken.
Vertrauenswürdige eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Nicht vertrauenswürdige eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
Virustypen	Anzahl der verschiedenen Arten von Antiviren-Ereignissen, die in dieser Instanz während des Kalendertags aufgetreten sind. Weitere Informationen zu Antivirus-Ereignistypen finden Sie unter Antivirus-Metriken.

Event-Trenddetails werden analysiert

Um Trenddetails für eine Event-Metrik anzuzeigen, klicken Sie auf die Event-Anzahl, um auf die Seite „Analyse-Hub“ zuzugreifen. Die für die Instanz angezeigten Details hängen vom Typ der Metrik ab.

So zeigen Sie beispielsweise eine Liste aller Fehlversuche auf der Seite „Ereignisprotokolle des Sicherheits-Dashboards“ an:

- Wählen Sie die Metrik **Fehlgeschlagene Anmeldungen** aus.
- Klicken Sie auf der Seite Analytics Hub auf **Datensätze**anzeigen.
- Klicken Sie auf einen der fehlgeschlagenen Anmeldeversuche.
- Die Details umfassen den Namen des Benutzers, der versucht hat, sich anzumelden, seine IP-Adresse und den Namen der Tabelle, auf die er zuzugreifen versucht hat.

Sie können Event-Schwellenwertauslöser in Analytics Hub einrichten, um Warnungen bereitzustellen, wenn ein bestimmtes Event innerhalb eines Punktzahlbereichs für einen Indikator auftritt. Sie können auch Ziele festlegen, mit denen Sie den Unterschied zwischen der gewünschten Punktzahl und der tatsächlichen Punktzahl eines Events visualisieren können.

Sie können beispielsweise einen Schwellenwert von 10 für die Metrik „ **Fehlgeschlagene Anmeldungen** “ festlegen. Wenn an einem Tag zehn oder mehr fehlgeschlagene Anmeldeversuche auftreten, wird eine Warnung an bestimmtes Sicherheitspersonal gesendet. Sie können auch ein ähnliches Ziel festlegen, das im Analytics Hub visuell hervorgehoben wird, wenn an einem Tag 10 fehlgeschlagene Anmeldungen auftreten.

Trenddaten und Diagramme, die in der Menübandkachel „Event“ angezeigt werden, und Analytics Hub werden aktualisiert, nachdem der Performance Analytics-Auftrag um 02:00 Uhr Ortszeit ausgeführt wurde. Weitere Informationen finden Sie unter Wie die Punktzahlen, Trends und Diagrammdaten der täglichen Compliance aktualisiert werden.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Now Intelligence

Analytics Hub

Performance Analytics Ziele und Schwellenwerte

Konfigurieren Sie das Sicherheits-Event-Menüband

Konfigurieren Sie das Sicherheits-Event-Menüband auf der Homepage des Instanz-Sicherheitszentrums so, dass nur die Events einbezogen werden, die für die Nachverfolgung der Instanzsicherheit in Ihren Vorgängen relevant sind. Sie können auch die Reihenfolge ändern, in der die Sicherheits-Event-Kacheln im Menüband angezeigt werden.

Vorbereitungen

Erforderliche Rolle: security_dashboard_user oder admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Das Sicherheits-Event-Menüband wird anfänglich mit einem vollständigen Satz von Standard-Sicherheits-Events ausgefüllt. Sie können sie anpassen, indem Sie die Events entfernen, die für Ihre Organisation nicht relevant sind.

- Wenn Sie beispielsweise vermuten, dass Sicherheitsprobleme auf die Aktionen von internem Personal zurückzuführen sind, beziehen Sie die Ereignisindikatoren „Administratoranmeldungen“, „Administratorbenutzer hinzugefügt“ und „Erhöhungen der Sicherheit“ ein.
- Diese Indikatoren überwachen, wie oft Benutzer mit Administratorrollen versucht haben, sich anzumelden, und, falls Administratorbenutzer hinzugefügt wurden, welche Versuche unternommen wurden, um die Sicherheitsrollen zu erhöhen.

Hinweis:
Weitere Informationen zu den Arten von Sicherheits-Events, die im Event-Menüband angezeigt werden, finden Sie unter Überwachen Sie Sicherheits-Ereignisse.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**.
2. Klicken Sie im Event-Menüband auf **Bearbeiten** (

„Bearbeiten“).
Im Formular „Events bearbeiten“ enthält die Spalte **Ausgewählt** die Events, die bereits aufgelistet sind.
3. Um dem Event-Menüband Sicherheits-Events hinzuzufügen, verschieben Sie sie aus der Spalte **Verfügbar** in die Spalte **Ausgewählt**.
Um die Reihenfolge zu ändern, in der die Events im Menüband angezeigt werden, wählen Sie ein Event aus und klicken Sie dann auf den Pfeil nach oben oder unten, um es an die richtige Position zu verschieben.
   - Platzieren Sie die Events in derselben Reihenfolge, in der sie im Event-Menüband des Instanz-Sicherheitszentrums angezeigt werden sollen.
   - Die Events, die Sie oben in der Spalte **Verfügbar** platzieren, werden der Reihe nach angezeigt, beginnend auf der linken Seite des Event-Menübands des Instanz-Sicherheitszentrums. Die Events am unteren Rand der Spalte werden rechts im Event-Menüband angezeigt.
4. So entfernen Sie Sicherheits-Events aus dem Event-Menüband:
   - Wählen Sie in der Spalte **Ausgewählt** die Sicherheits-Events aus, die Sie aus dem Event-Menüband entfernen möchten.
   - Verschieben Sie sie aus der Spalte **Ausgewählt** in die Spalte **Verfügbar**.
5. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Legen Sie die Einstellungen für Sicherheits-Event-Benachrichtigungen fest

Konfigurieren Sie die Voreinstellungen für die Arten von Benachrichtigungen, die Sie beim Auftreten bestimmter Sicherheits-Ereignisse erhalten möchten. Für jeden Typ legen Sie fest, ob Benachrichtigungen per E-Mail, per Push-Benachrichtigung in Now Mobileoder in Messaging-Anwendungen von Drittanbietern wie Slack oder Microsoft Teamsempfangen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Damit Messaging-Anwendungen von Drittanbietern Benachrichtigungen zu Sicherheitsereignissen senden können, müssen Sie das Plugin „Messaging Notification“ (com.glide.notification.messaging) aktivieren. Einzelne Benutzer müssen ihre eigenen Einstellungen konfigurieren. Weitere Informationen finden Sie unter Benachrichtigungen in Messaging-Anwendungen .

Erforderliche Rolle: admin.

Prozedur

1. Klicken Sie auf der Homepage des Instanz-Sicherheitszentrums auf das Profilmenü und dann auf **Benachrichtigungseinstellungen**.

Benachrichtigungseinstellungen

Benachrichtigungseinstellung	Beschreibung
Administratoranmeldung	Senden Sie die ausgewählte Art von Benachrichtigung, wenn sich andere Benutzer mit zugewiesenen Administratorrollen von einer anderen IP-Adresse aus bei dieser Instanz anmelden.
Administrator entsperren	Senden Sie die ausgewählte Art von Benachrichtigung, wenn ein Account für einen Benutzer mit hohen Berechtigungen entsperrt wurde.
Fehlgeschlagene Anmeldung	Senden Sie den ausgewählten Benachrichtigungstyp, wenn sich andere Benutzer nicht in weniger als der in der Eigenschaft `glide.user.max_unlock_attempts` definierten Anzahl von Versuchen bei dieser Instanz anmelden. Wenn Sie diese Eigenschaft nicht konfigurieren, lautet der Standardwert 5. Weitere Informationen zu dieser Eigenschaft finden Sie unter Sperrung für fehlgeschlagene Anmeldeversuche angeben.
HP-Rolle hinzugefügt	Senden Sie die ausgewählte Art von Benachrichtigung, wenn einem anderen Benutzer eine Sicherheitsrolle mit hohen Berechtigungen (einschließlich oauth_admin, admin, security_admin und Identitätswechsel) gewährt wird. Weitere Informationen zum Erhöhen der Benutzersicherheit finden Sie unter Führen Sie eine Erhöhung auf eine privilegierte Rolle durch und Rollen mit erhöhten Berechtigungen.
Identitätswechsel	Senden Sie die ausgewählte Art von Benachrichtigung, wenn ein anderer Benutzer die Identität eines anderen Benutzers annimmt. Weitere Informationen dazu, wie Sie die Identität von Benutzern annehmen, finden Sie unter Identitäten von Benutzern annehmen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
Erhöhung der Sicherheit	Senden Sie die ausgewählte Art von Benachrichtigung, wenn andere Benutzer in dieser Instanz auf eine Sicherheitsadministratorrolle hochgestuft werden.
Wöchentlicher Digest	Senden Sie eine wöchentliche Zusammenfassung für den ausgewählten Benachrichtigungstyp. Sie umfasst: ○ Eine Zusammenfassung aller Sicherheitsaktivitäten, die in dieser Instanz während der Woche stattgefunden haben. ○ Die aktuelle tägliche Compliance-Punktzahl für die Instanz.

2. Aktivieren Sie für jede Art von Sicherheitsereignis die entsprechenden Kontrollkästchen, um die Art der zu sendenden Benachrichtigungen festzulegen.
   Sie können jeweils mehrere Benachrichtigungsmethoden auswählen.

3. Klicken Sie auf **Speichern**.

Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften

Überprüfen Sie die Metrik „Tägliche Compliance-Punktzahl“ und die Sicherheitskonfigurationseigenschaften, um festzustellen, ob Ihre Instanz die vorgeschlagenen Sicherheitsanforderungen erfüllt. Sie können die tägliche Compliance-Punktzahl beeinflussen, indem Sie nicht konforme Sicherheitseigenschaften auf der Seite „Härtungs-Compliance-Konfigurationen“ aktualisieren.

Die tägliche Compliance-Punktzahl ist eine prozentuale Punktzahl. Sie basiert darauf, wie konform die aktuellen Einstellungen der Instanzsicherheitseigenschaften mit den im Härtungseinstellungen für die Instanzsicherheitveröffentlichten Compliance-Werten sind.

Überprüfen Sie regelmäßig die tägliche Compliance-Punktzahl Ihrer Instanz. Befolgen Sie diese Richtlinien, wenn Sie Ihre tägliche Compliance-Punktzahl auswerten:

- Größer oder gleich 90 % gibt an, dass die Instanz kritischen Sicherheitskontrollen entspricht.
- Größer oder gleich 50 % und weniger als 90 % weisen auf ein moderates Maß an Sicherheits-Compliance hin.
- Weniger als 50 % weisen auf ein geringes Maß an Sicherheits-Compliance hin.

Passen Sie die Sicherheitseinstellungen der Instanz an, um die Compliance zu erhöhen

Auf der Seite „Härtungs-Compliance-Konfiguration“ können Sie nicht konforme Sicherheitseigenschaften, die sich auf die tägliche Compliance-Punktzahl Ihrer Instanz auswirken, festigen und optimieren. Durch seine Verwendung wird sichergestellt, dass Ihre Instanz den veröffentlichten Sicherheitshärtungsstandards entspricht und gleichzeitig die Sicherheitsanforderungen Ihres Unternehmens erfüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: security_dashboard_user oder admin.

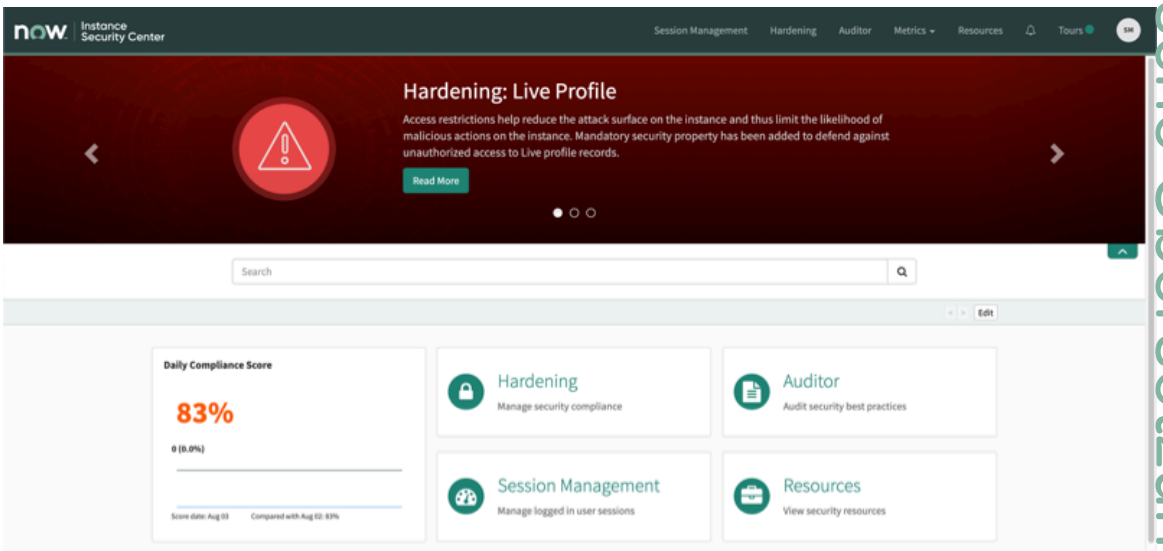
Im Inhalt Härtungseinstellungen für die Instanzsicherheit finden Sie detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform.

- Konsultieren Sie die Härtungseinstellungen für die Instanzsicherheit, wenn Sie sicherheitsbezogene Eigenschaften festlegen oder aktualisieren, auch wenn einige der Compliance-Werte für Ihre Instanz möglicherweise nicht geeignet sind.
- Wenn Sie diese Eigenschaften aktualisieren, stellen Sie sicher, dass sich die Instanz weiterhin wie erwartet verhält. Wenden Sie sich an das zuständige interne Personal, das über das nötige Fachwissen verfügt, um die Sicherheitsauswirkungen zu bestimmen.

Hinweis:
Wenn Sie über eine Administratorrolle verfügen, können Sie Sicherheitskontrollen anzeigen und bearbeiten. Wenn Sie die Rolle security_dashboard_user haben, können Sie Sicherheitskontrollen anzeigen, aber nicht bearbeiten.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**.
2. Klicken Sie auf die Kachel „ **Tägliche Compliance-Punktzahl** “ oder den Link **Härtung**, um auf die Seite „Härtungs-Compliance-Konfiguration“ zuzugreifen.



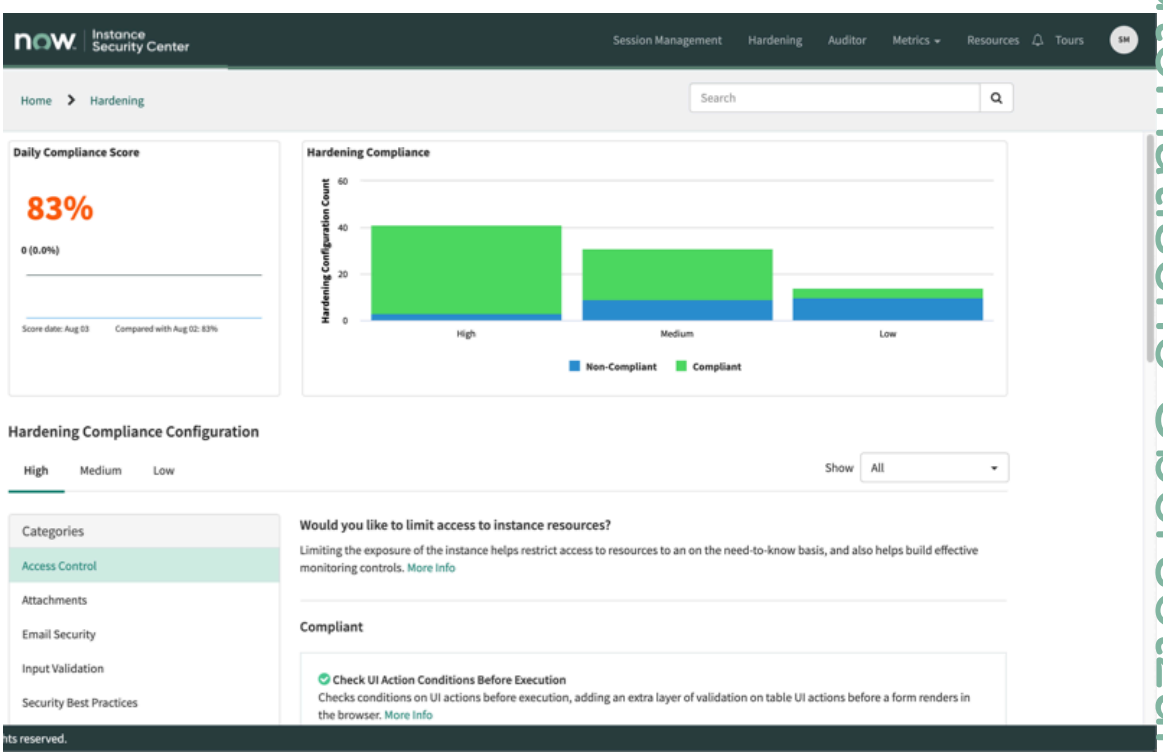
3. Zeigen Sie im Diagramm „Härtungscompliance“ die Statistiken für konforme und nicht konforme Sicherheitskonfigurationseigenschaften an.

Option	Bezeichnung
Konform	Anzahl der Sicherheitskonfigurationseigenschaften, die den Compliance-Werten in den Härtungseinstellungen für Instanzsicherheit entsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Hinweis: Sie können die Einstellungen für konforme Sicherheitseigenschaften in der Härtungs-Compliance-Konfiguration nicht ändern. Wenn Sie dies möchten, müssen Sie sie in den Systemeigenschaften aktualisieren. Weitere Informationen finden Sie unter Systemeigenschaften hinzufügen .
Nicht konform	Anzahl der Sicherheitskonfigurationseigenschaften, die nicht den Compliance-Werten in den Härtungseinstellungen für Instanzsicherheit entsprechen. Sie können die Einstellungen für nicht konforme Eigenschaften aktualisieren.



Hinweis:
Um die Anzahl der konformen oder nicht konformen Sicherheitspunktzahlen für einen bestimmten Datumsbereich anzuzeigen, verschieben Sie den blauen Punkt auf dem Schieberegler unter die tägliche Compliance-Punktzahl.

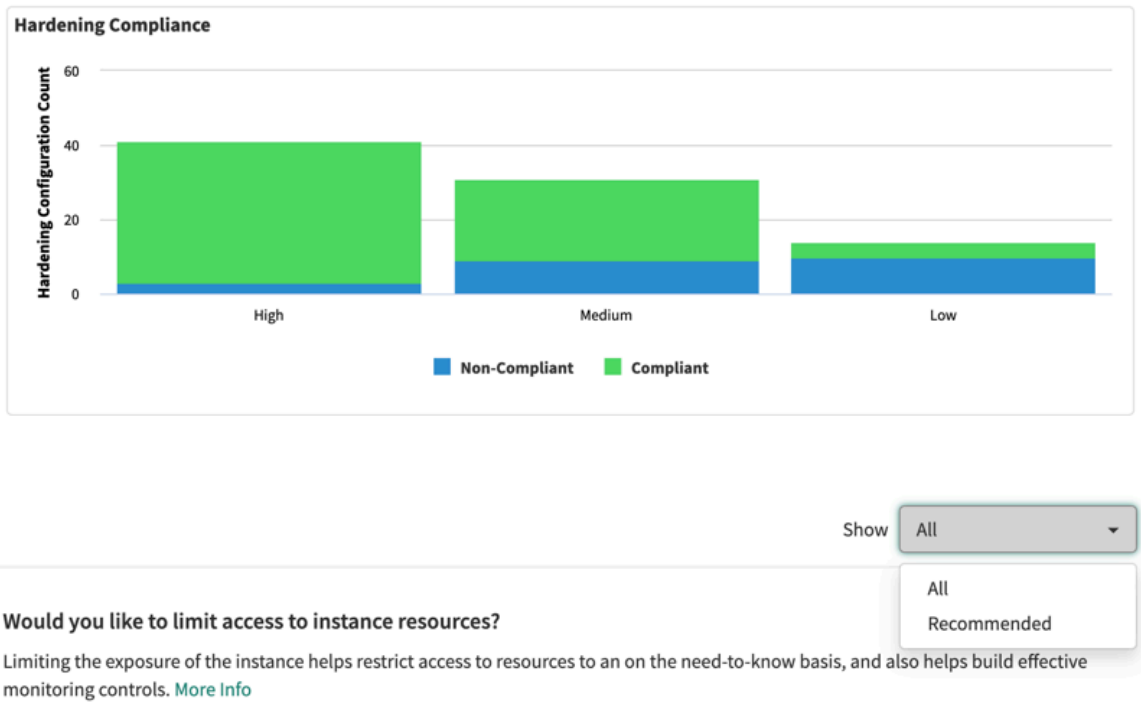
4. **Geben** Sie in der Liste Anzeigen unter dem Diagramm an, ob Sie auf alle oder nur auf empfohlene Sicherheitskonfigurationseigenschaften zugreifen möchten.

Option	Bezeichnung
Alle	(Standard) Alle konformen und nicht konformen Sicherheitskonfigurationseigenschaften in jeder ausgewählten Kategorie.
Empfohlen	In jeder ausgewählten Kategorie werden nur empfohlene Sicherheitskonfigurationseigenschaften ange-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

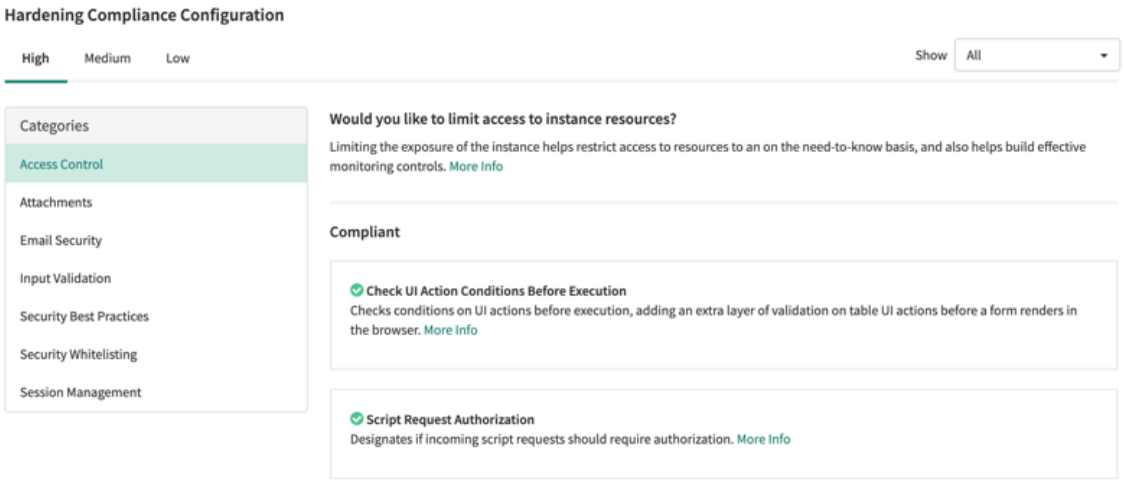
Option	Bezeichnung
	zeigt. Diese Sicherheitskonfigurationseigenschaften sind eine ausgewählte Teilmenge der wichtigsten, die zum Sichern von Now Platformverwendet werden. Betrachten Sie diese Sicherheitskonfigu–rationseigenschaften als die Mindestanzahl von Einstellungen, die Sie zum Sichern von Now Platformfestlegen müssen. **Hinweis:** Um Ihre Instanz vollständig zu sichern, ver-wenden Sie die Option **Alle**. Sie enthält auch alle empfohlenen Sicherheitskonfigurationsei-genschaften.



5. **Wählen**Sie unter Kategorien die Kategorie aus, die die Sicherheitskonfigurationseigenschaften enthält, auf die Sie zugreifen möchten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Option	Bezeichnung
Zugriffssteuerung	Zugriffskontrollen bestimmen, ob Benutzerzugriff auf eine bestimmte Ressource gewährt oder verweigert wird, je nachdem, wer diese Ressourcen verwenden darf. Weitere Informationen finden Sie unter Zugriffssteuerung in den Härtungseinstellungen für die Instanzsicherheit.
Anhänge	Sicherheitskontrollen für Anhänge ermöglichen die Validierung eingehender Anhänge, um Ihre Instanz vor schädlichen Dateien zu schützen, die von Angreifern gesendet werden. Weitere Informationen finden Sie unter Anlagen in den Härtungseinstellungen für die Instanzsicherheit.
E-Mail-Sicherheit	E-Mail-Sicherheit umfasst Sicherheitskonfigurationseigenschaften, die ein Administrator konfigurieren kann, um sicherzustellen, dass für alle eingehenden E-Mails die richtigen Sicherheitsrichtlinien vorhanden sind. Weitere Informationen finden Sie unter E-Mail-Sicherheit (Härtung der Instanzsicherheit) in den Härtungseinstellungen für die Instanzsicherheit.
Eingabevalidierung	Die Eingabevalidierung umfasst sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um die Eingabe fehlerhafter Daten unabhängig von der Quelle zu minimieren. Weitere Informationen finden Sie unter Eingabevalidierung in den Härtungseinstellungen für die Instanzsicherheit.
Sichere Kommunikation	Sichere Kommunikationseigenschaften sind diejenigen, die ein Administrator konfigurieren kann, um die Übertragung von HTTP-Datenverkehr zu sichern. Weitere Informationen finden Sie unter Sichere Kommunikation in den Härtungseinstellungen für die Instanzsicherheit.
Best Practices für Sicherheit	Best Practices für Sicherheit umfassen Sicherheitsaufgaben, die ein Administrator regelmäßig innerhalb eines bestimmten Zeitintervalls ausführen sollte, und zugehörige Konfigurationseigenschaften. Weite-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	re Informationen finden Sie unter Best Practices für Sicherheit in den Härtungseinstellungen für die Instanzsicherheit.
Sicherheitsaufnahmeliste	Die Sicherheitsaufnahmeliste enthält sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um das Verhalten auf bekannte Aufnahmelisten zu beschränken. Weitere Informationen finden Sie unter Sicherheitsaufnahmeliste in den Härtungseinstellungen für die Instanzsicherheit
Management von Benutzersitzungen	Die Sitzungsverwaltung umfasst sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um eine sichere Sitzungsverwaltung in der Now Platformzu gewährleisten. Weitere Informationen finden Sie unter Sitzungsverwaltung in den Härtungseinstellungen für die Instanzsicherheit

6. Konfigurieren Sie die nicht konformen Sicherheitseigenschaften in der ausgewählten Kategorie.
   - Sofern nicht anders angegeben, wird durch Schieben des Schalters auf eine Sicherheitseigenschaft auf die empfohlene Einstellung gesetzt. Beispielsweise legen Sie die meisten Steuerelemente auf „true“ oder „false“ fest, einige erfordern jedoch die Eingabe eines Werts oder von Werten, z. B. eine durch Kommas getrennte Werteliste.
   - Um auf das dedizierte Thema Härtungseinstellungen für Instanzsicherheit für die Sicherheitskontrolle zuzugreifen und mehr darüber zu erfahren, klicken Sie auf **Weitere Informationen**.

Ergebnisse

Die Punktzahl für tägliche Compliance nimmt zu oder ab, je nachdem, welche Änderungen Sie an den nicht konformen Sicherheitskontrolleinstellungen vornehmen.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Wie die Punktzahlen, Trends und Diagrammdaten der täglichen Compliance aktualisiert werden

Trend- und Diagrammdaten im Instanz-Sicherheitszentrum werden aktualisiert, nachdem der Performance Analytics-Auftrag um 02:00 Uhr Ortszeit ausgeführt wurde. Sie wird in der Kachel „Tägliche Compliance-Punktzahl“, in den Event-Menübandkacheln und im Seitendetail Analytics Hub angezeigt, wenn Sie auf eine der Event-Kacheln klicken.

Die tägliche Datenverwaltungsaufgabe [AppSec] ist eine regelmäßig geplante Aufgabe, die jede Nacht ausgeführt wird und die folgenden Aufgaben ausführt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Überprüft, ob den Aufgaben „[AppSec] Tägliche Datenverwaltung“ und „[PA AppSec] Tägliche Datensammlung“ gültige Benutzer zugewiesen wurden, wenn Sie sie zum ersten Mal planen.
   - Wenn Sie einen gültigen Benutzer in das Feld **Ausführen als** eingegeben haben, wird die Verarbeitung des Auftrags fortgesetzt. Ein gültiger Benutzer ist ein Benutzer, der nicht von der Instanz ausgesperrt ist und dem eine Administratorrolle zugewiesen ist.
   - Wenn Sie einen ungültigen Benutzer eingegeben haben, wird eine Fehlermeldung über dem rotierenden Sicherheitsbanner im Instanz-Sicherheitszentrum angezeigt.

   Hinweis:
   Weitere Informationen zum Aktualisieren des zugewiesenen Benutzers beim Ausführen von geplanten Aufgaben finden Sie unter Datenerfassungsaufgaben erstellen oder planen .

2. Führt Geschäftslogik aus, um den Compliance-Status für die Sicherheitseigenschaften festzulegen, die Sie auf der Seite „Härtungs-Compliance-Konfiguration“ konfigurieren. Weitere Informationen finden Sie unter Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften.
3. Führt den Performance Analytics-Auftrag „[PA AppSec] Tägliche Datensammlung“ aus, um Compliance-Daten zu sammeln und die tägliche Compliance-Punktzahl zu aktualisieren.

Tägliche Compliance-Punktzahl manuell aktualisieren

Wenn Ihnen alternativ eine Administratorrolle zugewiesen ist, können Sie die tägliche Compliance-Punktzahl jederzeit aktualisieren und neu berechnen, indem Sie auf Aktualisieren **klicken**.

Hinweis:
Die **Schaltfläche Aktualisieren** wird nicht für Benutzer mit der zugewiesenen Rolle security_dashboard_user angezeigt.

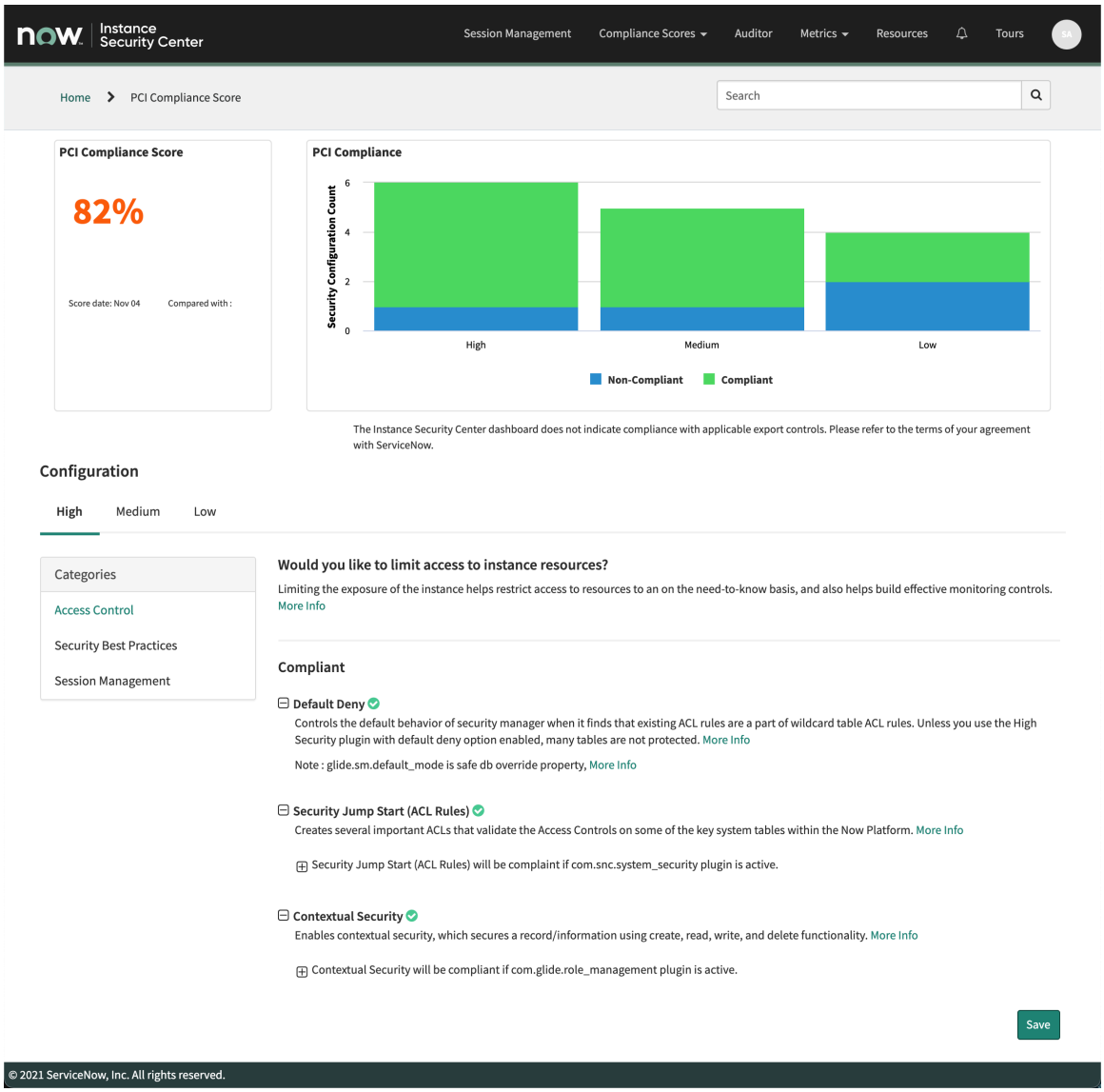
- Die Funktion „Aktualisieren“ führt die gleichen Aufgaben aus wie die Aufgabe „Tägliche Datensammlung“, jedoch in Echtzeit und nicht in einem Batch-Prozess.
- Sie verwenden es normalerweise, wenn Sie Aktualisierungen der täglichen Compliance-Punktzahl durchführen möchten, um die Auswirkungen von Instanzsicherheitsaktivitäten sofort anzuzeigen.
- Es kann eine geringfügige Verzögerung geben, bis die aktualisierte Punktzahl angezeigt wird.

Hinweis:
Wenn Sie ein Upgrade durchführen (z. B. von London auf Washington DC), wird das Plugin „Instance Security Center“ (ISC) automatisch aktiviert. Ein bereitgestelltes Korrekturskript weist automatisch einen benutzerdefinierten Benutzer ohne zugewiesene Rollen zu.

Dashboard „PCI-Compliance-Bewertung“.

Das Dashboard für die PCI-Compliance-Punktzahl zeigt, inwieweit Ihre Instanz den Sicherheitsstandards der Zahlungskartenbranche (PCI) entspricht. Verwenden Sie das Dashboard, um Ihre Compliance-Bewertung anzuzeigen und Ihre Konfiguration zur Verbesserung der Sicherheit zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erforderliche Now Platform-Rollen

security_dashboard_user oder admin, erforderlich zum Anzeigen des PCI-Compliance-Score-Dashboards.

Greifen Sie auf das Dashboard „PCI-Compliance-Punktzahl“ zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**. Klicken Sie im Sicherheitscenter der Instanz im Header auf **Compliance** -Bewertungen, und wählen Sie dann **PCI-Compliance**-Bewertung aus.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Sicherheits-Dashboard-Benutzer (security_dashboard_user)	Überwachen und verwalten Sie die Compliance der Instanzsicherheit kontinuierlich.

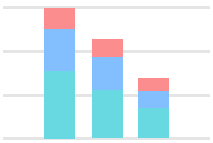
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
Administrator (admin)	Überwachen Sie kontinuierlich die Compliance der Instanzsicherheit, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

Indikator	Beschreibung
PCI-Compliance-Bewertung	Zeigt die Compliance-Punktzahl Ihrer Instanz als Prozentsatz an. Dieser Prozentsatz von stellt den Prozentsatz der Sicherheitskonfigurationen in Ihrer Instanz dar, die die Compliance-Standards erfüllen. Der Indikator zeigt auch das Datum an, an dem die Compliance-Punktzahl berechnet wurde, und einen Vergleich mit der zuvor berechneten Punktzahl.

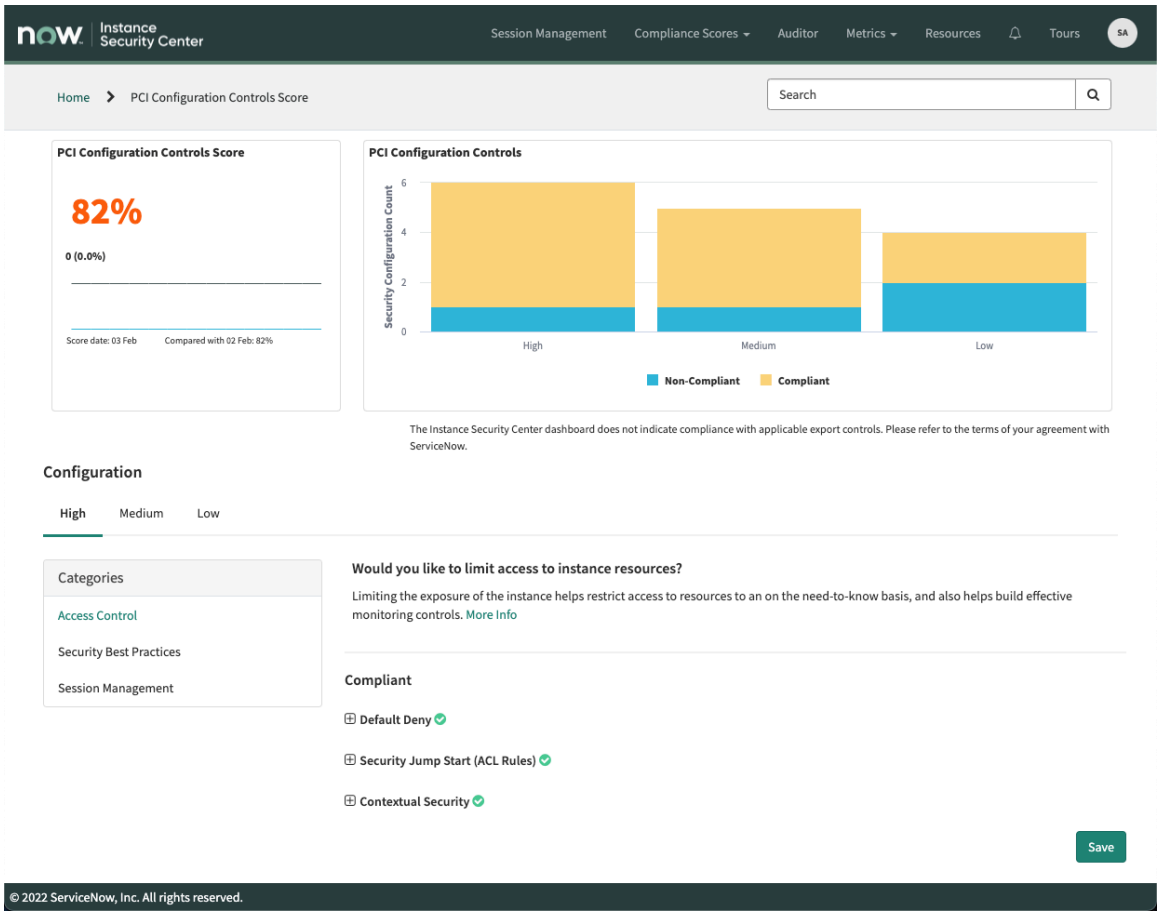
Datenvisualisierung

Titel	Typ	Quelltabelle	Beschreibung
PCI-Compliance	 Stapelbalkendiagramm	Sicherheitskonfigurationen [isc_security_configurations]	Zeigt konforme und nicht konforme Sicherheitskonfigurationen in den Kategorien „Hoch“, „Mittel“ und „Niedrig“ an. Klicken Sie auf einen Bereich des Berichts, um die entsprechenden Sicherheitskonfigurationen anzuzeigen.

PCI-Konfigurationssteuerungen – Punktzahl-Dashboard

Verwenden Sie das Bewertungs-Dashboard der PCI-Konfigurationssteuerungen, um Ihre PCI-Konfiguration zu überprüfen und zu bestimmen, welche Sicherheitsprüfungen nicht konform sind. Sie können die Konfiguration der nicht konformen Sicherheitsprüfungen im Instanz-Sicherheitszentrum ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erforderliche Now Platform-Rollen

Die Rolle security_dashboard_user oder admin ist erforderlich, um das Dashboard für die PCI-Compliance-Punktzahl anzuzeigen.

Greifen Sie auf das Punktzahl-Dashboard der PCI-Konfigurationssteuerungen zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**. Klicken Sie im Sicherheitscenter der Instanz im Header auf **Compliance** -Bewertungen, und wählen Sie dann **PCI-Konfigurationssteuerungspunktzahl**aus.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Sicherheits-Dashboard-Benutzer (security_dashboard_user)	Überwachen und verwalten Sie kontinuierlich die Compliance der PCI-Konfigurationskontrollen in Ihrer Instanz. Ändern Sie die PCI-Konfiguration, um die Compliance sicherzustellen und die Instanzsicherheit zu verbessern.
Administrator (admin)	Überwachen Sie kontinuierlich die Compliance der PCI-Konfigurationskontrollen, um potenzielle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

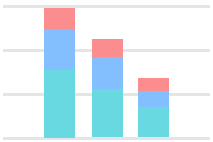
Anwender	Dashboard-Verwendung
	Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

Punktzahl der PCI-Konfigurationssteuerungen

Zeigt die Punktzahl der PCI-Konfigurationssteuerungen Ihrer Instanz als Prozentsatz an. Dieser Prozentsatz von stellt den Prozentsatz der Sicherheits-PCI-Steuerungskonfigurationen in Ihrer Instanz dar, die die Compliance-Standards erfüllen. Der Indikator zeigt auch das Datum an, an dem die Compliance-Punktzahl berechnet wurde, und einen Vergleich mit der zuvor berechneten Punktzahl.

Datenvisualisierung

Titel	Typ	Quelltabelle	Beschreibung
PCI-Konfigurationssteuerungen	 Stapelbalkendiagramm	Sicherheitskonfigurationen [isc_security_configurations]	Zeigt konforme und nicht konforme PCI-Steuerungskonfigurationen in den Kategorien „Hoch“, „Mittel“ und „Niedrig“ an. Klicken Sie auf einen Bereich des Berichts, um die entsprechenden Sicherheitskonfigurationen anzuzeigen.

Suchen Sie nach falschen Sicherheitsdefinitionen

Führen Sie den Auditor aus, um Ihre Instanz zu scannen und falsche Sicherheitsdefinitionen zu finden. Sie enthält Ergebnisse, die Sie korrigieren können, um die Sicherheitslage Ihrer Instanz zu verbessern.

Der Auditor führt eine vollständige Bewertung Ihrer Instanzintegrität durch, bei der Ihre Systemkonfiguration analysiert wird. Bei Sicherheitsscans wird Ihre aktuelle Sicherheitskonfiguration mit Best Practice-Definitionen und Compliance-Werten für Sicherheitseigenschaften verglichen.

Aus Sicht der Instanzsicherheit erhalten Sie Einblicke und Empfehlungen dazu, was Sie tun sollten und wo Sie sich verbessern können. Diese Einblicke und Empfehlungen helfen Ihnen, die folgenden Fragen zu beantworten:

- Sind die entsprechenden sicherheitsbezogenen Eigenschaften festgelegt?
- Ist das Plugin „High Security“ aktiviert?
- Sind die richtigen Zugriffskontrollregeln vorhanden?

Führen Sie den Auditor aus, und analysieren Sie die Scan-Ergebnisse

1. Um den Auditor auszuführen, klicken Sie auf der Homepage des Instanz-Sicherheitszentrums auf **Audit**.
2. Öffnen Sie nach Abschluss Scan-Ergebnisse, um die Sicherheitsergebnisse zu überprüfen und zu analysieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um die Details für ein bestimmtes Scan-Ergebnis zu überprüfen, doppelklicken Sie auf die Ergebnisnummer. Zu diesen Informationen gehören Status, Scan-Typ, Ausführungszeit und Fehlermeldungen.
4. Alle Auditor-Ergebnisse enthalten Lösungsdetails und eine URL zu Produktinhalten, in der erläutert wird, wie sie behoben werden können. Befolgen Sie die dokumentierten Richtlinien, um die Probleme in jedem der Ergebnisse zu beheben.

Zugehörige Informationen

Härtungseinstellungen für die Instanzsicherheit

Hochsicherheits-Plugin

Zugriffskontrolllistenregeln

Überwachen Sie Instanzmetriken

Überwachen Sie Benutzer-, Export-, Authentifizierungs-, E-Mail- und Virenschutzmetriken für Ihre Instanz. Sie können beispielsweise Ihre E-Mail-Sicherheit überwachen, indem Sie Metriken auf Spam, externe E-Mails und eingehende E-Mails aus nicht vertrauenswürdigen und vertrauenswürdigen Domänen für Ihre Instanz überprüfen. Analysieren Sie diese Metriken, um nach anomalem Sicherheitsverhalten zu suchen, das mit Aktivitäten in Ihrer Instanz zusammenhängt.

Benutzermetriken

Analysieren Sie Benutzermetriken, um nach anomalem Verhalten zu suchen, das sich auf bestimmte Arten von Benutzeraktivitäten in Ihrer Instanz bezieht.

Nicht protokolliert Letzter Monat/Letzte sechs Monate/Letztes Jahr

Gibt die Anzahl der Benutzer an, die sich im letzten Monat, in den letzten sechs Monaten und im letzten Kalenderjahr nicht bei der Instanz angemeldet haben. So zeigen Sie Benutzerdetails für eine bestimmte Metrik an:

- Klicken Sie auf die Metrik, um eine Liste der Benutzer anzuzeigen, die sich während des angegebenen Zeitraums nicht bei der Instanz angemeldet haben.
- Klicken Sie auf einen Benutzernamen, um weitere Details zu diesem Benutzer anzuzeigen.

Anwender mit Rollen mit hohen Berechtigungen

Gibt die Anzahl der Benutzer mit den folgenden Rollentypen mit hohen Berechtigungen an:

Benutzerrolle	Beschreibung
Administrator	Primäre Administratorrolle, die unabhängig von Sicherheitsbeschränkungen Zugriff auf alle Systemfeatures, -funktionen und -daten hat.
ais_high_security_admin	Rolle mit erhöhten Berechtigungen, die einem Benutzer den Zugriff auf strenge Sicherheitseinstellungen für KI-Sucheermöglicht. Weitere Informationen finden Sie unter Weisen Sie Rollen zu zu KI-Suche -Administratoren und -Benutzer .
password_reset_admin	Administratorrolle, mit der ein Benutzer den Status von Aktivitäten zum Zurücksetzen des Passworts anzeigen, potenzielle Sicherheitsbedrohungen identifizieren und die Compliance mit Passwortsicherheitsrichtlinien überwachen kann. Weitere Informationen finden Sie unter Passwortzurücksetzung und Passwortänderungsberichte und -protokolle .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerrolle	Beschreibung
script_include_admin	Administratorrolle, die auch Zugriff auf Skripteinbindungen hat.
security_admin	Rolle mit erhöhten Berechtigungen, mit der ein Benutzer Zugriffssteuerungen und Einstellungen für hohe Sicherheit erstellen und ändern kann. Weitere Informationen finden Sie unter Rolle „Security_admin“..
user_admin	Administratorrolle, die auch Benutzer, Rollen, Benutzergruppen, Rollen und Abteilungszuweisungen verwalten kann.

Hinweis:
Weitere Informationen zu diesen administrativen Rollentypen finden Sie unter Spezielle administrative Rollen .

So zeigen Sie Benutzerdetails für eine bestimmte Benutzerrollenmetrik an:

- Klicken Sie auf die Rollenmetrik „Benutzeranzahl“, um eine Liste der Benutzer mit diesem Rollentyp mit hohen Berechtigungen anzuzeigen.
- Klicken Sie auf einen Benutzernamen, um weitere Details zu diesem Benutzer anzuzeigen. Sie können dann bestimmen, ob diese sicherheitskritischen Rollen den richtigen Mitarbeitern zugewiesen sind.

Anwendertrend

Zeigt Informationen zum Anzahltrend über einen Zeitraum für die folgenden Benutzertypen an:

Zähltyp	Beschreibung
Aktive Benutzer	Anzahl der Benutzer, die in der Instanz als aktiv markiert sind
Inaktive Anwender	Anzahl der Benutzer, die in der Instanz als inaktiv markiert sind
Gesperrt	Anzahl der Benutzer, die von der Instanz ausgesperrt sind

So zeigen Sie Benutzerdetails für eine bestimmte Benutzeranzahl an (z. B. ausgesperrte Benutzer):

- Klicken Sie auf die Metrik **Ausgesperrte Benutzer**.
- Klicken Sie auf der Seite Analytics Hub auf **Datensätze**anzeigen.
- Klicken Sie auf einen Benutzernamen, um weitere Details zu diesem Benutzer anzuzeigen. Sie können dann feststellen, ob es einen Grund gibt, warum diese Person ausgesperrt wurde, und die Situation beheben.

Ereignistrend

Zeigt Informationen zum Anzahltrend für bestimmte Arten von Events über einen Zeitraum an:

Ereignistyp	Beschreibung
Administratoranmeldung	Anzahl der Benutzer mit Administratorrollen mit hohen Berechtigungen, die sich an einem bestimmten Tag angemeldet haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignistyp	Beschreibung
Externer Login	Anzahl der Benutzer mit der zugewiesenen Rolle snc_external, die sich während des Kalendertags bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen in der Regel zu Wartungs-, Support-, Beratungs- oder Auditzwecken. Durch die Überwachung dieser Metrik können Sie überprüfen, ob die externen Anmeldeversuche legitim sind und keine potenziellen Sicherheitsprobleme darstellen.
Anmeldung fehlgeschlagen	Anzahl der fehlgeschlagenen Anmeldeversuche an einem bestimmten Tag.
Identitätswechsel	Anzahl der an einem bestimmten Tag angemeldeten Benutzer, die die Identität anderer Benutzer annehmen
Erhöhung der Sicherheit	Anzahl der Fälle, in denen ein Sicherheitsadministrator die Sicherheit für Standardbenutzer erhöht hat, indem die zugewiesene Benutzerrolle während des Kalendertags in eine Sicherheitsrolle mit hohen Berechtigungen geändert wurde. Zu diesen Sicherheitsrollen mit hohen Berechtigungen gehören oauth_admin, admin, security_admin und impersonator.
SNC-Anmeldung	Anzahl der Kundenservice und Support, die sich an einem bestimmten Tag mithilfe der Hi-Hopping-Technik bei dieser Instanz angemeldet haben.

So zeigen Sie Benutzerdetails für eine bestimmte Event-Anzahl an (z. B. Identitätswechsel):

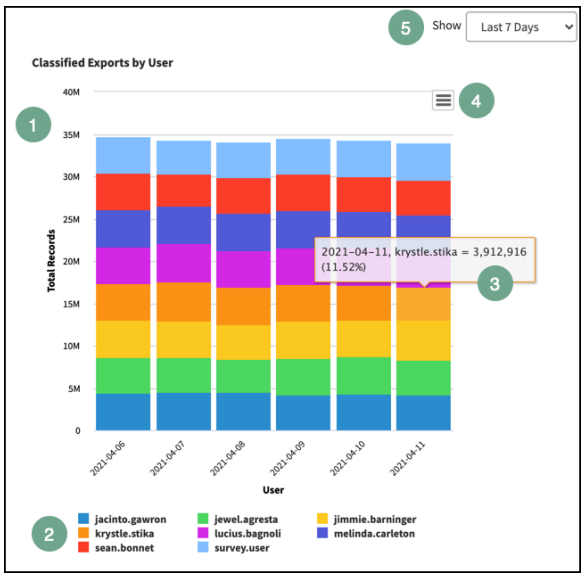
- Klicken Sie auf die Benutzeranzahlmetrik. Auf der Seite „Ereignisprotokolle des Sicherheits-Dashboards“ werden Ereignisprotokolle für diesen Ereignistyp aufgelistet.
- Klicken Sie auf einen Benutzernamen, um weitere Details zu diesem Event anzuzeigen.

Zugehörige Informationen

Analytics Hub

Exportieren Sie Metriken

Analysieren Sie Exportmetriken, um zu sehen, welche Daten am häufigsten exportiert werden und welche Benutzer die meisten Daten exportieren.



1. Exportieren Sie das Diagramm

Jeder Bericht zeigt die Anzahl der Export-Events nach Datum an, wobei ein farbcodierter Schlüssel verwendet wird, um anzugeben, welche Benutzer den Export durchgeführt haben. Klicken Sie auf einen farbigen Abschnitt einer Spalte, um die Liste der **Export** -Event-Datensätze [isc_export_event] anzuzeigen, die diesem Eintrag entsprechen.

2. Berichtsschlüssel

Die Taste am unteren Rand des Berichts gibt an, welche Farben welche Benutzer oder Tabellen identifizieren.

3. Popup-Vorschau

Zeigen Sie auf einen Eintrag im Diagramm, um eine Popup-Vorschau

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

anzuzeigen. Diese Vorschau zeigt den Benutzer- oder Tabellennamen sowie die Anzahl der Exporte und einen Prozentsatz der Gesamtsumme in dieser Spalte.

4. **Image-Export**

   Klicken Sie auf das Symbol, um den Bericht als Bild zu speichern. Sie können den Bericht im PNG- oder JPEG-Format speichern.

5. **Berichtdatumsbereich**

   Verwenden Sie die **Liste** Anzeigen, um Exporte innerhalb der letzten 24 Stunden oder innerhalb der letzten 7 Tage anzuzeigen.

Metrikberichte exportieren

Auf der Seite „Metriken exportieren“ werden vier Berichte angezeigt.

Exporte nach Benutzer

Verwenden Sie den Bericht „ **Exporte nach Benutzer** “, um zu sehen, welche Ihrer Benutzer die meisten Daten exportieren.

Klassifizierte Exporte nach Benutzer

Verwenden Sie den Bericht „ **Klassifizierte Exporte nach Benutzer** “, um zu sehen, welche Ihrer Benutzer die meisten Daten exportieren, die Klassifizierungen wie vertraulich, eingeschränkt oder personenbezogen entsprechen. Administratoren können auf der Registerkarte **Einstellungen** definieren, welche Klassifizierungen dieser Bericht verwendet.

Exportiert nach Tabelle

Verwenden Sie den Bericht „ **Exporte nach Tabelle** “, um zu sehen, aus welchen Tabellen am häufigsten exportiert wird.

Klassifizierte Exporte nach Tabelle

Verwenden Sie den Bericht „ **Klassifizierte Exporte nach Tabelle** “, um zu sehen, welche Tabellen aus am häufigsten exportiert werden, die Klassifizierungen wie vertraulich, eingeschränkt oder personenbezogen entsprechen. Administratoren können auf der Registerkarte **Einstellungen** definieren, welche Klassifizierungen dieser Bericht verwendet.

Hinweis:
Exportmetrikberichte verfolgen nur Export-Events nach. Exporte aus anderen Quellen, z. B. REST-APIs oder Workflows, werden im Rahmen dieser Funktion nicht nachverfolgt.

Exportieren Sie Metrikeinstellungen

Verwenden Sie die Konfigurationsoptionen auf der Registerkarte Einstellungen, um die Berichtsergebnisse einzugrenzen.

Greifen Sie auf die Einstellungen für Ihre Exportmetriken zu, indem Sie auf die Registerkarte **Einstellungen** klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsfelder für Einstellungen

Metrikkonfigurationen exportieren

Konfiguration	Beschreibung
Klassifizierungen für Metriken	Fügen Sie diesem Feld Klassifizierungen hinzu, oder entfernen Sie sie, um zu bestimmen, welche Exporte in den Berichten **„Klassifizierte Exporte nach Benutzer“** und **„Klassifizierte Exporte nach Tabelle** “ enthalten sind. Diese Berichte unterstützen die folgenden Klassifizierungen: • Persönlich identifizierbare Informationen • Vertraulich • Beschränkt • Intern • Öffentlich Weitere Informationen zu Datenklassifizierungen finden Sie unter Datenklassifizierungen
Klassifizierungen für Warnungen	Fügen Sie diesem Feld Klassifizierungen hinzu, oder entfernen Sie sie, um zu bestimmen, welche Exporte Instanzsicherheitsbenachrichtigungen auslösen. Die im Feld **Classifications for Metrics** (Klassifizierungen für Metriken) unterstützten Klassifizierungen werden hier unterstützt. Weitere Informationen zu diesen Warnungen finden Sie im Abschnitt „Sicherheitsbenachrichtigungen“ auf der Seite Instanz-Sicherheitszentrum. Das Feld **Datensatzschwellenwert** definiert die Anzahl der Datensätze, die exportiert werden, bevor Ihre Instanz eine Warnung auslöst.
Datensatzschwellenwert	Anzahl der Datensätze, die ein Benutzer exportieren muss, um eine Warnung auszulösen. Um eine Warnung auszulösen, müssen diese Datensätze auch den Klassifizierungen entsprechen, die im Feld **Klassifizierungen für Warnungen** aufgeführt sind.

Verwenden Sie die Schaltfläche **Speichern** (⌘ **+ s)**, um Ihre Einstellungen zu speichern.

Authentifizierungsmetriken

Analysieren Sie Authentifizierungsmetriken, um Informationen im Zusammenhang mit der Authentifizierung anzuzeigen, z. B. selten verwendete IP-Adressen, fehlgeschlagene Anmeldungen und Arten von Authentifizierungsschemata, die von Ihren Benutzern verwendet werden.

Verwenden Sie die Seite „ **Authentifizierungsmetriken** “, um Berichte zu Ihrer Authentifizierungskonfiguration anzuzeigen. Die folgenden Berichte werden auf dieser Registerkarte angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Seite „Authentifizierungsmetriken“ erfordert das **Plugin „REST API Access Policy“** (com.glide.rest.policy). Weitere Informationen zu dieser Funktion finden Sie unter REST API-Zugriffsrichtlinien.

APIs ohne Authentifizierungsrichtlinien

Zeigt eine Echtzeitanzahl aller APIs ohne Zugriffsrichtlinie an

Härtung: Account-Wiederherstellungs-Flow

Härtung: Einstellung im Zusammenhang mit der rollenbasierten MFA-Funktion

Nur Webservice-Zugriffskonten

Zeigt die Anzahl aller Benutzerdatensätze mit aktivierter Webservice-Zugriffsoption in der Tabelle `User` [sys_user] an.

X509-Zertifikate, die in 30 Tagen ablaufen

Zeigt die Anzahl aller X.509-Zertifikate aus der Tabelle `X.509 Certificates` [sys_certificate] an, die in 30 Tagen ablaufen.

Metriken der adaptiven Authentifizierung

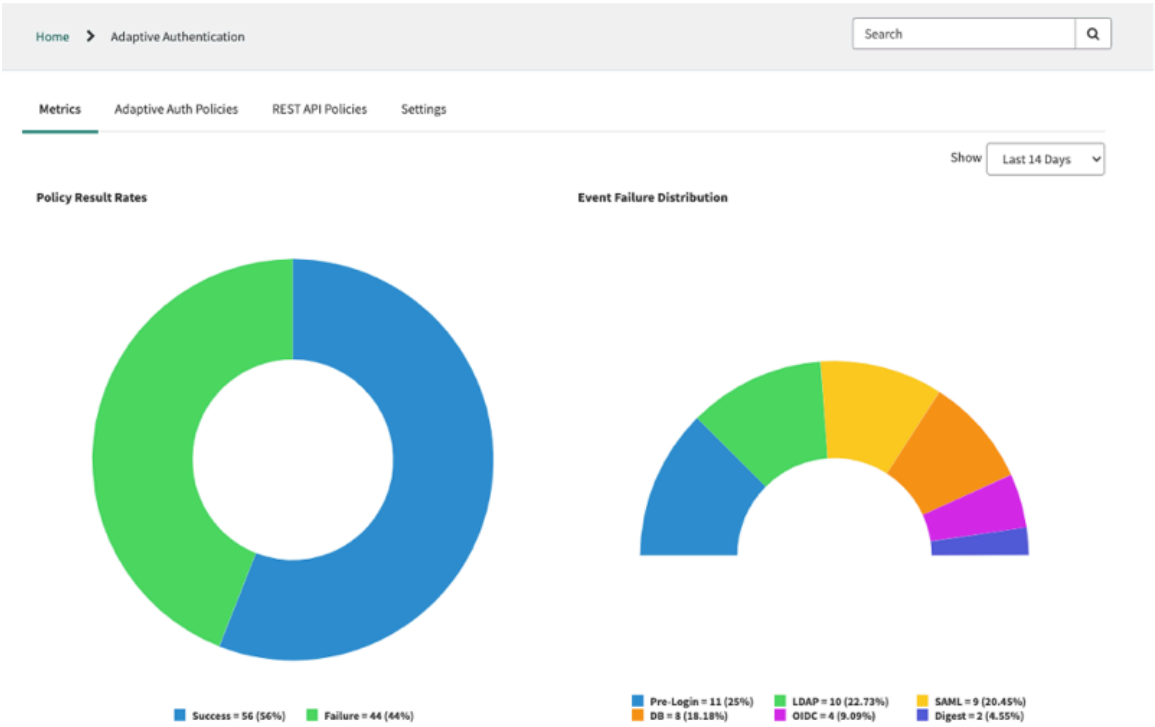
Analysieren Sie Metriken der adaptiven Authentifizierung, um zu überwachen und Einblicke darüber hinzuzufügen, wie die adaptive Authentifizierung in Ihrer Instanz verwendet wird.

Zeigen Sie Berichte, Einstellungen und Richtlinien, die der adaptiven Authentifizierung in zugeordnet sind, vor Ort auf der Seite mit den Metriken der adaptiven Authentifizierung an. Sicherheitsadministratoren können Berichte verwenden, um die Ergebnisse ihrer Richtlinien für adaptive Authentifizierung zu überwachen. Verwenden Sie diese Daten, um Einblicke zu gewinnen und Ihre Richtlinien anzupassen, um ihre Leistung zu verbessern.

Hinweis:
Die Seite mit adaptiven Authentifizierungsmetriken erfordert das Plugin „ **Adaptive Authentifizierung** “ (com.snc.adaptive_authentication). Weitere Informationen zu dieser Funktion finden Sie unter Adaptive Authentifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken



Verwenden Sie die Registerkarte **Metriken**, um Berichte zu Ihrer Konfiguration der adaptiven Authentifizierung anzuzeigen. Die folgenden Berichte werden auf dieser Registerkarte angezeigt.

- Policenergebnisraten
- Ereignisfehlerverteilung
- Verteilung des Ereigniserfolgs
- Abgelehnete IP-Adressen
- Authentifizierung Benutzeranmeldungen
- API-Benutzeranmeldungen
- Authentifizierungstrend

Verwenden Sie die **Liste** Anzeigen, um eine Zeitspanne für die angezeigten Berichte auszuwählen

Adaptive Auth-Richtlinien

Verwenden Sie die Registerkarte „ **Adaptive** Authentifizierungsrichtlinien“, um die Richtlinien für die adaptive Authentifizierung und die Richtlinienkontexte in Ihrer Instanz anzuzeigen. Klicken Sie auf einen beliebigen Eintrag in diesen Listen, um den zugehörigen Datensatz anzuzeigen. Weitere Informationen zu diesen Datensätzen finden Sie unter Adaptive Authentifizierung

Einstellungen

Verwenden Sie die Registerkarte „Einstellungen“, um Systemeigenschaften der adaptiven Authentifizierung anzuzeigen und zu konfigurieren. Weitere Informationen zu diesen Eigenschaften finden Sie unter Eigenschaften der adaptiven Authentifizierung konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Metriken

Analysieren Sie Ihre E-Mail-Metriken, um nach anomalem Verhalten zu suchen, das mit den eingehenden E-Mails in Ihrer Instanz zusammenhängt. Wenn die Metriken beispielsweise eine Spitze bei Spam-E-Mails aus bestimmten Domänen anzeigen, können Sie eingehende Aktionen definieren, die die Zustellung an die Instanz verhindern.

Für jede E-Mail-Metrik wird eine Anzahl für jeden Typ von E-Mail angezeigt, die während des Kalendertags zugestellt oder an die Instanz gesendet wurde.

Benachrichtigungseinstellung	Beschreibung
Externe eingehende E-Mail	Anzahl der eingehenden E-Mails für den Kalendertag, die von externen E-Mail-Domänen an die Instanz übermittelt wurden. **Hinweis:** Die externen E-Mail-Domänen sind die Domänen, die nicht in der Systemeigenschaft `security.list.internal.domains` aufgeführt sind, da diese Eigenschaft nur Ihre internen E-Mail-Domänen nachverfolgt. Weitere Informationen zu dieser Eigenschaft finden Sie unter Verfügbare Systemeigenschaften.
Spam	Anzahl der eingehenden E-Mails für den Kalendertag, die an die Instanz zugestellt und als Spam markiert wurden. Eine Zahl, die nicht mit historischen Trends übereinstimmt, kann darauf hinweisen, dass versucht wird, die Sicherheit Ihrer Instanz zu gefährden.
Vertrauenswürdige eingehende E-Mail	Anzahl der eingehenden E-Mails in der Instanz für den Kalendertag von als vertrauenswürdig eingestuften E-Mail-Domänen.
Nicht vertrauenswürdige eingehende E-Mail	Anzahl der eingehenden E-Mails in der Instanz für den Kalendertag aus E-Mail-Domänen, die als nicht vertrauenswürdig eingestuft wurden. Sie können nicht vertrauenswürdige oder vertrauenswürdige E-Mail-Domänen im Formular „Nicht vertrauenswürdige und vertrauenswürdige Domäne“ festlegen, damit Sie Ihre eingehenden E-Mails nachverfolgen können, die von ihnen gesendet werden. Informationen zum Festlegen nicht vertrauenswürdiger oder vertrauenswürdiger E-Mail-Domänen finden Sie unter Legen Sie E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig fest.

Nachdem Sie auf eine E-Mail-Metrik geklickt haben, können Sie mehr über die möglichen E-Mail-Sicherheitsprobleme in Ihrer Instanz erfahren, indem Sie auf eine der folgenden Optionen klicken:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
Diagramm	Anzahl eingehender E-Mails und Anzahltrends im Zeitverlauf für den ausgewählten E-Mail-Typ (Spam, eingehende externe E-Mails, nicht vertrauenswürdig oder vertrauenswürdig).
Datensätze	Einzelne E-Mail-Datensätze, die die tägliche Anzahl für den ausgewählten E-Mail-Typ beeinträchtigen.
Weitere Informationen	Zusätzliche Informationen für den ausgewählten E-Mail-Typ.

Hinweis:
Die E-Mail-Metriken gelten nur für eingehende E-Mails an die Instanz. Die Metriken gelten nicht für den normalen Datenverkehr, der über Ihre unternehmensweiten E-Mail-Server verarbeitet wird. Weitere Informationen zum Definieren von Aktionen bei eingehender E-Mail und ihren Auswirkungen auf die Verarbeitung eingehender E-Mails finden Sie unter Aktionen bei eingehender E-Mail.

Legen Sie E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig fest

Legen Sie bestimmte E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig fest, damit Sie die Metriken für eingehende E-Mails aus diesen Quellen in Ihrer Instanz überwachen können.

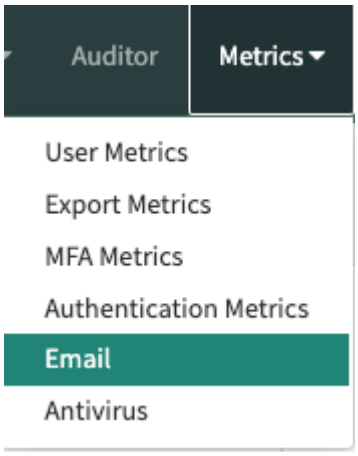
Vorbereitungen
Erforderliche Rolle: security_dashboard_user oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn nicht vertrauenswürdige oder vertrauenswürdige Domänen E-Mails an Ihre Instanz senden, wird deren tägliche Anzahl in den Metriken **Nichtvertrauenswürdige eingehende E** -Mails oder Vertrauenswürdige eingehende E-Mails auf der Seite „E-Mail“ angezeigt. Sie können dann die E-Mail-Aktivität dieser Domänen nachverfolgen und E-Mail-Protokolle verwenden, um bestimmte eingehende E-Mails anzuzeigen. Sie können auch einen Benutzer angeben, in der Regel einen Manager oder einen Sicherheitsanalysten, der benachrichtigt werden soll, wenn Aktivitäten in der nicht vertrauenswürdigen Domäne ausgeführt werden.

Hinweis:
Die Kennzeichnung einer E-Mail-Domäne als nicht vertrauenswürdig dient nur der Sicherheitsnachverfolgung. Administratoren können auch einen Systemadressfilter einrichten, um E-Mails aus nicht vertrauenswürdigen Domänen zu ignorieren. Weitere Informationen zum Filtern von E-Mails, um ihre Zustellung zu blockieren, finden Sie unter Systemadressfilter .

Prozedur
1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**.
2. Wählen Sie auf der Homepage des Instanz-Sicherheitszentrums im Menü „ **Metriken** “ die Option E- **Mail** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

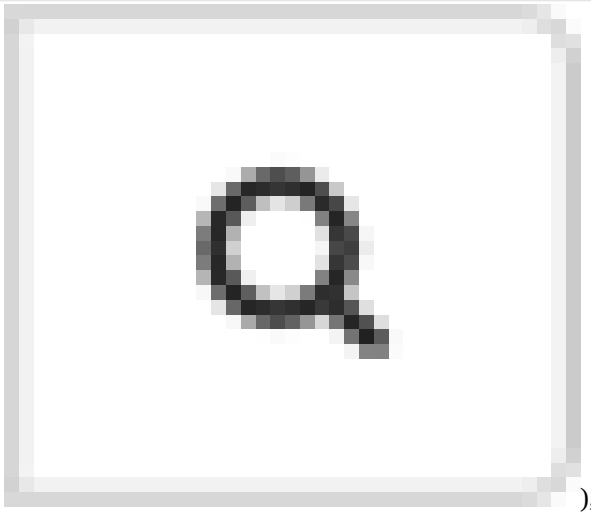


3. Klicken Sie auf der Seite „E-Mail“ im Abschnitt „Nicht vertrauenswürdige und vertrauenswürdige Domänen“ auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Nicht vertrauenswürdige und vertrauenswürdige Domäne“

Feld	Beschreibung
Domäne	Name der E-Mail-Domäne, die Sie als nicht vertrauenswürdig oder vertrauenswürdig festlegen. Geben Sie beispielsweise servicenow.com ein, um anzugeben, dass ServiceNow Mitarbeiter vertrauenswürdige E-Mails an die Instanz senden können.
Kategorie	Kategorie, die angibt, ob die E-Mail-Domäne nicht vertrauenswürdig oder vertrauenswürdig ist: **Nicht vertrauenswürdige** Kennzeichnet die E-Mail-Domäne als nicht vertrauenswürdig. Sie verwenden es, um Domänen zu identifizieren, die verdächtige oder E-Mails senden, die eine potenzielle Sicherheitsbedrohung für die Instanz darstellen. **Vertrauenswürdig** Kennzeichnet die E-Mail-Domäne als vertrauenswürdig. Sie verwenden es, um Domänen zu identifizieren, wenn Ihre Metriken darauf hinweisen, dass die eingehenden E-Mails keine Sicherheitsbedrohungen darstellen. Wenn Sie die Domäne als vertrauenswürdig kennzeichnen, können Sie die Aktivität eingehender E-Mails im Laufe der Zeit nachverfolgen.
Aktiv	Kontrollkästchen zum Aktivieren oder Deaktivieren des festgelegten Status „Nicht vertrauenswürdig“ oder „Vertrauen“ für die angegebene E-Mail-Domäne.
Notify	Name des Benutzers, der per E-Mail benachrichtigt werden soll, wenn Aktivität in der nicht vertrauenswürdigen oder vertrauenswürdigen Domäne auftritt. Klicken Sie auf das Spotlight-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Suchsymbol (), um nach dem Namen des Benutzers zu suchen. Lassen Sie das Feld **Notify** leer, wenn keine Benachrichtigungen gesendet werden sollen.

5. Wählen Sie **Speichern**.

Ergebnisse

Nicht vertrauenswürdige oder vertrauenswürdige E-Mail-Domäneninformationen werden auch der **Liste „Nicht vertrauenswürdige und vertrauenswürdige Domänen“** auf der Seite „E-Mail“ hinzugefügt.

Zugehörige Informationen

Instanz-Sicherheitszentrum

E-Mail-Metriken

Virenschutzmetriken

Wenn das Plugin Antivirus-Scanning aktiviert ist, wird Antivirus-Scanning in Ihrer Instanz ausgeführt, um sie vor Virusinfektionen durch Anhänge zu schützen.

Die folgenden Metriken werden für die letzten 60 Aktivitätstage angezeigt und ermöglichen es Ihnen, die Effektivität der Antivirus-Scanning -Funktionen zu bewerten.

Antivirus-Ereignisse

Antivirus-Ereignisse geben die Anzahl der Antivirus-Ereignisse in Ihrer Instanz nach Datum an. Um auf die Antiviren-Ereignisse zuzugreifen, navigieren Sie zu **Systemsicherheit** > **Instanz-Sicherheitszentrum** und wählen Sie die Registerkarte Metriken aus. Farbcodierte Diagrammlinien stellen die folgenden Arten von Antivirus-Ereignissen dar:

Farbe	Beschreibung
Blau	Anzahl der Dateien, die von Antivirus-Scanning in dieser Instanz für das angegebene Datum unter Quarantäne gestellt wurden.
Grün	Anzahl der infizierten Dateien, die in die Instanz heruntergeladen und dann für das angegebene Datum unter Quarantäne gestellt wurden. Bei diesen Dateien handelt es sich in erster Linie um E-Mail-Anhänge, die einen Virus oder Rouge-Code enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Farbe	Beschreibung
Gelb	Anzahl der unter Quarantäne gestellten Dateien in der Instanz, die für das angegebene Datum gelöscht wurden.
Orange	Anzahl der unter Quarantäne gestellten Dateien in der Instanz, die für das angegebene Datum wiederhergestellt wurden. **Hinweis:** Nachdem Antivirus-Scanning ausgeführt wurde und Falschmeldungen gefunden hat, können Sie eine unter Quarantäne gestellte Datei wiederherstellen und in der Instanz zugänglich machen.

- Um auf die Seite Analytics Hub zuzugreifen und die detaillierte Bewertungsliste und Analyseinformationen für ein bestimmtes Datum anzuzeigen, klicken Sie auf eine farbige Linie im Diagramm „Antivirus-Ereignisse“. Klicken Sie beispielsweise auf die blaue Grafiklinie, um Analyseinformationen für Dateien anzuzeigen, die für ein bestimmtes Datum unter Quarantäne gestellt wurden.
- Um die folgenden Aufgliederungen auf der Seite Analytics Hub anzuzeigen, klicken Sie auf das und dann auf:

Aufgliederung	Beschreibung
AppSec – Antivirus-Ereignisquelle	Quelle des Antivirenereignisses. ○ **Beim Hochladen:** Dies ist auf das Hochladen einer infizierten Datei zurückzuführen, in der Regel eines Anhangs. ○ **Aus Quarantäne:** Dies ist auf die Quarantäne einer infizierten Datei zurückzuführen, in der Regel eines Anhangs. ○ **Beim Download:** Dies ist auf den Download einer infizierten Datei zurückzuführen, in der Regel eines Anhangs. ○ **Aus Datensatz:** Aufgrund eines infizierten Datensatzes in einer Tabelle aufgetreten.
AppSec – Antivirus-Ereignistyp	Typ des Antivirenereignisses. ○ In**Quarantäne:** Dies ist auf die Quarantäne einer Datei zurückzuführen, in der Regel eines Anhangs. ○ **Heruntergeladen:** Tritt aufgrund des Downloads einer Datei auf, normalerweise eines Anhangs. ○ **Wiederhergestellt:** Aufgrund der Wiederherstellung einer unter Quarantäne gestellten Datei aufgetreten. ○ **Gelöscht:** Dies ist auf das Löschen einer unter Quarantäne gestellten Datei zurückzuführen.
AppSec – Antivirus-Uploader	Name des angemeldeten Benutzers, der die Dateien hochgeladen hat, die die Quelle der von der Anwendung Antivirus-Scanning erkannten Virusinfektionen waren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateien in Quarantäne

Listet die infizierten Dateien in der Instanz auf, die von Antivirus-Scanningunter Quarantäne gestellt wurde:

Feld	Beschreibung
Dateiname	Name der infizierten Datei.
Inhaltstyp	Typ des Inhalts, der in der Datei infiziert war Zum Beispiel ist **application/x-dosexec** eine infizierte Anwendung oder ausführbare DOS-Datei, während **text/plain** eine infizierte .txt-Datei ist.
Tabelle	Name der Tabelle, die die infizierte Datei enthält. Beispielsweise wird **Incident** für einen Incident-Dateidatensatz angezeigt.
Virus	Name der von Antivirus-Scanningunter Quarantäne gestellten Datei.
Erkannt	Datum und Uhrzeit der Erkennung der infizierten Datei
Erstellt von	Name des Benutzers, der die infizierte Datei unter Quarantäne gestellt hat.
Erstellt	Datum und Uhrzeit der Erstellung des Quarantänedatei-Datensatzes.
Tabellen-Sys-ID	Tabellensystembezeichner, der dem Quarantänedatei-Datensatz zugewiesen ist.

Hinweis:
Sie können dem Event-Menüband auch Kacheln **„Dateien in Quarantäne“** und „ **Virentypen** “ hinzufügen. Weitere Informationen finden Sie unter Überwachen Sie Sicherheits-Ereignisse und Konfigurieren Sie das Sicherheits-Event-Menüband.

Zugehörige Informationen

- Antivirus-Scanning
- Antivirus-Scanning konfigurieren
- Dateien in Quarantäne werden überprüft
- Antivirenaktivität wird überprüft
- Analytics Hub
- Performance Analytics – Aufgliederungen
- Analytics, Intelligence and Reporting

Dashboard für MFA-Metriken

Das Dashboard für MFA-Metriken zeigt Informationen zur Konfiguration der Multifaktor-Authentifizierung Ihrer Instanzen an. Verwenden Sie das Dashboard, um sicherzustellen, dass Ihre MFA-Konfiguration Ihren Sicherheitsstandards entspricht.

Erforderliche Now Platform-Rollen

security_dashboard_user oder admin, erforderlich zum Anzeigen des PCI-Compliance-Score-Dashboards.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Greifen Sie auf das Dashboard für MFA-Metriken zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**. Klicken Sie im Sicherheitscenter der Instanz im Header auf **Metriken**, und wählen Sie dann **MFA-Metriken**aus.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Sicherheits-Dashboard-Benutzer (security_dashboard_user)	Überwachen und verwalten Sie die Compliance der Instanzsicherheit kontinuierlich.
Administrator (admin)	Überwachen Sie kontinuierlich die Compliance der Instanzsicherheit, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

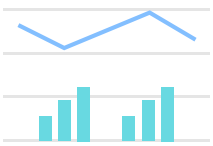
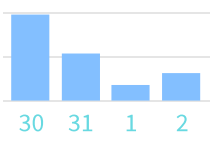
Für MFA registrierte Anwender

Zeigt die Gesamtzahl der Benutzer in der Instanz an, die bei MFA registriert sind. Klicken Sie, um den Analyse-Hub zu öffnen, um weitere Details anzuzeigen.

Benutzer, die die MFA-Umgehung verwenden

Zeigt die Gesamtzahl der Benutzer an, die die MFA-Umgehung verwenden . Klicken Sie, um den Analyse-Hub zu öffnen, um weitere Details anzuzeigen.

Datenvisualisierungen

Titel	Typ	Quelltabelle	Beschreibung
MFA-Anwender mit hohen Berechtigungen			
MFA-Anwendertrend	 Trend		

Aktivieren Sie die ISC-Schnittstelle Virtual Agent .

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „ISC Virtual Agent Conversations“ (com.glide.isc_virtualagent) aktivieren. Durch die Aktivierung dieses Plugins

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden die Inhaltspakete Virtual Agent und Natural Language Understanding (NLU installiert, die Virtual Agent Zugriff über das Instanz-Sicherheitszentrum gewähren.

Vorbereitungen

Die Schnittstelle Virtual Agent im Instanz-Sicherheitszentrum ist nur für Benutzer mit kostenpflichtigen Abonnements von Virtual Agent verfügbar, die das Plugin „Glide Virtual Agent“ (com.glide.cs.chatbot) aktiviert haben. Weitere Informationen finden Sie unter Virtual Agent aktivieren .

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Mit der ISC-Schnittstelle Virtual Agent können Sie die folgenden Aufgaben ausführen:

- Stellen Sie sicherheitsbezogene Fragen, und erhalten Sie dann kurze Antworten und Referenzlinks, um mehr zu erfahren.
- Erhalten Sie Antworten im Zusammenhang mit Instance Security Center, Platform Security, ServiceNow-Sicherheitsrichtlinien, Vertrauen, Governance, Risiko und anderen Prozessen.
- Suchen Sie im Now Support-Sicherheitsportal nach sicherheitsbezogenen Ressourcen, z. B. Knowledge Base-Themen.

Plugins für ISC Virtual Agent

Plugin	Beschreibung
ISC Virtual Agent Konversationen [com.glide.isc_virtualagent]	Aktiviert das Inhaltspaket „ISC Virtual Agent Conversations“ für das Instanz-Sicherheitszentrum.
ISC NLU -[]- Modell für Virtual Agent -Konversationen [com.glide.isc_nlu]	Aktiviert das Inhaltspaket Natural Language Understanding (NLU) für das Instanz-Sicherheitszentrum.

Hinweis:
Durch die Aktivierung des Plugins „com.glide.isc_virtualagent“ wird automatisch „com.glide.isc_nlu“ aktiviert. Wenn Sie jedoch zuerst das Plugin com.glide.isc_nlu aktivieren, müssen Sie auch com.glide.isc_virtualagent manuell aktivieren.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

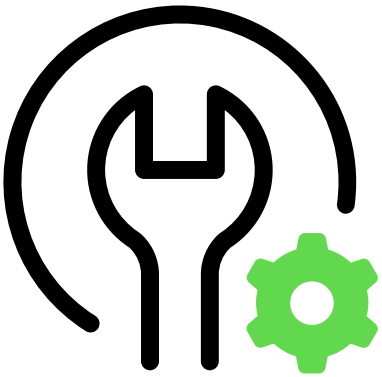
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

   Hinweis:
   Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

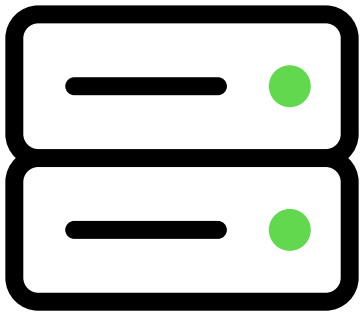
Andere Einstellungen und Sicherheitsressourcen

Dieser Abschnitt enthält Sicherheitseigenschaften, die Sie außerhalb des Instanz-Sicherheitszentrums festlegen, sowie andere sicherheitsbezogene Ressourcen.



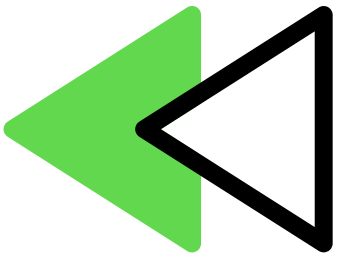
Eigenschaften des Sicherheitssystems

Sicherheitseinstellungen bieten mehrere Eigenschaften, um die Sicherheitsstufe in Ihrer Instanz zu steuern.



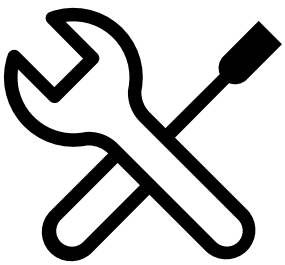
Leitfaden zur MID Server-Bereitstellung

Der MID-Server (ServiceNow Management, Integration, and Discovery) ist eine schlanke Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf Standardhardware ausgeführt wird, einschließlich virtueller Computer.



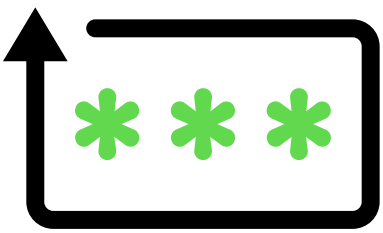
Umkehrbares Verhalten

Es gibt Systemeigenschaften, die entweder als „safe_overrides“ oder „no_db_override“ kategorisiert sind.



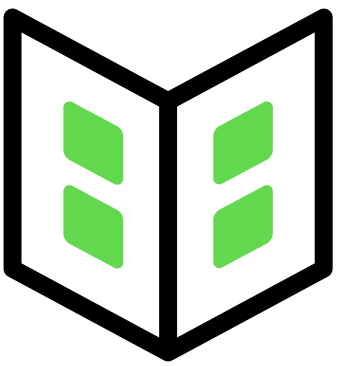
Veraltete Sicherheitseigenschaften

Diese Sicherheitseigenschaften waren in früheren Releases veraltet.



Verwenden der Javascript-Inhaltszugriffssteuerung

Sie können die JavaScript-Inhaltszugriffssteuerung verwenden, um die Liste der blockierten JavaScript-URLs von Drittanbietern in Ihrer Instanz zu ändern.



Andere Sicherheitshärtungsressourcen

Zusätzliche Informationsquellen zur Härtung von Sicherheitskontrollen im Zusammenhang mit der Now Platform.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollierung, Auditing und Fehler (Härtung der Instanzsicherheit)

Wenden Sie eine Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Weitere Informationen darüber, was in der Instanz protokolliert werden kann, finden Sie unter Systemprotokolle. Stellen Sie sicher, dass es einen Zeitplan für die Überwachung von Systemereignissen wie Anmeldungen und fehlgeschlagenen Anmeldungen gibt, indem Sie verwenden **Systemprotokolle** > **Ereignisse**.

SQL-Fehlermeldungen deaktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.db.loguser*, um die Darstellung von SQL-Fehlermeldungen in einem Browser zu deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.db.loguser
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	So deaktivieren Sie die Anzeige von SQL-Fehlermeldungen im Browser.
Typ	Wahr|Falsch
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Dies hat keine Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Mittel) Keine vertraulichen SQL-Informationen, die einem Angreifer helfen könnten, sollten als Teil der Fehlermeldung auf einer Webseite angezeigt werden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Andere Sicherheitshärtungsressourcen

Im Folgenden finden Sie zusätzliche Informationsquellen zur Härtung von Sicherheitskontrollen im Zusammenhang mit Now Platform.

Ressource	Beschreibung
Sicherheitstestportal	Sicherheitsservices-Portfolio auf HI
KB0538598	Penetrationstests für Kundenanwendungen | Richtlinie und Verfahren
KB0546756	Deaktivieren des Zugriffs auf das öffentliche Content Management System (CMS).
KB0550071	ServiceNow, Inc. Überprüfung der Instanzzugriffskontrolle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressource	Beschreibung
KB0550613	IP-Adressbeschränkungen erkennen und aktivieren
KB0550828	Audit und Überprüfung von GlideAjax-Transaktionen
KB0550837	Skript-Sandboxing-Korrektur
KB0551031	Sicherheitskorrektur für die Passwortzurücksetzungs-UI
KB0552835	Fehlerkorrektur für Demo-Benutzerkonten
KB0529232	ServiceNow, Inc. Monitoring – Übersicht und Einblick
KB0564232	Verwenden der Mobile-App ServiceNow, Inc. mit externer Authentifizierung
Sicherheit und Risiko	ServiceNow, Inc. Community

Härtungseinstellungen für die Instanzsicherheit

Der Inhalt „Härtungseinstellungen für Instanzsicherheit“ enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform. Sie können die meisten dieser Eigenschaften auf der Seite „Härtungs-Compliance-Konfiguration“ im Instanz-Sicherheitszentrum festlegen.

Übersicht und Zweck

Das Instanz-Sicherheitszentrum berechnet eine tägliche Compliance-Punktzahl, ausgedrückt als Prozentsatz. Sie basiert darauf, wie konform Ihre aktuellen Instanzsicherheitseinstellungen mit den Compliance-Werten in den Härtungseinstellungen für die Instanzsicherheit sind.

Auf der Seite „Härtungs-Compliance-Konfiguration“ können Sie die spezifischen Sicherheitskonfigurationseinstellungen verwalten, die sich auf die Punktzahl für Ihre Instanz auswirken können. Weitere Informationen zum Sicherstellen, dass Ihre Instanzen die Härtungsanforderungen erfüllen, finden Sie unter:

- Instanz-Sicherheitszentrum
- Passen Sie die Sicherheitseinstellungen der Instanz an, um die Compliance zu erhöhen

Konsultieren Sie die Härtungseinstellungen für die Instanzsicherheit, wenn Sie sicherheitsbezogene Eigenschaften festlegen oder aktualisieren, auch wenn einige der Compliance-Werte für Ihre Instanz möglicherweise nicht geeignet sind. Wenn Sie diese Eigenschaften aktualisieren, stellen Sie sicher, dass sich die Instanz weiterhin wie erwartet verhält. Wenden Sie sich an das zuständige interne Personal, das über das nötige Fachwissen verfügt, um die Sicherheitsauswirkungen zu bestimmen.

Andere Ressourcen

Zur Benutzerreferenz enthält Now Platform ausführliche Informationen zu Konfigurationsfunktionen in der Produktdokumentation. Sie greifen auf die meisten Sicherheitsinhalte über die Links in Instanz sichernzu. Siehe auch:

- Verfügbare Systemeigenschaften
- Eigenschaften der Sicherheitseinstellungen
- Strenge Sicherheitseinstellungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Härtungstabellen für Instanzsicherheit

Sicherheitskonfigurationstabelle

Datensätze in der Tabelle „Sicherheitskonfigurationen“ [isc_security_configurations] enthalten die Details einer Sicherheitskonfiguration. In einem Datensatz finden Sie die Beschreibung einer Konfiguration, ihren Compliance-Status und andere wichtige Details.

Verwenden Sie den Sicherheitskonfigurationsdatensatz, um alle Eigenschaften und Abhängigkeiten anzuzeigen, die Sie konfigurieren müssen, um Ihre Konfiguration an einem Ort konform zu machen.

Im Sicherheitskonfigurationsdatensatz sehen Sie die zugehörigen Sicherheitsabhängigkeits- und Abhängigkeitsgruppendatensätze, die dieser Konfiguration zugeordnet sind.

Tabelle „Sicherheitsabhängigkeiten“.

Datensätze in der Tabelle „Sicherheitsabhängigkeiten“ [isc_security_dependencies] definieren die eingehenden und ausgehenden Kriterien sowie einen empfohlenen Typ. Dieser Typ definiert, wie die Abhängigkeit im Sicherheitscenter der Instanz angezeigt wird.

Tabelle „Abhängigkeitsgruppen“

Verwenden Sie Datensätze in der Tabelle „Abhängigkeitsgruppen“ [isc_dependency_groups], um mehrere Abhängigkeiten zu gruppieren. Alle Abhängigkeiten in einer Gruppe müssen konform sein, damit die Gruppe als konform betrachtet wird.

Zugriffskontrolle (Härtung der Instanzsicherheit)

Zugriffskontrollen bestimmen, ob der Zugriff auf eine bestimmte Ressource gewährt oder verweigert werden soll. Ermöglicht den Zugriff auf Ressourcen nur für die Benutzer, die berechtigt sind, sie zu verwenden.

Autorisierung ist nicht gleichbedeutend mit Authentifizierung, da diese Begriffe und ihre Definitionen häufig verwechselt werden.

- Die Authentifizierung stellt die Identität bereit und validiert sie.
- Die Autorisierung umfasst Ausführungsregeln, die bestimmen, auf welche Funktionen und Daten der Benutzer (oder Prinzipal) zugreifen kann, um die richtige Zuteilung der Zugriffsrechte nach erfolgreicher Authentifizierung sicherzustellen.

Die Autorisierung ist ein Prozess, der nach einer erfolgreichen Authentifizierung ausgeführt wird. Sie können Sicherheitseigenschaften konfigurieren, die festlegen, ob nach der Feststellung, dass ein Benutzer über gültige Anmeldeinformationen verfügt, die einem gut definierten Satz von Rollen und Berechtigungen zugeordnet sind, eine Ressourcenautorisierung erfolgt.

Im Folgenden finden Sie einige Sicherheitskontrollen, die ein Administrator konfigurieren kann, um den nicht autorisierten Zugriff auf vertrauliche Entitäten in Now Platformeinzuschränken.

- Zugriffskontrolllistenregeln
- Konfigurieren einer ACL-Regel
- ServiceNow-Zugriffssteuerung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf skriptfähige GlideSystemUserSession-API

Die vom Client aufrufbare skriptfähige GlideSystemUserSessionSandbox-API stellt die Methoden addErrorMessageNoSanitization und addInfoMessageNoSanitization von GlideSystemUserSession der Javascript-Sandbox bereit. Dadurch können alle Benutzer diese Methode per Skript aufrufen.

Bei Festlegung auf **true**darf eine Sandbox-Benutzersitzung Informationen oder Fehlermeldungen ohne Bereinigung aufrufen. Beim Aufruf der Nachricht wird eine Warnung protokolliert. Bei „ **false"**ist der Anruf nicht zulässig.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sandbox.usersession.allow_unsanitized_messages`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Eigenschaft verhindert, dass nicht bereinigte Informations- oder Fehlermeldungen in einer Sandbox-Benutzersitzung aufgerufen werden.
Typ	wahr | false boolean
Empfohlener Wert	false
Sicherheitsabhängigkeiten	Der Wert für diese Eigenschaft ist eine sichere Überschreibung und kann nach der Änderung nicht mehr geändert werden.
Funktionale Auswirkung	(Hoch) Wenn Sie die Eigenschaft auf den Wert „false" festlegen, werden keine Nachrichten erstellt oder protokolliert, wenn diese Funktionen aufgerufen werden.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Bereinigung kann auf potenziell gefährliche Inhalte zugegriffen werden, und die nicht bereinigte Fehlerfunktion ist für Skripts verfügbar.
Referenzen	Zugriffssteuerung Sichere Überschreibung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für Skriptausführung

Verwenden Sie die Eigenschaft `glide.script_processor.authorized_script_module_role`, um die Verwendung von ausgeführten Skripts aus der Tabelle `„sys_app_module"` auf die definierte Rolle in der Eigenschaft zu beschränken.

Diese Eigenschaft verhindert, dass alle Systembenutzer Skripts aus sys_app_module ausführen, es sei denn, sie haben die in der Eigenschaft angegebene Rolle. Verwenden Sie die Eigenschaft glide.script_processor.authorized_script_module_role, um die Rolle anzugeben, die Skripts ausführen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.script_processor.authorized_script_module_role`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine bestimmte Rolle für die Ausführung eines Skripts aus `sys_app_module anzufordern`.
Empfohlener Wert	Textfeld mit einer durch Kommas getrennten Liste von Rollen.
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Authentifizierung in Form einer Autorisierung durch die definierte Rolle. • Diese Authentifizierung wird während der Verarbeitung von Skriptanforderungen für die Instanz durchgeführt. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für Skriptanforderungen können nicht autorisierte Benutzer auf vertrauliche Inhalte/Daten in der Instanz zugreifen.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Standardauthentifizierung: JSONv2-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.jsonv2`, um anzugeben, ob für eingehende JSONv2-Anforderungen eine Standardautorisierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.jsonv2
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen der Autorisierung von JSONv2-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von JSON-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Benutzer, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter JSONv2-Webservice JSONv2-Webservice .
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung, die für die JSON-Anforderungen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Benutzer auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung Basic Authentication für eingehende JSONv2-Anforderungen anfordern

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Standardauthentifizierung: SOAP-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.soap`, um anzugeben, ob für eingehende SOAP-Anforderungen eine Standardautorisierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.soap
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Autorisierung von SOAP-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Benutzer, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Anmeldeinformationen für SOAP Web Service und MID Server-Authentifizierung und SOAP-Anforderungen.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung, die für die SOAP-Datenquellenanforderungen konfiguriert ist, kann ein nicht autorisierter Benutzer auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

Zugriff für delegierten Entwickler blockieren

Diese Konfiguration wirkt sich auf den Zugriff für delegierte Entwickler aus, die Benutzerrollen über ein Skript aktualisieren. Wenn die Konfiguration konform ist, kann der Entwickler ohne die Rolle user_admin keine Datensätze aktualisieren oder in die Tabelle `sys_user_has_role` einfügen.

Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf. Wenn die Eigenschaft Rollen enthält, können nur diese Rollen Skriptmodule ausführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.sys.security.delegateddev.block_grant_roles`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf.
Typ	Umschalter
Empfohlener Wert	Wahr
Sicherheitsabhängigkeiten	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Hoch) Wenn ein Benutzer mit der Rolle „delegated_developer“ versucht, einen Datensatz in `sys_user_has_role`zu ändern, aktiviert diese Eigenschaft zusätzliche Sicherheitsprüfungen für den Vorgang. Die zusätzlichen Sicherheitsprüfungen überprüfen, ob dem Benutzer die Rolle „`user_admin`“ `zugewiesen` wurde, wenn er versucht, `sys_user_has_role`zu erstellen oder zu aktualisieren. Wenn sie nicht über die Rolle `user_admin` verfügen, wird der Zugriff verweigert. Wenn die Eigenschaft „false“ ist, werden diese zusätzlichen Prüfungen nicht validiert.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung können nicht autorisierte Benutzer auf vertrauliche Inhalte/Daten in der Instanz zugreifen.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Bedingungen der UI-Aktion vor der Ausführung überprüfen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.security.strict.actions`*, um die Überprüfung der Bedingungen für UI-Aktionen in Formularen und Listen zu aktivieren, bevor sie ausgeführt werden. Wenn Sie diese Eigenschaft auf **true**setzen, wird den Tabellen-UI-Aktionen eine zusätzliche Validierungsebene hinzugefügt, bevor sie ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.strict.actions
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine zusätzliche Validierungsebene für die Tabellen-UI-Aktionen sicherzustellen, bevor sie ausgeführt werden.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt nur eine zusätzliche Validierungsebene hinzu, um nach UI-Aktionen in der Zieltabelle/-seite in der Instanz zu suchen. Solange die Zugriffskontrollen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Mittel) Zugriffsanforderung wird immer überprüft, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang validiert alle UI-Aktionen, bevor das Formular für den Endbenutzer gerendert wird.
Referenzen	Hochsicherheits-Plugin

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin „Contextual Security: Role Management“ (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin „Contextual Security: Role Management“ (`com.glide.role_management`), um die kontextbezogene Sicherheit zu aktivieren, die einen Datensatz/Informationen mithilfe der Funktionen zum Erstellen, Lesen, Schreiben und Löschen sichert.

Nach der Installation und Aktivierung werden die Wörterbuchrollen (erstellt von Simple Security Manager) nicht mehr getestet. Stattdessen sucht Now Platform nach ACL-Regeln für Felder und Tabellen. Sie sichert die Daten mithilfe von ACL-Regeln anstelle herkömmlicher, rollenbasierter Dictionary-Regeln, die von einem einfachen Sicherheitsmanager implementiert werden. Auch wenn Sie das Wörterbuchformular konfigurieren und einem Wörterbucheintrag Rollen hinzufügen, werden die Rechte nicht geändert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	com.glide.role_management
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Im Gegensatz zum einfachen Sicherheitsmanager kennt der kontextbezogene Sicherheitsmanager die Systemtabellenhierarchie. Sie können möglicherweise unterschiedliche Sicherheitsregeln für ein Feld haben, je nachdem, wo es in der Hierarchie angezeigt wird.
Empfohlener Wert	Aktiv (Plugin standardmäßig aktiviert)
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Funktionsebene der Zugriffskontrollen, wodurch die Anwendung die Zugriffsbeschränkungen nur basierend auf der ACL-Tabelle bestimmen kann.
Sicherheitsrisiko	(Hoch) Zugriffskontrollen auf funktionaler Ebene müssen vor der Ausführung von CRUD-Vorgängen serverseitig erzwungen werden, um die entsprechende Zugriffsebene für Instanzbenutzer sicherzustellen.
Referenzen	Contextual Security Manager

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin .

Autorisierung von CSV-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.csv`, um anzugeben, ob für eingehende CSV-Anforderungen (Comma-Separated Values) die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.csv

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Basic Authentication für CSV-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von CSV-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen .
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende CSV-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Webservice-Sicherheit

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Standardverweigerung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.sm.default_mode*, um das Standardverhalten des Sicherheitsmanagers zu steuern, wenn festgestellt wird, dass vorhandene ACL-Regeln Teil der ACL-Regeln der Platzhaltertabelle sind.

Wenn das Plugin für hohe Sicherheitseinstellungen (*com.glide.high_security*) während der Erstinstallation der Instanz aktiviert wird, wird diese Eigenschaft erstellt, und Platzhalter-ACL-Regeln werden erstellt. Um rollenbasierten Zugriff auf Systemtabellen bereitzustellen, steuern diese Regeln eine erhebliche Anzahl von ACLs und die häufigsten datensatzbasierten Vorgänge:

- Lesen
- Schreiben
- Erstellen
- Löschen

Wenn Sie das High Security-Plugin nicht mit aktivierter Standardverweigerungsoption verwenden, sind viele Tabellen nicht geschützt. Now Platform verwendet ein standardmäßiges Deny-Sicherheitsmodell, das verhindert, dass Nicht-Administratoren auf -Objekte zugreifen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

es sei denn, sie erfüllen eine übereinstimmende ACL-Regel. Mit diesem Modell werden viele Angriffsvektoren entfernt, z. B. unsichere Skripts.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.sm.default_mode
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Die beste Sicherheitspraxis wäre es, den Zugriff auf die Tabellen durch nicht autorisierte Benutzer einzuschränken. • Wenn keine ACL-Regeln für Tabellen vorhanden sind, stellt diese Eigenschaft sicher, dass mindestens Platzhalter-ACLs für alle CRUD-Vorgänge validiert werden, die für die Tabelle/das Feld ausgeführt werden. • Diese Regeln schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Benutzer hat die Administratorrolle oder erfüllt die Anforderungen einer anderen Tabellen-ACL-Regel.
Empfohlener Wert	verweigern
Funktionale Auswirkung	(Hoch) Wenn Sie diese Eigenschaft auf Zulassen festlegen, **erlauben**die ACL-Regeln der Platzhaltertabelle CRUD-Vorgänge für alle Tabellen, es sei denn, es sind bestimmte Tabellen-ACL-Regeln vorhanden, um solche Vorgänge einzuschränken. **Hinweis:** Dieses Plugin ist nicht für vorhandene Instanzen gedacht, da es den Sicherheitszugriff auf Tabellen ändern kann, die bereits in einer Produktionsumgebung verwendet werden.
Sicherheitsrisiko	(Hoch) Benutzer ohne Administratorrechte können auf Objekte zugreifen, die den ACL-Regeln der Platzhaltertabelle entsprechen.
Referenzen	Standardmäßige Deny-Eigenschaft

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Eingehende Transaktionen noch einmal überprüfen (Instanzsicherheitshärtung)

Die Eigenschaft `glide.security.strict.updates` ermöglicht die doppelte Überprüfung der Sicherheit bei eingehenden Transaktionen während der Formularübermittlung und fügt eine zusätzliche Ebene der Tabellenvalidierung hinzu, bevor ein Formular im Browser gerendert wird. Diese Eigenschaft ist standardmäßig auf „ **true** “ festgelegt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Hinweis:
Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.

Attribut	Beschreibung
Eigenschaftsname	glide.security.strict.updates
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine zusätzliche Überprüfungsebene der Benutzerberechtigungen sicherzustellen, bevor das Formular im Browser angezeigt wird.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur fügt eine zusätzliche Validierungsebene hinzu, um nach Benutzerberechtigungen für die Zieltabelle/-seite in der Instanz zu suchen. Solange die Zugriffskontrollen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Hoch) Sie sollten die Zugriffsanforderung immer überprüfen, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang prüft auf Berechtigungen, wenn das Formular angefordert wird und bevor das Formular gerendert wird.
Referenzen	Eigenschaften der Sicherheitseinstellungen

ACLs aktivieren, um Live-Profildetails zu steuern (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.live_profile.details`, um anzugeben, ob ein Benutzer in der Lage sein soll, alle Detailfelder wie Firmenname und Telefonnummern in einem Live-Profil anzuzeigen.

Abhängig von der Einstellung der Eigenschaft `glide.live_profile.details` geschieht Folgendes:

- Wenn der Wert auf **Anzeigen**festgelegt ist, wird der Zugriff auf die Live-Profilinformationen unabhängig von den für das Benutzerprofil erstellten ACLs gewährt.
- Wenn der Wert auf **ACL**festgelegt ist, ist der Zugriff auf die Live-Profilinformationen gemäß den für das Benutzerprofil erstellten ACLs eingeschränkt.
- Wenn der Wert auf **Ausblenden**festgelegt ist, ist der Zugriff auf die Live-Profilinformationen unabhängig von den für das Benutzerprofil erstellten ACLs eingeschränkt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.live_profile.details
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Der Zweck besteht darin, nur autorisierten Benutzern den Zugriff auf die Details eines Live-Profils (z. B. Firmenname, Telefonnummern) zu ermöglichen.
Empfohlener Wert	Sys-Sicherheits-ACL
Funktionale Auswirkung	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Benutzer auf die Live-Profildetails aller anderen Benutzer zugreifen.
Sicherheitsrisiko	(Mittel) API-Anforderungen sollten Tabellen-ACLs immer berücksichtigen. Die Einschränkung muss angewendet werden, um zu verhindern, dass nicht autorisierte Benutzer auf Details eines Live-Profils zugreifen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktivieren der AJAXGlideRecord-ACL-Überprüfung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.script.secure.ajaxgliderecord*, um eine Validierung der Zugriffskontrollregel (ACL) durchzuführen, wenn auf serverseitige Datensätze, z. B. Tabellen, mit GlideAjax-APIs in einem Client-Skript zugegriffen wird.

Von Client-Skripts ist es möglich, beliebige Daten vom Server abzufragen, indem AJAXGlideRecord () verwendet wird.GlideAjax Client)-API, indem Sie eine Syntax wie einen serverseitigen Glide-Datensatz verwenden. Es ist ein leistungsstarkes und nützliches Tool in vielen Bereitstellungen.

Wenn Sie Zugriffskontrolllisten (ACLs) auf Aufrufe der GlideAjax-API anwenden, können Sie nur Daten abfragen, auf die der aktuell verbundene Benutzer Zugriff hat. Wenn beispielsweise ein ESS-Benutzer angemeldet ist, der keine Rechte zum Lesen der Tabelle „cmn_location“ hat, schlägt ein Aufruf der GlideAjax-API für diese Tabelle fehl.

Wenn Now Platform ohne Überprüfung des Aufrufs der GlideAjax-ACL ausgeführt wird, kann eine API Informationen zurückgeben, auf die der aktuell angemeldete Benutzer andernfalls nicht zugreifen könnte.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.secure.ajaxgliderecord
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Stellt sicher, dass Sicherheits-ACLs auch dann überprüft und validiert werden, wenn auf die Datensätze über clientseitige APIs zugegriffen wird.
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die ACL-Beziehung zu serverseitigen Datensätzen, wenn die Anforderungen mithilfe der AJAXGlideRecord-API-Aufrufe gestellt werden. Wenn die ACL-Konfiguration nicht ordnungsgemäß konfiguriert ist, kann dies Auswirkungen haben. Weitere Informationen zu ihren Auswirkungen und ihrer Identifizierung finden Sie im Artikel Audit and review client-side GlideRecord (AJAXGlideRecord)Transaktionen [KB0550828] im HI Knowledge Base .
Sicherheitsrisiko	(Hoch) Über Client-Skripts ist es möglich, beliebige Daten vom Server über die GlideAjax-API abzufragen. Auf serverseitige Ressourcen kann ohne entsprechende Autorisierung zugegriffen werden. Daher hilft die Verwendung der ACL-Validierung der Anwendung, die Anforderung basierend auf der konfigurierten Autorisierung zu validieren.
Workaround	Stellen Sie sicher, dass die richtigen ACLs für Skripteinbindungen, Prozessoren und andere Entitäten erstellt werden, die von einer GlideAjax-API (AJAXGlideRecord) verwendet werden, damit sie mit der richtigen Autorisierung ausgeführt wird. Implementieren Sie Methoden wie `canRead ()`, `canWrite ()`, `canCreate ()`und `canDelete ()`, um eine Benutzerautorisierung durchzuführen, bevor Sie mit GlideRecord auf Tabellendatensätze zugreifen. Eine andere Methode ist die Verwendung von GlideRecordSecure. Die Klasse wird vom GlideRecord-Server geerbt, der dieselben Funktionen wie GlideRecord ausführt und auch ACLs erzwingt.
Referenzen	ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz) Diese Eigenschaft gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *`glide.script.use.sandbox`*: Siehe vom Client generierte Skripts in der Sandbox. • *`glide.script.allow.ajaxevaluate`*: Siehe AJAXEvaluate aktivieren.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung von Excel-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.basicauth.required.excel`*, um anzugeben, ob für eingehende Excel-Anforderungen die Basic Authentication erforderlich sein soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.excel
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Basic Authentication für Excel-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von Excel-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende Excel-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Plugin „Explicit Role“ (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin „Explicit Role“ (`com.glide.explicit_roles`), um die Instanz mit den neuen Rollen snc_internal und snc_external für B2B- und B2C-Anwendungen bereitzustellen, sodass externe Benutzer nicht auf interne Daten zugreifen können. Enterprise-Benutzer (Mitarbeiter) müssen die interne Rolle haben, während Nicht-Enterprise-Benutzer (keine Mitarbeiter) die externe Rolle haben müssen.

Wenn Sie das explizite Rollen-Plugin installieren:

- Sie weist allen vorhandenen Benutzern die neue Rolle snc_internal zu. Außerdem werden alle Tabellen ohne Rolle mit der Rolle snc_internal zugewiesen.
- Wenn Sie nach der Aktivierung des Plugins „Explicit Role“ einen Benutzer oder eine Tabelle erstellen, weist Now Platform dem Benutzer oder der Tabelle die Rolle snc_internal zu.
- Now Platform verhindert, dass Benutzer mit der Rolle „snc_external“ auf Tabellen zugreifen, denen nicht explizit die Rolle „snc_external“ zugewiesen ist.
- Alle Tabellen mit der öffentlichen Rolle sind sowohl für interne als auch für externe Benutzer zugänglich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Einige Service Portal-Widgets erfordern eine Anmeldung, aber keine bestimmten Benutzerrollen. Nach der Installation des Plugins für explizite Rollen sind diese Portale für externe Benutzer nicht mehr zugänglich.

- ○ Um den Zugriff für externe Benutzer zu ermöglichen, bearbeiten Sie Ihr Widget, um die erforderlichen Rollen von **leer** in **snc_internal, snc_external**zu ändern.
  - ○ Ein Beispiel für dieses Problem sind Kunden, die die Fallverwaltungsanwendung verwenden und benötigen, dass externe Benutzer Dateien an ihre Falldatensätze anhängen können. Wenn Sie die Konfiguration für das Widget „ **encryption-context-auswahl** “ wie beschrieben ändern, können externe Benutzer wie erwartet anhängen.
  - ○ Weitere Informationen zum Konfigurieren von Widgets finden Sie unter Widget-Instanzoptionen konfigurieren

Hinweis:
Verschieben Sie keine System-Update Sets zwischen Instanzen, unabhängig davon, ob das Plugin „Explicit Roles“ aktiviert oder deaktiviert ist. Weitere Informationen finden Sie unter System-Update Sets .

Rollenzusammenfassung

snc_internal

Diese Rolle wird allen internen Benutzern (Mitarbeiter oder Interne einer Organisation) zugewiesen. Alle neuen Benutzer, die hinzugefügt werden, erhalten diese Rolle ebenfalls bei der ersten Anmeldung bzw. beim ersten Identitätswechsel, sofern dem Benutzer die Rolle „snc_external“ nicht bereits zugewiesen ist. Alle vorhandenen Zugriffskontrollregeln (ACLs) ohne Rolle werden mit der Rolle „snc_internal“ gepatcht. Bei neuen ACLs fügt Now Platform diese Rolle automatisch hinzu, wenn die ACL ohne Rolle gespeichert wird.

snc_external

Diese Rolle gibt an, dass der Benutzer außerhalb Ihrer Organisation ist und keinen Zugriff auf Ressourcen haben sollte, es sei denn:

- Sie erlauben den Zugriff über ACLs für die Rolle snc_external oder explizit
- Sie gewähren ihnen explizit zusätzliche Rollen.

Standardmäßig können Benutzer mit der Rolle snc_external nicht auf Ressourcen zugreifen, die keine Datensatztypen sind, z. B. Prozessoren und UI-Seiten.

Öffentlich

Alle Entitäten mit zugewiesener öffentlicher Rolle sind sowohl für snc_internal- als auch für snc_external-Benutzer zugänglich.

Bei Verwendung des Plugins „Explicit Role“:

1. Überprüfen und validieren Sie, dass eine Tabelle mit der öffentlichen Rolle keine vertraulichen Datensätze für externe Benutzer enthält, einschließlich nicht authentifizierter öffentlicher Benutzer.
2. Wenn die Tabelle mit der öffentlichen Rolle vertrauliche Daten enthält und Sie die vertraulichen Datensätze für externe Benutzer einschränken möchten, gilt Folgendes:
   - ○ Entfernen Sie die öffentliche Rolle aus der Tabelle oder
   - ○ Fügen Sie der Tabelle zusätzliche geskriptete ACL hinzu.
3. Überprüfen und validieren Sie, ob alle Endpunkte, z. B. die Scripted REST APIs, *`GlideRecordSecure`* verwenden, oder überprüfen Sie Rollen explizit mit `canRead()`, `canWrite()`, `canUpdate()`und `canDelete()`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.explicit_roles
Konfigurationstyp	Systemdefinition > Plugin
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Um zu verhindern, dass externe Benutzer auf interne Daten zugreifen.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Keine nennenswerten Auswirkungen, da das Plugin die Rolle „snc_internal“ automatisch der Tabelle zuweist, sodass die vorhandenen internen Benutzer weiterhin den erforderlichen Zugriff haben.
Sicherheitsrisiko	(Hoch) Externe Benutzer (keine Mitarbeiter) können auf viele vertrauliche Tabellen in Now Platform zugreifen, denen keine Rollen zugewiesen sind. Sie sollen nur für interne Benutzer (Mitarbeiter) zugänglich sein.
Referenzen	Explizite Rollen

Schritte zum Konfigurieren von

Beim Erstellen einer Funktion oder Anwendung mit den expliziten Rollen:

1. Erstellen Sie eine Rolle, die die Rolle snc_external für Ihre neue Funktion oder Anwendung übernimmt.
2. Entfernen Sie beim Erstellen eines externen Benutzers die Rolle „snc_internal“, und fügen Sie die neu erstellte Rolle hinzu, die die Rolle „snc_external“ erbt.
3. Wenn Sie der vorhandenen Tabelle die neue Rolle hinzufügen, die die Rolle „snc_external“ übernimmt, überprüfen und validieren Sie, dass die Tabelle keine vertraulichen Datensätze enthält.
4. Überprüfen Sie beim Erstellen einer Tabelle, ob nur autorisierte interne und externe Benutzerrollen auf die Tabelle zugreifen können.
5. Verwenden Sie beim Erstellen von Endpunkten wie der Scripted REST API GlideRecordSecure, oder überprüfen Sie Rollen explizit mit `canRead()`, `canWrite()`, canUpdate() und `canDelete()`.

Stellen Sie beim Erstellen einer Tabelle mit der öffentlichen Rolle sicher, dass die Tabelle keine vertraulichen Datensätze für externe Benutzer enthält, einschließlich nicht authentifizierter öffentlicher Benutzer.

Autorisierung von Importanforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.basicauth.required.importprocessor`*, um anzugeben, ob für eingehende Importanforderungen die Basic Authentication erforderlich sein soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.importprozessor
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Basic Authentication für Importanforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird beim Importieren von Datenquellen in die Instanztabellen/-seiten durchgeführt. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung, die für die Datenquellen-Importanforderungen konfiguriert ist, kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	SOAP-Webservices Sicherheit SOAP-Webservice

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

Autorisierung von PDF-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.pdf*, um anzugeben, ob für eingehende PDF-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.pdf
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	So erzwingen Sie die Basic Authentication für PDF-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von PDF-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Webservice-Importsätze .
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende PDF-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Leistungsüberwachung (ACL) (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.security.diag_txns_acl*, um den Zugriff auf „stats.do“, „threads.do“, „thread_pool_stats“ und „replication.do“ über eine nicht authentifizierte Verbindung zu steuern.

Wenn Sie diese Eigenschaft auf **true**festlegen, ermöglicht die Eigenschaft *glide.security.diag_txns_acl* nur dem Administratorkonto den Zugriff auf Folgendes:

- https://<instancename> .servicenow.com/stats.do
- https://<instancename> .servicenow.com/threads.do
- https://<instancename> .servicenow.com/replication.do
- https://<instancename> .servicenow.com/thread_pool_stats.do

Ohne diese Einstellung zu aktivieren, ist es weiterhin möglich, über eine nicht authentifizierte Verbindung auf diese Ressourcen zuzugreifen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.diag_txns_acl
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Beschränken Sie den Zugriff auf Konfigurationsseiten nur auf das Administratorkonto
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt, dass nur der Administratoraccount zu Protokollierungs- und Fehlerbehebungszwecken Zugriff auf vertrauliche Anwendungsdaten erhält.
Sicherheitsrisiko	(Niedrig) Vertrauliche Daten wie Serverdetails, Threads und auf dem Server ausgeführte Prozesse sollten für Endbenutzer ohne entsprechende Berechtigungen niemals sichtbar oder zugänglich sein.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Leistungsüberwachung IP-Einschränkung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.custom.ip.authenticate.allow`, um nur einer angegebenen kommagetrennten Liste oder einem Bereich von IP-Adressen den Zugriff auf die Seiten „stats.do“, „threads.do“ und „replication.do“ zu ermöglichen. Wenn diese Eigenschaft nicht aktiviert ist, ist der Zugriff auf diese Seitentypen von jeder IP-Adresse möglich.

Hinweis:
Basierend auf einigen kürzlichen Änderungen muss die IP-Adresszugriffssteuerung für alle IP-Einschränkungen verwendet werden. Weitere Informationen finden Sie im Abschnitt „Schritte zur Konfiguration“ in Zugriff auf bestimmte IP-Bereiche beschränken.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.custom.ip.authenticate.allow
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Beschränken Sie den Zugriff nur auf Konfigurationsseiten für die IP-Adressen in der Aufnahmeliste.
Empfohlener Wert	Kommagetrennte Liste der IP-Adressen.
Funktionale Auswirkung	(Niedrig) Auf Seiten mit vertraulichen Informationen kann auch von einer nicht vertrauenswürdigen IP-Adresse aus zugegriffen werden.
Sicherheitsrisiko	(Niedrig) Unnötige Gefährdung der Zielinstanz im Internet sollte mithilfe der IP-Zugriffssteuerungsfunktionalität eingeschränkt werden.
Referenz	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz für vom Client aufrufbare Skripteinbindungen (Härtung der Instanzsicherheit)

Standardmäßig sind vom Client aufrufbare Skripteinbindungen, die die Sichtbarkeit nicht explizit festlegen, öffentlich. Fügen Sie bei Bedarf die Eigenschaft *glide.script.ccsi.ispublic* hinzu, um die Datenschutzsteuerung für alle vom Client aufrufbaren Skripteinbindungen zu aktivieren, auf die von öffentlichen Seiten zugegriffen wird.

Wenn Sie diese Eigenschaft hinzufügen, müssen Sie ihren Wert auf **false**festlegen, was angibt, dass alle vom Client aufrufbaren Skripteinbindungen privat sind, und ihre Sichtbarkeit auf öffentlichen Seiten ändert.

Hinweis:
Sie können die Eigenschaft nicht mit dem Wert **true**hinzufügen oder ihren Wert von **false** in **true**ändern. Wenn Sie dies versuchen, wird eine Fehlermeldung angezeigt.

Bei Bedarf können Sie die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion isPublic() hinzufügen.

- Die Einstellung isPublic() hat Vorrang vor der Eigenschaft *glide.script.ccsi.ispublic*.
- Wenn Sie beispielsweise isPublic() in einem einzelnen Skript auf „ **true** “ festlegen, wird es öffentlich gemacht, wodurch die Eigenschaft *glide.script.ccsi.ispublic* überschrieben wird, die alle anderen vom Client aufrufbaren Skripteinbindungen privat macht.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.ccsi.ispublic
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Wenn Sie vom Client aufrufbare Skripteinbindungen privat machen, können Gäste, die auf öffentliche Seiten zugreifen, nicht auf die vom Client aufrufbaren Skripteinbindungen zugreifen. Ein nicht angemeldeter Benutzer kann kein privates Skript ausführen.
Empfohlener Wert	false
Funktionale Auswirkung	(Hoch) Wenn die vom Client aufrufbaren Skripteinbindungen als öffentlich gekennzeichnet sind (d. h. diese Eigenschaft fehlt), können nicht authentifizierte Benutzer Client-Skripts ausführen. Fügen Sie die Eigenschaft hinzu, die die Ausführung von Skripts durch einen nicht angemeldeten Benutzer einschränkt.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft nicht hinzufügen, umgehen clientseitige Skripteinbindungen ACLs, was zu unbeabsichtigten öffentlichen Funktionen führen kann. Wenn das Client-Skript vertrauliche Informationen bereitstellt, kann dies ein nachteiliges potenzielles Sicherheitsrisiko darstellen.
Workaround	Wenn Sie die Eigenschaft *glide.script.ccsi.ispublic* auf „ **false** “

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	setzen, werden alle vom Client aufrufbaren Skripteinbindungen privat. Sie können die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion `isPublic()` hinzufügen. Die Funktion `isPublic` hat Vorrang vor der Eigenschaft *`glide.script.ccsi.ispublic`*. Fügen Sie der Skripteinbindung die folgende Syntax hinzu: `isPublic:function(){return[true/false];},`

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Öffentlicher Zugriff auf Favoriten

Verwenden Sie *`glide.ui.magellan.favorites.allow_public`*, um anzugeben, ob nicht authentifizierte Benutzer **Favoriten** im Navigator anzeigen dürfen.

Öffentlicher Zugriff auf Favoriten ist konform, wenn *`glide.ui.magellan.favorites.allow_public`* auf „ **falsch**“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*`glide.ui.magellan.favorites.allow_public`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Steuern Sie, ob nicht authentifizierte Benutzer **Favoriten** im Navigator anzeigen dürfen.
Typ	wahr/falsch
Empfohlener Wert	*`false`*
Sicherheitsabhängigkeiten	Legen Sie *`glide.ui.magellan.favorites.allow_public`* auf **false fest**.
Funktionale Auswirkung	(Mittel) Die Aktivierung dieser Eigenschaft dient als Schutzschicht vor nicht autorisierten Benutzern.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Favoriten erstellen oder anzeigen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf bestimmte IP-Bereiche beschränken (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `com.snc.ipauthenticator`, um den Zugriff auf bestimmte IP-Bereiche einzuschränken. Sofern kein öffentlicher Zugriff für die Instanz vorgesehen ist, sollten Administratoren den Zugriff auf die ihnen zugewiesenen IP-Netzblöcke beschränken.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, müssen Sie das Plugin „IP Range Based Authentication `com.snc.ipauthenticator` “ aktivieren. Weitere Informationen finden Sie unter IP-Bereichsbasierte Authentifizierung und im Abschnitt „Schritte zum Konfigurieren“ (unten).

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.snc.ipauthenticator
Konfigurationstyp	Systemsicherheit > IP-Adresszugriffssteuerung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So fügen Sie den IP-Adressbereich, der auf die Instanz zugreifen kann, den Listen der vertrauenswürdigen und nicht vertrauenswürdigen Domänen hinzu.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Vom Kunden verweigerte IP-Bereiche werden für dieses Korrekturelement verwendet. Keine Auswirkung, da der Kunde die Zielliste definiert.
Sicherheitsrisiko	(Niedrig) Unnötige Gefährdung der Zielinstanz im Internet sollte mithilfe der IP-Zugriffssteuerungsfunktionalität eingeschränkt werden.
Referenzen	IP-Bereichsbasierte Authentifizierung

Schritte zum Konfigurieren von

1. Stellen Sie sicher, dass das Plugin „com.snc.ipauthenticator“ aktiv ist.
2. Navigieren zu **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung**.
3. Klicken Sie auf **Neu**, um eine Ausschlussliste (Deny) oder eine Aufnahmeliste (Allow) von IP-Adressen zu erstellen.
4. Klicken Sie auf **Absenden**.

Autorisierung von RSS-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.rss`, um anzugeben, ob für eingehende RSS-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.rss

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Basic Authentication für RSS-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird während der Verarbeitung von RSS-Anforderungen für die Instanz durchgeführt. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter RSS-Feed-Generator.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende RSS-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	RSS-Basic Authentication

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

SSO-Profil für SAML 2.0-Webbrowser (Härtung der Instanzsicherheit)

Das Plugin *com.snc.integration.sso.saml20.update1* stellt sicher, dass der Status des SAML 2.0 Single Sign-On-Plugins aktiv ist.

Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen. SAML tauscht Sicherheitsinformationen zwischen einem Identitätsanbieter (Ersteller von Assertionen) und einem Service Provider (Verbraucher von Assertionen) aus.

Das Plugin *com.snc.integration.sso.saml20.update1* ist ein erforderliches Plugin, Sie müssen es jedoch nicht manuell aktivieren. *sso.multi.installer* installiert alle erforderlichen SAML-bezogenen Plugins und enthält außerdem saml2-Implementierungsskripts, die Optionen für die Antwortvalidierung bereitstellen. Weitere Informationen finden Sie in den Themen unter Referenzen in Weitere Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.snc.integration.sso.saml20.update1 (neu)
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Schutz vor websiteübergreifenden Skripting-Angriffen.
Empfohlener Wert	Aktiv
Erforderliche Rolle	Ihr Administrator kann das Plugin nicht aktivieren. Fordern Sie die Person mit erhöhten Sicherheitsberechtigungen auf, sie in der Instanz zu aktivieren.
Referenzen	Authentifizierung mit SAML- SAML Integration Aktualisieren Sie Ihre vorhandene SAML 2.0-Integration

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin .

Autorisierung von Skriptanforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.scriptedprocessor`, um anzugeben, ob für eingehende Skriptanforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.scriptedprocessor
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Basic Authentication für Skriptanforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Authentifizierung in Form der Standardautorisierung. • Diese Authentifizierung wird während der Verarbeitung von Skriptanforderungen für die Instanz durchgeführt. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende Skriptanforderungen greift ein nicht autorisierter Benutzer auf vertrauliche Inhalte/Daten in der Zielinstanz zu.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sicherheits-Jump-Start (ACL-Regeln) (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin „Security Jump Start (ACL Rules)“ (`com.snc.system_security`), um mehrere wichtige ACLs zu erstellen, die die Zugriffskontrollen für einige der wichtigsten Systemtabellen in Now Platformvalidieren.

Diese Regeln bieten eine Starthilfe für die Sicherung vieler Systemtabellen und erleichtern es einer Organisation, eine Instanz in die Produktion zu bringen. Das Plugin „Security Jump Start (ACL Rules)“ wird automatisch auf allen neuen Instanzen installiert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	com.snc.system_security
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Aktivieren Sie das Plugin Security Jump Start (ACL Rules), um eine ordnungsgemäße Sicherheits-Compliance zu erreichen. Sie bietet einige grundlegende ACLs, die Systemtabellen an erster Stelle sichern, anstatt für jede Systemtabelle, die mit der Standardbereitstellung einer Instanz einhergeht, manuell erstellt zu werden. Diese ACLs sind hilfreich, wenn die neu erstellte Instanz schnell in die Produktion gehen muss.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Mittel) Es gibt erhebliche funktionale Auswirkungen, wenn dieses Plugin ohne Audit der vorhandenen ACLs in der Instanz installiert wird. Kundenkontakt und Definitionen sind erforderlich, bevor die Fehlerkorrektur erfolgen kann.
Sicherheitsrisiko	(Hoch) Die Zugriffskontrolle sollte erzwungen werden, um den unbeabsichtigten Zugriff auf die Instanz zu sperren. ACL-Jumpstart-Regeln wurden erstellt, um einen Ausgangspunkt für die Sicherung vieler Systemtabellen zu bieten, damit eine Organisation schnell in die Produktion gehen kann.
Referenzen	Sicherheits-Jump-Start – ACL-Regeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritte zum Konfigurieren von

Wenn dieses Plugin in Ihrer Instanz nicht aktiviert ist, wenden Sie sich an den ServiceNow. Wenn Sie das Plugin zu diesem Zeitpunkt aktivieren, kann dies den Sicherheitszugriff auf Tabellen ändern, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die das Plugin bereitstellt, können Sie bei Bedarf eine oder mehrere davon manuell in einer vorhandenen Instanz erstellen. Diese Liste von ACLs kann in diesem Fall als Leitlinie verwendet werden.

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin .

SNC Access Control-Plugin (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin „SNC Access Control“ (`com.snc.snc_access_control`), um den Zugriff auf Ihre Instanzen durch Mitarbeiter von Kundenservice und Support zu steuern.

Die Standardkonfiguration für Now Platform ermöglicht dem Kundenservice und dem Support den Zugriff auf -Instanzen über einen internen Prozess, der Anmeldeinformationen für den kurzfristigen Support erstellt. Obwohl jeder Zugriff geprüft wird, ziehen es einige Kunden vor, diesen Zugriff zu steuern.

Mit diesem Plugin kann der Kundenadministrator Kundenservice und Support Mitarbeitern den Zugriff auf die Instanz verweigern. Diese Entscheidung wirkt sich auf Support-SLAs aus, da Sie den Zugriff Now Platform aktivieren müssen, bevor Support-Aktivitäten beginnen können. Weitere Informationen finden Sie unter ServiceNow-Zugriffssteuerung.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.snc.snc_access_control
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verbietet Kundenservice und Support Mitarbeitern den Zugriff auf die Instanz
Empfohlener Wert	Aktiv
Erforderliche Rolle	Der Kundenadministrator kann dieses Plugin nicht aktivieren. Es muss explizit angefordert werden, da es erhöhte Berechtigungen erfordert, um das Plugin zu aktivieren.
Funktionale Auswirkung	(Niedrig) Wenn dieses Plugin inaktiv ist, können alle Kundenservice und Support Mitarbeiter auf die Instanz des Kunden zugreifen. Durch die Aktivierung des Plugins kann der Kunde den Zugriff auf autorisierte Kundenservice und Support Mitarbeiter beschränken.
Sicherheitsrisiko	(Niedrig) Unnötige Offenlegung des Instanzzugriffs für eine breitere Gruppe von Personen.
Referenzen	ServiceNow-Zugriffssteuerung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritte zum Konfigurieren von

1. Führen Sie die Schritte in ServiceNow Zugriffssteuerung wird aktiviertaus, um das Plugin anzufordern. Kunden müssen das Plugin „SNC Access Control“ (com.snc.snc_access_control) von HI anfordern.
2. Führen Sie die Schritte in ServiceNow Zugriffssteuerung konfigurierenaus, um die SNC-Zugriffssteuerung zu aktivieren. Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere Kundenservice und Support Mitarbeiter anzugeben, die berechtigt sind, sich bei Ihrer Instanz anzumelden.

Überprüfung des SOAP-Inhaltstyps (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.soap.require_content_type_xml`*, um die Validierung eines Inhaltstyps als text/xml zu aktivieren und vor ungültigen SOAP-Anforderungen zu schützen.

- Bei Festlegung auf **true**validiert Now Platform den Inhaltstyp als text/xml und schützt vor ungültigen SOAP-Anforderungen.
- Bei **false**ist jeder Inhaltstypwert zulässig.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.soap.require_content_type_xml
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schutz vor ungültigen SOAP-Anforderungen
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur ermöglicht die Validierung des SOAP-Inhaltstyps für alle eingehenden SOAP-Anforderungen. • Wenn Sie für eingehende Anforderungen einen anderen Inhaltstyp als Text/XML verwenden, kann dies zu einem potenziellen Fehler bei SOAP-Transaktionen führen. • Wenn Sie nicht den richtigen MIME-Typ verwenden, kann dies die Integration von Drittanbietern unterbrechen.
Sicherheitsrisiko	(Hoch) Bei der Annahme eingehender SOAP-Anforderungen wird die entsprechende Validierung durchgeführt, um sicherzustellen, dass der relevante Inhaltstyp als Teil der Anforderung definiert wird. Sie schränkt die ungültigen SOAP-Antworten ein, die als Sicherheitsrisiko angesehen werden können.
Referenz	Inhaltstypen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Strikte IP-Einschränkung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ip.authenticate.strict`, um einen strikten Satz von IP-Adressen, z. B. DC und sicheres VPN, für den Zugriff auf diese Instanz zu aktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ip.authenticate.strict
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Ermöglicht ServiceNow-Mitarbeitern den Zugriff auf die Instanz nur über gesicherte IP-Bereiche
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Wenn diese Eigenschaft nicht aktiviert ist, können ServiceNow-Mitarbeiter über alle IP-Bereiche auf die Instanz des Kunden zugreifen. Durch Aktivieren der Eigenschaft wird der Zugriff auf einen sicheren Satz von IP-Bereichen (Sicheres VPN, DC) eingeschränkt. **Hinweis:** Wenn Sie diese Eigenschaft auf „true“ festlegen, verwendet Now Platform eine restriktivere `glide.ip.authenticate.allow.secured` -Eigenschaft anstelle der Leistungsüberwachung IP-Einschränkungs-Eigenschaft (`glide.ip.authenticate.allow.secured`) für eine Reihe von IP-Bereichen, die auf die Instanz zugreifen können.
Sicherheitsrisiko	(Niedrig) Unnötige Offenlegung des Instanzzugriffs für eine breitere Gruppe von Personen.
Referenz	IP-Bereichsbasierte Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Hinweis:
Eine Deny-All-Regel muss der IP-Zugriffssteuerung hinzugefügt werden, um den Zugriff von IP-Adressen einzuschränken, die nicht der IP-Zugriffssteuerung hinzugefügt wurden. Alle erforderlichen zulässigen IPs müssen dann der IP-Zugriffssteuerung hinzugefügt werden.

Autorisierung von Entlade-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.unl` (useUnloadFormat), um anzugeben, ob für eingehende Entladeanforderungen die Basic Authentication erforderlich sein soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.unl
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen der Basic Authentication bei Entladeanforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von Entladedaten für die Instanz abgerufen werden.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung, die für die Entladeanforderungen für Datenquellen konfiguriert ist, kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

WSDL-Anforderungsautorisierung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.wsdl`, um anzugeben, ob für eingehende WSDL-Anforderungen (Web Services Description Language) die Basic Authentication erforderlich sein soll.

Hinweis:
Wenn Sie keine Basic Authentication für eingehende WSDL-Anforderungen anfordern möchten, müssen Sie die Zugriffskontrollregeln (ACL) ändern, damit Gastbenutzer auf den WSDL-Inhalt zugreifen können.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.wsdl
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen der Basic Authentication für WSDL-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von WSDL-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung, die für die WSDL-Webservices konfiguriert ist, kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche WSDL-Inhalte/-Daten in der Zielinstanz erhalten.
Referenzen	Webservice-Sicherheit

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung von XML-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.xml`, um anzugeben, ob für eingehende XML-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.xml
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Basic Authentication für XML-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von XML-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter XML-Parser-Schritt .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende XML-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung von XSD-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.basicauth.required.xsd`, um anzugeben, ob für eingehende XSD-Anforderungen (XML-Schemadefinition) die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.xsd
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Basic Authentication für XSD-Anforderungen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von XSD-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Nicht interaktive Sitzungen .
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende XSD-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anhänge (Härtung der Instanzsicherheit)

Viele Now Platform Geschäftsprozesse ermöglichen das Hochladen von Daten/Informationen. Sie überprüft regelmäßig die Gültigkeit und Sicherheit von Text, aber das Akzeptieren dieser Dateien kann ein noch höheres Risiko darstellen.

Um das Risiko zu verringern, sollten Sie auf schädliche Dateien validieren, damit Now Platform ordnungsgemäß vor Angreifern schützen kann, die diese Dateien senden. Sie verarbeiten diese Dateien, indem Sie Geschäftslogik einbeziehen, die Dateien während des Upload-Vorgangs scannt und die als schädlich erkannten Dateien ablehnt.

Interne Referenzen

- Anhänge verwalten
- Konfigurieren Sie Systemeigenschaften für Anhänge

Herunterladbare MIME-Typen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.ui.attachment.download_mime_types`*, um eine Liste von durch Kommas getrennten MIME-Anhangtypen anzugeben, die heruntergeladen, aber nicht inline im Browser gerendert werden sollen.

Um eine Liste vorhandener MIME-Typen anzuzeigen, geben Sie `/sys_attachment_icon_rule_list.do` ein. Sie können einen dieser MIME-Typen aktivieren, um die Sicherheits-Compliance-Anforderungen in Now Platformzu erfüllen.

Hinweis:
Wenn Sie die Eigenschaft **Download von MIME-Typen** erzwingen auf **true**setzen, wird die Eigenschaft **Herunterladbare MIME-Typen** überschrieben, die eine durch Kommas getrennte Liste der herunterladbaren MIME-Typen ist. Weitere Informationen finden Sie unter Download von MIME-Typen erzwingen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.attachment.download_mime_types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Darstellung der Dateitypen im Browser einzuschränken, um die Ausführung versteckter schädlicher Skripts zu vermeiden.
Empfohlener Wert	Einige definierte Dateitypen, z. B. text/html,text/csv.
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt die Durchführung von Validierungsprüfungen, bevor eine Aktion ausgeführt wird, wenn Sie in einer Now Platform -Anwendung auf einen Anhang klicken. Es gibt keine potenziellen Auswirkungen, aber die Benutzer-Experience wird geändert.
Sicherheitsrisiko	(Mittel) Clientseitige Skripting-Angriffsvektoren gibt es in verschiedenen Varianten, und der Missbrauch von MIME-Typ-Anhängen ist keine Ausnahme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Angreifer können MIME-Typen missbrauchen und unbeabsichtigte Skriptinhalte im Anhang auf der Seite des Opfers platzieren, um vertrauliche Informationen zu erfassen. Füllen Sie im aktuellen Kontext die Eigenschaft mit einer Liste von kommagetrennten MIME-Typen für Anhänge aus, die im Browser nicht inline dargestellt werden sollen. Beispiel: text/html

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sperrliste für Anhänge aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.security.attachment_type.use_blacklist*], um anzugeben, ob Now Platform den Anhang anhand einer angegebenen Ausschlussliste validieren soll.

Hinweis:
Legen Sie die Eigenschaft *glide.security.attachment_type.use_blacklist* erst auf „ true “ fest, wenn Sie die Eigenschaften *glide.attachment.blacklisted.extensions* und *glide.attachment.blacklisted.types* konfiguriert haben. Weitere Informationen finden Sie unter Geben Sie abgelehnte Verlängerungen an und Geben Sie die abgelehnten Dateitypen an.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.attachment_type.use_blacklist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Beschränken Sie den Upload-Vorgang (Einfügen/Schreiben/Aktualisieren) von Anhängen mit fragwürdigen Dateierweiterungen und Dateitypen, z. B. exe, dll, JAR, Text/HTML.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Keine Auswirkungen auf die Funktionalität, es sei denn, es wird versucht, Dateierweiterungen oder Dateitypen hochzuladen, die in den Eigenschaften der Ausschlussliste (*glide.attachment.blacklisted.extensions* und *glide.attachment.blacklisted.types*) angegeben sind.
Sicherheitsrisiko	(Mittel) Ein böswilliger Benutzer kann mit Malware infizierte Anhänge mit gängigen ausführbaren Dateierweiterungen und/oder -typen hochladen.
Workaround	Im Basissystem sind Eigenschaften verfügbar, die dasselbe Problem mit Aufnahmelisten anstelle von Ausschlusslisten beheben. Weitere Informationen finden Sie unter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Dateierweiterungen einschränken • MIME-Typeinschränkung für Uploads

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Einschränkungen beim Dateidownload aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.strict_customer_uploaded_static_content`, um Einschränkungen für die Dateitypen zu aktivieren, die heruntergeladen werden können, wenn sie mit der Funktion „Datei hochladen“ hochgeladen wurden.

Sie verwenden diese Eigenschaft mit der Eigenschaft `glide.ui.strict_customer_uploaded_content_types`, die eine durch Kommas getrennte Liste mit eingeschränkten herunterladbaren Dateitypen erstellt. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.strict_customer_uploaded_static_content
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Um sicherzustellen, dass sichere Dateitypen aus der Anwendung heruntergeladen werden dürfen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung von Dateidownloads basierend auf den in der Eigenschaft `glide.ui.strict_customer_uploaded_content_types` angegebenen Werten. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.
Sicherheitsrisiko	(Mittel) Dateidownload-Einschränkungen sollten auf alle nicht vertrauenswürdigen Benutzereingabequellen angewendet werden.

Strikten Upload von Anwenderbildern erzwingen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.security.strict.user_image_upload`, um die Zugriffssteuerung für das Hochladen/Aktualisieren eines Profilbildes zu aktivieren, wenn sie für einen Benutzerdatensatz ausgeführt wird.

Diese Einstellung ermöglicht es einem nicht autorisierten Benutzer, ein Bild in das Profil eines anderen Benutzers hochzuladen.

- Wenn Sie diese Eigenschaft auf **true**festlegen, werden die Tabellen-ACLs beim Hochladen von Fotos erzwungen, sodass nur autorisierte Benutzer ein Bild hochladen können.
- Wenn Sie die Option auf **false**festlegen, werden ACLs beim Hochladen von Bildern in das Feld Foto nicht erzwungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.strict.user_image_upload
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So beschränken Sie das Hochladen von Benutzerbildern nur auf autorisierte Benutzer.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Keine Auswirkungen auf die Funktionalität, da autorisierte Benutzer weiterhin Bilder in ihr Benutzerprofil hochladen können.
Sicherheitsrisiko	(Mittel) Wenn Sie diese Eigenschaft auf **false**festlegen, kann ein authentifizierter Benutzer ein Bild ohne Autorisierung in den Account eines anderen Benutzers hochladen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Download von MIME-Typen erzwingen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.attachment.force_download_all_mime_types*, um den Download aller MIME-Typ-Anhänge zu erzwingen.

Hinweis:
Wenn Sie die Eigenschaft **Download von MIME-Typen** erzwingen auf **true**setzen, wird die Eigenschaft **Herunterladbare MIME-Typen** überschrieben, die eine durch Kommas getrennte Liste der herunterladbaren MIME-Typen ist. Weitere Informationen finden Sie unter Herunterladbare MIME-Typen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.attachment.force_download_all_mime_types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Um das Herunterladen aller Anhänge zu erzwingen, anstatt sie im Browser auszuführen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt den Download aller Anhänge. Keine Auswirkungen auf die Funktionalität, führt jedoch zu einer veränderten Benutzer-Experience.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Um die clientseitigen Skripting-Angriffe zu reduzieren, sollte das Herunterladen von Dateianhängen erzwungen werden, anstatt im Browserkontext gerendert zu werden.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Dateierweiterungen einschränken (Härtung der Instanzsicherheit)

Definieren Sie mithilfe der Systemeigenschaft `glide.attachment.extensions`, welche Dateitypen in Ihre Instanz hochgeladen werden können. Diese Eigenschaft verwendet eine durch Kommas getrennte Liste der zulässigen Dateierweiterungstypen. Nur die angegebenen Dateierweiterungstypen werden als Anhänge hochgeladen.

Verwenden Sie die Eigenschaft `glide.attachment.extensions` in Ihrer Instanz, um die folgenden Vorteile zu erzielen:

Verbesserte Sicherheit

Verwenden Sie diese Eigenschaft, um die Sicherheit zu verbessern, indem Sie verhindern, dass Benutzer schädliche Dateien wie Viren als Anhänge hochladen. Sichern Sie Ihre Instanz, indem Sie Typen blockieren, die normalerweise von ausführbaren Programmen oder Skripts verwendet werden.

Vermeiden Sie inkompatible Dateitypen

Verwenden Sie diese Eigenschaft, um zu verhindern, dass Benutzer inkompatible Dateien hochladen. Beispielsweise unterstützen einige Browser keine Symbole im PNG-Format. Wenn Sie die PNG-Dateierweiterung nicht einbeziehen, können Sie verhindern, dass Benutzer PNG-Dateien hochladen.

Wichtig:
Diese Eigenschaft schränkt Dateien nicht basierend auf dem tatsächlichen Dateityp (MIME-Typ) ein, sondern nur basierend auf der Erweiterung. Um Uploads basierend auf dem MIME-Typ einzuschränken, konfigurieren Sie die Eigenschaft `glide.security.file.mime_type.validation`, nachdem Sie die Konfiguration der Eigenschaft `glide.attachment.extensions` abgeschlossen haben. Weitere Informationen zum Konfigurieren von `glide.security.file.mime_type.validation`finden Sie unter MIME-Typeinschränkungfür Uploads.

Schritte zum Konfigurieren von

1. Geben Sie im Filternavigator Ihrer Instanz sys_properties.listein, und drücken Sie die Eingabetaste.
2. Suchen und öffnen Sie die Eigenschaft `glide.attachment.extensions`.
3. Geben Sie im Feld **Wert** die Dateierweiterungen ein, die als Anhänge hochgeladen werden sollen. Trennen Sie mehrere Einträge im Feld durch Kommas. Ein Beispielwert für mehrere Einträge wäre `doc,docx,xls,xlxs,pdf,jpeg,jpg,png,ico`.

   Hinweis:
   Wenn im Feld **Wert** keine Dateitypen angegeben sind, kann jeder Dateityp als Anhang hochgeladen werden.

4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.attachment.extensions
Konfigurationstyp	Systemeigenschaft (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	Um nur zulässige Dateierweiterungen während des Dateianhangs hochzuladen. Es blockiert einen Versuch, potenziell schädliche Erweiterungen hochzuladen.
Empfohlener Wert	Einige definierte Dateierweiterungen, z. B. doc, docx, pdf, xls, xlsx
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur schränkt alle Dateierweiterungen mit Ausnahme der in der Aufnahmeliste enthaltenen Dateierweiterungen ein. Keine Auswirkungen auf die Funktionalität, es sei denn, es wird versucht, eine andere Datei als die von der Organisation akzeptierten Erweiterungen hochzuladen.
Sicherheitsrisiko	(Mittel) Da die MIME-Typverifizierung von dieser Eigenschaft abhängt, wird empfohlen, die Schwachstellen im Zusammenhang mit dem Hochladen schädlicher Dateien zu minimieren.

Nicht authentifizierten Zugriff auf Anhänge beschränken (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.image_provider.security_enabled`*, um die Sicherheitseinstellungen für Images zu steuern. Bei Festlegung auf **true**sind Images nur für authentifizierte und autorisierte Benutzer sichtbar. Bei **false**sind Bilder für alle sichtbar, die eine URL zum Anhang haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.image_provider.security_enabled
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um den nicht authentifizierten Zugriff auf den Anhang zu verhindern, wenn er im iix-Format gerendert wird.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Keine nennenswerten Auswirkungen auf die Funktionalität. Die Benutzer-Experience kann etwas beeinträchtigt werden, da der Benutzer, der zuvor direkt auf .iix zugegriffen hat, sich authentifizieren muss.
Sicherheitsrisiko	(Hoch) Für nicht authentifizierte Benutzer muss eine Einschränkung angewendet werden, da einige Anhänge vertrauliche Informationen enthalten können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Anhänge verwalten Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Ausgeschlossene Anhangerweiterungen angeben (Härtung der Instanzsicherheit)

Wenn Sie die Validierung der Ausschlussliste in Now Platformaktivieren, verwenden Sie die Eigenschaft `glide.attachment.blacklisted.extensions`, um eine durch Kommas getrennte Liste mit eingeschränkten hochladbaren Dateierweiterungstypen zu erstellen. Das Hochladen der angegebenen Dateierweiterungstypen ist eingeschränkt.

Voraussetzungen

Legen Sie diese Eigenschaft fest, bevor Sie die Eigenschaft `glide.security.attachment_type.use_blacklist` auf „true“ festlegen. Weitere Informationen finden Sie unter Schwarze Liste für Anhänge aktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.attachment.blacklisted.extensions
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Beschränken Sie den Upload-Vorgang (Einfügen/Schreiben/Aktualisieren) von Anhängen mit fragwürdigen Dateierweiterungen.
Typ	Zeichenfolge
Empfohlener Wert	Benutzerdefinierte Dateierweiterungen. Gängige Beispiele sind ex, dll, xslx.
Funktionale Auswirkung	(Niedrig) Keine Auswirkungen auf die Funktionalität, es sei denn, es wird versucht, eine unter dieser Eigenschaft angegebene Dateierweiterung hochzuladen.
Sicherheitsrisiko	(Mittel) Ein böswilliger Benutzer kann mit Malware infizierte Anhänge mit gängigen ausführbaren Dateierweiterungen hochladen.
Workaround	Eigenschaften sind in der Basissystemfunktionalität verfügbar, die dasselbe Problem behandelt, mit Aufnahmeliste anstelle von Ausschlussliste. Weitere Informationen finden Sie unter: • Dateierweiterungen einschränken • MIME-Typeinschränkung für Uploads

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgeschlossene Anhangsdateitypen angeben (Härtung der Instanzsicherheit)

Wenn die Validierung der Ausschlussliste in Now Platformaktiviert ist, verwenden Sie die Eigenschaft `glide.attachment.blacklisted.types`, um eine durch Kommas getrennte Liste mit eingeschränkten hochladbaren Dateitypen zu erstellen. Das Hochladen der angegebenen Dateitypen ist eingeschränkt.

Voraussetzungen

Legen Sie diese Eigenschaft fest, bevor Sie die Eigenschaft `glide.security.attachment_type.use_blacklist` auf „true“ festlegen. Weitere Informationen finden Sie unter Schwarze Liste für Anhänge aktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.attachment.blacklisted.types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Upload-Vorgang (Einfügen/Schreiben/Aktualisieren) von Anhängen mit fragwürdigen Dateitypen einschränken. Beispiel: text/html.
Empfohlener Wert	Einige definierte Dateitypen (Beispiel: text/html,text/csv).
Funktionale Auswirkung	(Niedrig) Keine Auswirkungen auf die Funktionalität, es sei denn, es wird versucht, einen unter dieser Eigenschaft angegebenen Dateityp hochzuladen.
Sicherheitsrisiko	(Mittel) Ein böswilliger Benutzer kann mit Malware infizierte Anhänge mit gängigen ausführbaren Dateitypen hochladen.
Workaround	Eigenschaften sind in der Funktionalität des Basissystems verfügbar, die das gleiche Problem mit der Aufnahmeliste und nicht mit der Ausschlussliste beheben. Weitere Informationen finden Sie unter: • Dateierweiterungen einschränken • MIME-Typeinschränkung für Uploads

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Herunterladbare Dateitypen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.strict_customer_uploaded_content_types`, um eine durch Kommas getrennte Liste mit eingeschränkten herunterladbaren Dateitypen zu erstellen. Die angegebenen Dateitypen sind die einzigen, die als statischer Inhalt von einer Instanz heruntergeladen werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.strict_customer_uploaded_content_types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um sicherzustellen, dass nur Dateitypen in Aufnahmelisten heruntergeladen werden dürfen.
Empfohlener Wert	Benutzerangegeben (Allgemein: doc, docx, xls, xlsx, pdf und ähnlich)
Funktionale Auswirkung	(Mittel) Es können nur Dateien heruntergeladen werden, die sich in Aufnahmelisten befinden, was sich auf die Organisationsrichtlinie auswirken kann. Die durch Kommas getrennte Aufnahmeliste muss geändert werden, um der Richtlinie der Organisation für akzeptable herunterladbare Dateitypen zu entsprechen.
Sicherheitsrisiko	(Niedrig) Dateidownload-Einschränkungen sollten auf alle nicht vertrauenswürdigen Benutzereingabequellen angewendet werden.
Referenzen	Eigenschaften der Sicherheitseinstellungen Inhaltstypen

Schritte zum Konfigurieren von

1. Navigieren zu **/sys_properties_list.do**.
2. Suchen Sie nach der Eigenschaft `glide.ui.strict_customer_uploaded_content_types`.
3. Geben Sie die zulässigen herunterladbaren Dateitypen in einer durch Kommas getrennten Liste an, wie gezeigt, und klicken Sie dann auf **Aktualisieren**.
   Ein Beispiel für einen korrekt formatierten Wert für die Liste wäre `ico,gif,png,jpg,jpeg,bmp,ogg,mp3,doc,docx,xls,pdf`.

MIME-Typeinschränkung für Uploads (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.security.file.mime_type.validation`, um die MIME-Typprüfung für Uploads zu aktivieren. Sie können die MIME-Typvalidierung für Dateianhänge aktivieren (setzen Sie die Eigenschaft auf **true**) oder deaktivieren (setzen Sie sie auf **false**).

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, legen Sie die Eigenschaft `glide.attachment.extensions` fest. Nur die in `glide.attachment.extensions` angegebenen Erweiterungen werden während des Uploads auf den MIME-Typ überprüft. Weitere Informationen finden Sie unter Dateierweiterungen einschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.file.mime_type.validation
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingt die Überprüfung des MIME-Typs/der „Magic Byte“ beim Datei-Upload.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur ermöglicht die Überprüfung des MIME-Typs für die Anhänge der Anwendung. Keine Auswirkungen auf die Funktionalität, es sei denn, es liegt eine böswillige Absicht beim Hochladen der Dateien vor, da bei dieser Validierung lediglich nach Synchronisierungsfehlern zwischen dem MIME-Typ und den Daten gesucht wird.
Sicherheitsrisiko	(Mittel) Um Schwachstellen wie Dateieinschluss und Uploads schädlicher Dateien zu reduzieren, sollte die MIME-Typverifizierung aktiviert sein.
Referenzen	Anhänge verwalten

Weitere Informationen zum Konfigurieren von Eigenschaften für die Härtung finden Sie unter Härtungseinstellungen für die Instanzsicherheit.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

E-Mail-Sicherheit (Härtung der Instanzsicherheit)

Dieser Abschnitt enthält Sicherheitskontrollen, die ein Administrator konfigurieren kann, um sicherzustellen, dass für alle eingehenden E-Mails die richtigen Sicherheitsrichtlinien vorhanden sind.

Eingehende E-Mails in HTML konvertieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft `glide.email.inbound.convert_html_inline_attachment_references`, um anzugeben, ob eingehende E-Mail-HTML so konvertiert werden soll, dass E-Mail-Bilder in der HTML-Textvorschau der E-Mail angezeigt werden.

Folgendes geschieht, wenn die Systemeigenschaft `glide.email.inbound.convert_html_inline_attachment_reference` auf „false“ festgelegt ist:

- In Now Platformwerden anstelle der empfangenen Bilder defekte CID-Links (Inhalts-ID) angezeigt. Das Format, in dem das E-Mail-Bild angezeigt wird, hängt von der Eigenschaftseinstellung zum Zeitpunkt des Empfangs der E-Mail ab, nicht von der aktuellen Eigenschaftseinstellung.
- Der im Anhang empfangene „böswillige“ Inhalt wird im HTML-Code der E-Mail nicht referenziert. Der Anhang selbst wird in der Tabelle „sys_attachment“ gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bei der Verarbeitung eingehender E-Mails werden die HTML-Daten der E-Mail nicht aktualisiert, um den Speicherort des Anhangs in der Tabelle „sys_attachment“ wiederzugeben. Dies führt zu Folgendem:
  - Inline-Bilder werden im Aktivitätsformatierer nicht in der E-Mail-Anzeige angezeigt.

    Hinweis:
    Um dieses Problem mit dem Aktivitätsformatierer zu beheben, überprüfen Sie zuerst, ob keine Sicherheitsbedenken bestehen. Legen Sie dann die Systemeigenschaft `glide.email.inbound.convert_html_inline_attachment_reference` auf „**true** “ fest, damit zukünftige empfangene E-Mails die erforderliche HTML-URL enthalten können, um auf das Bild zu verweisen. Durch das Ändern der Eigenschaft werden bereits empfangene E-Mails nicht aktualisiert. Der neue Wert wirkt sich nur auf eingehende E-Mails aus, die nach dem Ändern der Eigenschaft empfangen wurden.

  - Inline-Bilder werden nicht angezeigt, wenn die E-Mail in der HTML-Vorschau der E-Mail angezeigt wird.
  - Beim Anfügen von email.body_htm in eingehenden Aktionen zwischen Code-Tags fehlen die Bilder.

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft `glide.email.read.active` auf „true“ fest. Weitere Informationen finden Sie unter Eigenen POP3-Server verwenden .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.email.inbound.convert_html_inline_attachment_references
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So beschränken Sie das Rendern von Bildern in der HTML-Textvorschau.
Empfohlener Wert	false
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, kann der Benutzer die Bildvorschau im E-Mail-Text nicht sehen.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer ein schädliches Image senden, das Malware enthält.
Referenzen	E-Mail-Eigenschaften Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertung und Filterung von E-Mail-Spam (Härtung der Instanzsicherheit)

Installieren Sie das Plugin „E-Mail-Filter“ (*com.glide.email_filter*), um die E-Mail-Filterung innerhalb der Instanz zu installieren. Diese Filterung identifiziert vorhandene Header, sodass Sie basierend auf dem zugeordneten Header entscheiden können, was mit der E-Mail geschehen soll.

Jede Nachricht, die über Now Platform E-Mail-Server gesendet wird, wird auf die Wahrscheinlichkeit geprüft, Spam zu sein.

Hinweis:
Wenn eine Instanz einen privaten E-Mail-Server verwendet, ist dieses Thema nicht anwendbar. Weitere Informationen finden Sie unter Bewertung und Filterung von E-Mail-Spam.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaft *glide.email.read.active* auf „Wahr“ fest. Weitere Informationen finden Sie unter Eigenen POP3-Server verwenden.
- Dieser Filter überschreibt die Eigenschaft *glide.pop3.ignore_headers*. Weitere Informationen finden Sie unter Verfügbare Systemeigenschaften.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.email_filter
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Filterung zu erzwingen, um Spam von E-Mails zu vermeiden.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) E-Mails werden im Rahmen der Spam-Bewertung niemals in der Instanz gefiltert, blockiert oder unter Quarantäne gestellt. Sie wird nur bewertet und dann an die Instanz gesendet. Alle Filter werden innerhalb der Instanz mit dem Plugin „E-Mail Filter“ durchgeführt.
Sicherheitsrisiko	(Mittel) E-Mail-Filter ermöglichen es Administratoren, einen Bedingungsgenerator oder ein bedingtes Skript zu verwenden, um anzugeben, wann böswillige eingehende E-Mails von bekannten/unbekannten Absendern ignoriert werden sollen.
Referenzen	E-Mail-Filter https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf E-Mails mit leerer Zieltabelle beschränken (Härtung der Instanzsicherheit)

Aktivieren Sie die Eigenschaft `glide.email.email_with_no_target_visible_to_all`, um den Benutzerzugriff auf E-Mails einzuschränken, es sei denn, er war der Absender der E-Mail oder hat eine Administratorrolle.

Nicht autorisierte Benutzer können in der Tabelle „E-Mails“ [sys_email] auf E-Mails zugreifen, denen ein Zieldatensatz fehlt. Anstatt ACLs für E-Mail-Einträge zu erzwingen, beschränkt diese Eigenschaft den Zugriff nur auf den E-Mail-Absender und Benutzer mit der Administratorrolle.

Hinweis:
E-Mails, die an die Instanz gesendet und von ihr empfangen werden, werden in der Tabelle „E-Mails“ [sys_email] angezeigt. Allerdings sollten nur empfangene E-Mails, die mit einem Fehler und dem Status Ignoriert markiert wurden, eine leere Zieltabelle haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.email.email_with_no_target_visible_to_all
Konfigurationstyp	Systemeigenschaften [sys_properties]
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um zu verhindern, dass der E-Mail-Client E-Mails anzeigt, wenn der Benutzer den Zugriff nicht autorisiert.
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Benutzer können E-Mails mit leerer Zieltabelle nicht mehr sehen, es sei denn, sie sind Administratoren oder der Absender der E-Mail.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Benutzer auf E-Mails zugreifen, bei denen das Feld target_table leer ist.
Referenzen	Erweiterte E-Mail-Eigenschaften https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

E-Mails für Anwendererstellung nach Domäne beschränken (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft `glide.user.trusted_domain`, um die durch Kommas getrennte Liste der vertrauenswürdigen Domänen anzugeben, die bei der Erstellung von Benutzern aus eingehenden E-Mails verwendet wird.

Standardmäßig wird ein Sternchen (*) verwendet, um allen Domänen zu vertrauen. Bestimmte Domänen sollten angegeben werden, wenn nicht E-Mails von jeder Domäne zugelassen werden müssen. Die Instanz ignoriert eingehende E-Mails aus anderen Domänen, es sei denn, sie stammen von der Adresse eines vorhandenen Benutzers. Die Instanz erstellt keine Gastbenutzer aus E-Mails aus nicht vertrauenswürdigen Domänen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaft `glide.email.read.active` auf „Wahr“ fest. Weitere Informationen finden Sie unter Eigenen POP3-Server verwenden.
- Legen Sie die Eigenschaft `glide.pop3readerjob.create_caller` auf „Wahr“ fest. Weitere Informationen finden Sie unter Automatische Benutzererstellung aktivieren.

Hinweis:
Überspringen Sie die Eigenschaft `glide.user.default_password`, wenn die Eigenschaft `glide.pop3readerjob.create_caller` auf **false**festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.user.trusted_domain
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Empfohlener Wert	Kommagetrennte Liste der vertrauenswürdigen Domänen [Bsp. servicenow.com (ein bestimmter Domänenname)].
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, akzeptiert die Instanz nur E-Mails von vertrauenswürdigen Domänen. Wenn Sie die Domäne nicht in die vertrauenswürdige Liste aufnehmen, wirkt sich dies auf Gastbenutzer aus, da Konten automatisch erstellt werden.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer eine E-Mail-Spoofing-/Spam-Kampagne verwenden, um mehrere E-Mails zu senden, was dazu führt, dass weitere unnötige Gastbenutzer erstellt werden.
Referenzen	E-Mail-Eigenschaften Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

Eingabevalidierung (Härtung der Instanzsicherheit)

Now Platform führt eine Eingabevalidierung durch, um Probleme zu verhindern, die aus der Eingabe fehlerhafter Daten resultieren.

In diesem Abschnitt werden Sicherheitskontrollen in Now Platform beschrieben, die ein Administrator konfigurieren kann, um die Eingabe fehlerhafter Daten unabhängig von der Quelle zu minimieren. Zu diesen Quellen gehören die manuelle Benutzereingabe oder Quellen aus einer Infrastruktur, externen Entitäten oder Datenbanksystemen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingebetteten HTML-Code zulassen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.security.allow_codetag*, um die Unterstützung für die Einbettung von HTML-Code zu deaktivieren, der mit dem Tag [code] erstellt wurde.

Now Platform mindert viele Einschleusungs- und Cross-Site-Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Benutzer keine HTML-formatierten Eingaben für Journalfelder schreiben/übermitteln. Journalfelder können jedoch in Code-Tags eingeschlossenen Text als HTML darstellen.

- Es besteht jedoch ein Sicherheitsrisiko. Bei Festlegung auf `true`können böswillige Benutzer schädlichen HTML-JS-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Setzen Sie diese Eigenschaft auf „ `false` “, damit Administratoren verhindern können, dass Journalfelder HTML-Code rendern, indem sie die Unterstützung für das Tag `[code]` deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.security.allow_codetag
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schützen Sie sich vor websiteübergreifendem Skripting und der Ausführung böswilliger Skripts
Empfohlener Wert	false
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die HTML-Codierung in der Benutzeroberfläche und rendert die codierten Ergebnisse für den Benutzer. Diese Eigenschaft ist standardmäßig auf „ `true` “ festgelegt. In diesem Status zeigt Ihre Instanz gerenderten HTML-Code in Journalfeldern und Formularen an. Wenn diese Eigenschaft auf „ `false`“ festgelegt ist, wird HTML nicht ordnungsgemäß dargestellt, und HTML-Tags werden möglicherweise in Journalfeldern in Formularen angezeigt. Dies kann sich negativ auf die Funktionalität und die Benutzerinteraktionen mit den resultierenden Daten auswirken.
Sicherheitsrisiko	(Mittel) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Beschränken Sie das CODE-Tag in Journalfeldern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Journalfeldeinträge als HTML darstellen Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

JavaScript-Tags in eingebettetem HTML zulassen (Härtung der Instanzsicherheit)

Die Eigenschaft *glide.ui.security.codetag.allow_script* deaktiviert die Unterstützung für die Einbettung von HTML-JavaScript-Code, der mit dem Tag [code] erstellt wurde.

Hinweis:
Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.

Now Platform mindert viele Einschleusungs- und Cross-Site-Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Benutzer keine HTML-formatierten Eingaben für Journalfelder schreiben und übermitteln. Journalfelder können jedoch in Code-Tags eingeschlossenen Text als HTML darstellen.

- Es besteht jedoch ein Sicherheitsrisiko. Bei Festlegung auf **true**können böswillige Benutzer schädlichen HTML-JavaScript-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Setzen Sie diese Eigenschaft auf „ **false** “, damit Administratoren verhindern können, dass Journalfelder HTML-JavaScript-Code rendern, indem sie die Unterstützung für das Tag [code] deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.security.codetag.allow_script
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schützt vor websiteübergreifendem Skripting und der Ausführung böswilliger Skripts
Empfohlener Wert	false
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt JavaScript-Escaping in der Benutzeroberfläche und rendert die codierten Ergebnisse für den Benutzer. Sie kann sich basierend auf der Interaktion des Instanzbenutzers mit den resultierenden Daten auf die Funktionalität auswirken.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Benutzersitzung im Kontext des angemeldeten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Beschränken Sie das CODE-Tag in Journalfeldern Journalfeldeinträge als HTML darstellen Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Nicht bereinigten HTML-Code überprüfen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *com.glide.security.check_unsanitized_html*, um das Bereinigungsverhalten von „translated_html“-Feldern auf globaler Ebene für Feldzuweisungen zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Die Zuweisung von HTML-Feldern zu einem beliebigen Feldtyp bietet die Funktionalität zum Formatieren von Inhalten mithilfe von HTML-Tags (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Um böswillige Aktivitäten zu verhindern, können bestimmte HTML-Tags mithilfe einer Sperrliste gesperrt werden. Diese Eigenschaft verhindert, dass unzulässige Tags in „translated_html“-Feldern in Ihrer Instanz verwendet werden.

- Legen Sie diese Eigenschaft fest, um das Bereinigungsverhalten von „translated_html“-Feldern zu **erzwingen**.
- Legen Sie die Eigenschaft auf „disable“ fest, um die HTML-Bereinigung zu **deaktivieren** und blockierte HTML-Tags in „translated_html“-Feldern zuzulassen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.security.check_unsanitized_html
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verhindert die Verwendung unsicherer HTML-Tags zum Schutz vor Angriffen wie websiteübergreifendem Skripting.
Typ	Zeichenfolge
Empfohlener Wert	*erzwingen*
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die HTML-Bereinigung in der Benutzeroberfläche und rendert übersetzte HTML-Felder für den Benutzer. Dies kann Auswirkungen auf die Lesbarkeit und Formatierung haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts für Benutzersitzungen im Kontext des angemeldeten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	HTML-Bereinigung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Vom Client generierte Skripts in der Sandbox (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.script.use.sandbox*, um das Skript-Sandboxing zu aktivieren.

Es gibt zwei Fälle in Now Platform, die es dem Client ermöglichen, Skripts zur Auswertung an den Server zu senden:

Filter oder Abfragen

Es ist zulässig, einen Filter an den Server zu senden, z. B. `assigned_to=JavaScript:getMyGroups()`.

System-API

Der API-Aufruf ermöglicht es dem Client, beliebige Skripts auf dem Server auszuführen und eine Antwort zu erhalten.

Wenn Sie das Skript-Sandboxing aktivieren, wird das an einem dieser beiden Einstiegspunkte ausgewertete Skript in einer Sandbox mit eingeschränkten Rechten mit den folgenden Eigenschaften ausgeführt:

- Nur die Business Rules, die als vom Client aufrufbar markiert sind, sind in der Sandbox verfügbar.
- In der Sandbox sind nur Skripteinbindungen verfügbar, die als vom Client aufrufbar markiert sind.
- Bestimmte API-Aufrufe (weitgehend, aber nicht vollständig, beschränkt auf Aufrufe, die sich mit direktem DB-Zugriff befassen) sind nicht zulässig.
- Sie können Daten in der Sandbox nicht einfügen, aktualisieren oder löschen. Beispielsweise werden alle Aufrufe von `current.update()`ignoriert. Wenn Sie Now Platform ausführen, ohne das Skript-Sandboxing zu aktivieren, gilt keine dieser Einschränkungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.verwenden.sandbox
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für die Plattform gestartet werden
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Fehlerkorrektur erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für Now Platformgestartet werden. Dies hat potenzielle Auswirkungen, wenn der Kunde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	über Anpassungen verfügt, die hartcodierte JavaScript-Abfragen zum Ausführen von CRUD-Vorgängen enthalten.
Sicherheitsrisiko	(Hoch) Now Platform bietet eine Vielzahl von Features und Funktionen über JavaScript-Abfragen. Ohne entsprechende Autorisierung und Validierung besteht jedoch für einen Angreifer die Möglichkeit, nicht autorisierte Vorgänge auf der Plattform durchzuführen.
Referenzen	Konfigurieren der Skript-Sandbox-Eigenschaft *glide.script.use.sandbox* gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *glide.script.allow.ajaxevaluate*: Siehe AJAXEvaluate aktivieren. • *glide.script.secure.ajaxgliderecord*: Siehe Aktivieren der AJAXGlideRecord-ACL-Überprüfung.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

AJAXEvaluate aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.script.allow.ajaxevaluate*, um die Ausführung beliebiger Clientskripts mit der System-API auf der Serverseite einzuschränken.

Es gibt zwei Fälle in Now Platform, die es dem Client ermöglichen, Skripts zur Auswertung an den Server zu senden:

Filter und/oder Abfragen

Es ist zulässig, einen Filter an den Server zu senden, z. B. `assigned_to=javascript:getMyGroups()`

System-API

Der API-Aufruf AJAXEvaluate ermöglicht es dem Client, beliebige Skripts auf dem Server auszuführen und eine Antwort zu erhalten.

Wenn Sie diese Eigenschaft auf **false**festlegen, aktiviert Now Platform nicht die Verwendung des AJAXEvaluate-API-Aufrufs aus dem Client-Skript.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.allow.ajaxevaluieren
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Beschränken Sie die Ausführung beliebiger Clientskripts mithilfe der System-API auf der Serverseite
Empfohlener Wert	false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt das Deaktivieren des AJAEvaluate-Prozessors. Dies kann Auswirkungen auf die Funktionalität haben, wenn Sie den AJAX-Auswertungsprozessor explizit als Teil benutzerdefinierter Skripts verwenden. Weitere Informationen finden Sie unter GlideAjax .
Sicherheitsrisiko	(Hoch) AJAXEvaluate kann die Ausführung von beliebigem JavaScript-Code im Client-Browser durch Anwenden der serverseitigen Objekte zulassen.
Referenzen	Konfigurieren der Skript-Sandbox-Eigenschaft GlideAjax `glide.script.allow.ajaxevaluate` gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • `glide.script.use.sandbox`: Siehe vom Client generierte Skripts in der Sandbox. • `glide.script.secure.ajaxgliderecord`: Siehe AJAXGlideRecord-ACL-Überprüfung aktivieren.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Excel-Formel mit Escape-Zeichen versehen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.export.escape_formulas`, um die Excel-Einschleusung zu verhindern, die auch als Formeleinschleusung bezeichnet wird.

Excel-Injektion erfolgt, wenn Websites nicht vertrauenswürdige Einträge in Excel-Dateien einbetten. Wenn Sie eine Tabellenkalkulationsanwendung wie Microsoft Excel oder LibreOffice Call verwenden, um eine Datei zu öffnen, werden alle Zellen, die mit +, -, = oder @ beginnen, als Formel interpretiert. Wenn Sie die Eigenschaft `glide.export.escape_formulas` auf **true**festlegen, werden Zeichenfolgenwerte, die mit +, -, = oder @ beginnen, beim Export in CSV-, XLS- oder XLSX-Dateien mit einem einzelnen Apostroph versehen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.export.escape_formulas
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Anwendung gegen die Excel- oder Formeleinschleusung zu verhindern.
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Böswillig erstellte Formeln können dazu verwendet werden, den Computer des Benutzers zu kapern, indem Schwachstellen in der Tabellenkalkulationssoftware ausgenutzt werden.
Sicherheitsrisiko	(Mittel) Böswillige Formeln stellen ein Risiko dar, auch wenn die eingebettete Tabelle keine vertraulichen Informationen enthält, da sie dazu verwendet werden können, den Computer des Betrachters zu gefährden.
Workaround	Alternativ können Sie nach Möglichkeit alle Leerzeichen entfernen und alle vom Client bereitgestellten Daten auf alphanumerische Zeichen beschränken.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Escape-HTML (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.escape_html_list_field*, um HTML-Escape-Zeichen für HTML-Felder in einer Listenansicht zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Die Zuweisung von HTML-Feldern zu einem beliebigen Feldtyp bietet die Funktionalität zum Formatieren von Inhalten mit HTML-Codes (z. B. <p>, <a href>, <b>, <font>, <img>). Ein böswilliger Benutzer kann HTML-Code innerhalb des Formularfelds einfügen, um unerwünschte Skripts in verschiedenen Client-/Benutzersitzungen auszuführen.

- Legen Sie diese Eigenschaft auf „ **true** “ fest, um ein HTML-Escaping durchzuführen, bevor die Datensätze/Felder im Browser gerendert werden, wenn die Tabelle als Listenansicht angezeigt wird.
- Wenn diese Option auf **false**gesetzt ist und Sie diese Spalte in einer Listenansicht auswählen, wenn Sie eine Tabelle oder Datensatzliste anzeigen, werden diese HTML-formatierten Felder möglicherweise angezeigt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.escape_html_list_field
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Anwendung gegen websiteübergreifende Skripting-Angriffe zu schützen
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die HTML-Codierung in der Benutzeroberfläche auf HTML-Parser-Ebene und gibt dem Benutzer codierte Ergebnisse zurück. Sie kann sich basierend auf der Interaktion des Instanzbenutzers mit den resultierenden Daten auf die Funktionalität auswirken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts für Benutzersitzungen im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

JavaScript mit Escape-Zeichen versehen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.html.escape_script*, um in Listenansichten Escape-Zeichen für JavaScript-Tags (<script></script>) in HTML-Feldern zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Die Zuweisung von HTML-Feldern zu einem beliebigen Feldtyp bietet dem Benutzer die Funktionalität, den Inhalt mit HTML-Codes zu formatieren (z. B. <p>, <a href>, <b>, <font>, <img>). Wenn Sie *glide.html.escape_script* auf **false**festlegen, werden die Tags (<script></script>) möglicherweise angezeigt, wenn Sie diese Spalte in einer Listenansicht auswählen, während Sie eine Tabellen- oder Datensatzauflistung anzeigen.

Ein böswilliger Angreifer kann JavaScript-Code einfügen, indem er ihn in die Tags (<script></script>) einbettet. Der Angreifer kann dies ausnutzen, indem er einen ausgefeilten JS-Vektor einfügt, der ausgeführt werden kann, wenn ein Benutzer den Tabellendatensatz öffnet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.html.escape_script
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um websiteübergreifende Skripting-Angriffe auf eine Anwendung zu verhindern.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt JavaScript-Escaping in der Benutzeroberfläche und rendert codierte Ergebnisse für den Benutzer. Dies kann sich basierend auf der Instanzbenutzerinteraktion mit den resultierenden Daten auf die Funktionalität auswirken
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Verfügbare Systemeigenschaften Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Escape Jelly (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.escape_all_script`, um die Escape-Zeichen aller in Jelly eingefügten Skripts zu erzwingen.

Alle in enthaltenen JS- und HTML-Zeichenfolgen werden mit Escape-Zeichen versehen<j:jelly> … </j:jelly> bevor sie in den Ausgabestrom geschrieben werden, wodurch das Auftreten mehrerer XSS-Probleme verhindert wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.escape_all_script
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

Zweck	Wenn die Eigenschaft nicht auf **true**festgelegt ist, müssen Entwickler für jedes benutzerdefinierte Jelly-Skript mehrere Schritte ausführen, um XSS-Probleme zu vermeiden. Diese Schritte umfassen das Suchen der Jelly-Variablen, die an den Ausgabestream gesendet werden, um sie auf Webseiten zu rendern, und das Ausführen von Escaping für jedes der folgenden Tags:
	
	`$ à {JS:Ausdruck}`
	
	`$ à {HTML: Ausdruck}`
	
	ODER
	
	`$à {JS,HTML:Ausdruck}`

Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt Jelly-Escaping auf Parser-Ebene. Sie kann Auswirkungen auf die Funktionalität der Benutzerinteraktion mit den resultierenden Daten haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss für alle Benutzereingaben erfolgen, die in der Anwendung eingegeben werden. Auf diese Weise können Einschleusungsangriffe auf die Plattform verteidigt und geschützt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Workaround	Die Benutzeroberfläche kann beeinträchtigt werden, da einige der Skripts und HTML-Tags, die für das Rendern auf einer Webseite entwickelt wurden, möglicherweise fehlerhaft erscheinen. Diese Korrektur sendet die codierte Ausgabeseite zum Rendern an den Browser. Beispielsweise kann anstelle von „meine Zeichenfolge hier“ „meine Zeichenfolge hier“<u>angezeigt werden</u>, da das Tag <u> ordnungsgemäß mit Escape-Zeichen versehen wurde. Um in diesem Fall ein Escaping zu verhindern, fügen Sie dem Jelly-Ausdruck das NOESC-Präfix hinzu, um ein JS-Escaping zu verhindern. Beispiel: • Vorher: ($[jvar_context_menus]); • Nach: ($[NOESC:jvar_context_menus]); • Vorher: $[jvar_ui_policy_scripts] • Nach: $[NOESC:jvar_ui_policy_scripts]
Referenzen	Strenge Sicherheitseinstellungen Jelly Tags

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Escape-XML (Härtung der Instanzsicherheit)

Die Eigenschaft *glide.ui.escape_text* erzwingt Escape-Zeichen für XML-Werte auf Parser-Ebene, bevor sie an den Browser des Clients übertragen werden.

Hinweis:
Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.

Siteübergreifendes Skripting tritt auf, wenn ein Angreifer schädliches JavaScript in einen Einstiegspunkt einfügt. Die Plattform/Anwendung kann das schädliche JavaScript nicht mit Escape-Zeichen versehen, bevor es zur Ausführung an den Browser des Opfers übertragen wird. Escaping bedeutet in diesem Kontext Folgendes:

- **&** -> &
- **<** --> <
- **>** --> >
- **„** --> “
- **'** --> '
- **/** --> /

Beispiel: <![CDATA[<script> alert('XSS-Angriff');</script>]]>

Escaping: <script>alert('XSS Attack');</script>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.escape_text
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Durch das Escaping von XML wird sichergestellt, dass Browser das in nicht vertrauenswürdige Daten eingebettete schädliche JavaScript nicht analysieren und als JavaScript ausführen. • Ein böswilliger Benutzer kann einen XSS-Angriff versuchen, um entweder die Sitzung anderer Benutzer zu kapern oder den Benutzer auf eine schädliche Website umzuleiten. • Now Platform enthält Code zum Sichern von Cookies. Um ihn jedoch mit Escape-Zeichen zu versehen, muss diese Eigenschaft auf **true**festgelegt werden.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die XML-Codierung auf XML-Parser-Ebene in der Benutzeroberfläche. Dadurch werden die codierten Ergebnisse für den Benutzer gerendert, was sich je nach Instanzbenutzerinteraktion mit den resultierenden Daten auf die Funktionalität auswirken kann.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

Workaround	Nachdem Sie diese Eigenschaft auf **true**festgelegt haben, wird das Rendern der HTML-Tags in der Katalogelementbeschreibung oder im Hilfetext der Katalogelementvariablen angehalten. Möglicherweise können Sie die HTML-Formatierung für einige Felder nicht verwenden.
	Wenn jedoch die Eigenschaft *`glide.ui.escape_text`* deaktiviert ist, wird allen JEXL-Ausdrücken ein Ausgabe-Encoder vorangestellt:
	`${JS:Ausdruck}`
	`${HTML:Ausdruck}`
	oder
	`${JS,HTML:Ausdruck}`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

HTML-Bereinigung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.html.sanitize_all_fields*, um die HTMLSanitizer-Skripteinbindung zu aktivieren, die HTML-Eingaben basierend auf den in einem Skript konfigurierten Ausschluss- und Aufnahmeattributen bereinigt.

Die mit Dictionary/Fields verfügbaren Feldtypen umfassen HTML und übersetztes HTML. Mit diesen HTML-Eingabefeldern können Benutzer HTML-formatierte Eingaben schreiben, z. B.:

<h1>Test</h1>) mit den einfachsten HTML-Tags wie <img>, <a href ⋯>und <iframe>.

Sie kann einem böswilligen Angreifer die Möglichkeit geben, schädliche Vektoren mit HTML-Tags einzuschleusen, z. B.:

[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href="" onclick=alert(/xss/)].

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.html.sanitize_all_fields
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verhindert, dass die Anwendung Cross Site Scripting und HTML-Injektionsangriffe durchführt
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Benutzerdaten an den Benutzer zurückgegeben werden. Wenn der Kunde eine Anpassung hat, die das Rendern der HTML-Attribut- oder Inhaltsdaten umfasst, hat dies Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Hoch) Benutzereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden. Dadurch werden clientseitige Cross-Site-Scripting-Angriffe durch Ausgabecodierung der Daten reduziert.
Workaround	Diese Eigenschaft bereinigt alle HTML-Felder im System. Wenn Sie die HTML-Bereinigung für einzelne Felder aktivieren müssen, finden Sie weitere Informationen unter Bereinigung einzelner Felder aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Sie können auch die Aufnahme- oder Ausschlussliste konfigurieren, um HTML-Tags und -Attribute gemäß den Richtlinien Ihrer Organisation zu bereinigen.
Referenzen	Aktivieren der HTML-Bereinigung HTML-Bereinigung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Jelly/JS-Interpolation (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.jelly.js_interpolation.protect`, um sicherzustellen, dass JavaScript-Code, der auf einer Jelly-Seite ausgeführt werden soll, mithilfe der Jelly-Interpolation vor der Eingabe geschützt wird.

Wenn Sie die Eigenschaft auf **true**festlegen, durchläuft eine Anwendung eine Jelly-Skriptstruktur (verschachtelt). Potenziell gefährliche Jelly-Ausdrücke werden mit einem Filter umschlossen, der:

- Versieht ihre Ergebnisse aus Sicherheitsgründen mit Escape-Zeichen, oder
- Wenn ihre Sicherheit nicht garantiert werden kann, generiert eine SecurityException, da der Ausdruck, der ausgewertet werden sollte, ein mögliches Sicherheitsproblem darstellt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.jelly.js_interpolation.schützen
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zur Verringerung von Angriffen mit Ausführung von böswilligem Code, die durch Jelly-Injektion auftreten können.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Eigenschaft ermittelt am besten, ob ein Ausdruck in Anführungszeichen steht. Möglicherweise wird ein gültiger Ausdruck falsch in Anführungszeichen gesetzt. In diesem Fall kann es erforderlich sein, einen Ausdruck manuell als sicher zu kennzeichnen.
Sicherheitsrisiko	(Mittel) Die JEXL-Injektion ist eine für Now Platform eindeutige Form der Eingabeinjektion, die sowohl zur standortübergreifenden Anforderungsfälschung als auch zur Codeausführung führen kann. Wenn Sie den Schutz vollständig deaktivieren, können möglicherweise viele P1-Sicherheitsschwachstellen geöffnet werden.
Workaround	Um einen Ausdruck manuell als sicher zu kennzeichnen, fügen Sie dem Jelly-Ausdruck das SAFE-Präfix hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	${SAFE:sysparm_input}; Das blinde Hinzufügen von SAFE zu jedem Ausdruck ist die falsche Herangehensweise an das Problem, da dadurch eine Sicherheitslücke geöffnet werden kann. • Fügen Sie SAFE nur dann zu einem Ausdruck hinzu, wenn Sie garantieren können, dass der Ausdruck keine Eingaben vom Client enthält. • Wenn dies der Fall ist, kann ein böswilliger Client die Auswertung von privilegiertem JavaScript verursachen.
Referenzen	Jelly Tags Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Strikte Sicherheit der SOAP-Anforderung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.soap.strict_security`, um die Sicherheit von Webservices zu erzwingen.

Diese Eigenschaft verwendet eine Kombination aus:

- Abfrage/Rückmeldung der Standardauthentifizierung über das HTTP-Protokoll und
- Zugriffskontrollen auf Systemebene im Plugin „Contextual Security: Role Management“.

Wenn Sie diese Eigenschaft auf **true**festlegen, werden die folgenden Aktionen ausgeführt:

- Wenn der Benutzer über die entsprechende Rolle zum Ausführen des Vorgangs verfügt, wird die eingehende SOAP-Anforderung auf Rollenberechtigung zur Validierung überprüft. Es tritt bei Aufrufen/Anforderungen von SOAP-Webservices für Tabellen Now Platform auf, wenn CREATE-, READ-, UPDATE- oder DELETE-Vorgänge ausgeführt werden.
- Überprüft die ACLs auf Systemebene beim Abrufen von Daten in Form von SOAP-Daten aus der Tabelle.
- Überprüft die ACLs auf Feldebene auf CRUD-Vorgänge, die für ein Feld der Tabelle ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.soap.strict_security
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Stellt sicher, dass Sicherheits-ACLs auch dann überprüft und validiert werden, wenn auf die Datensätze über SOAP-Aufrufe zugegriffen wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Fehlerkorrektur erzwingt die Zugriffskontrolle auf Systemebene beim Abrufen von Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz. Wenn derzeit Benutzer auf diese Daten zugreifen, ist der Zugriff auf die Daten gemäß den ACL-Regeln eingeschränkt/erlaubt. Informationen zu den Standardrollen, die Zugriff auf die SOAP-Daten haben, finden Sie unter SOAP-Rollen .
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende SOAP-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Strikte Sicherheit für eingehende SOAP durchsetzen SOAP Web Service

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sichere Kommunikation (Härtung der Instanzsicherheit)

Die sicheren Kommunikationseigenschaften beziehen sich auf die Sicherheit der Übertragung von HTTP-Datenverkehr.

Zertifikatvertrauen (Härtung der Instanzsicherheit)

Standardmäßig ist die Eigenschaft *com.glide.communications.trustmanager_trust_all* auf **false**festgelegt. Now Platform vertraut nur Zertifikaten, die mit dem JVM-Zertifikatspeicher verifiziert werden können. Selbstsignierten und unternehmenssignierten Zertifikaten wird nicht vertraut.

Hinweis:
Die Werte für diese Eigenschaften sind Sichere Überschreibung und können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden). Ändern Sie diesen Eigenschaftswert aus Sicherheitsgründen nicht. Wenn Sie weitere Fragen haben, wenden Sie sich an Kundenservice und Support.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.communications.trustmanager_trust_all
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erzwingen Sie die Zertifikatvalidierung für ausgehende Anforderungen.
Empfohlener Wert	false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine strikte Validierung im Feld der Zertifizierungsstelle (Certificate Authority, Zertifizierungsstelle). Wenn eine vertrauenswürdige Entität (CA) das Zertifikat ausgegeben hat, akzeptiert die Instanz es zur weiteren Verwendung.
Sicherheitsrisiko	(Mittel) Aus Gründen der Vertraulichkeit und Integrität sollte die Anwendung die Zertifizierungsstelle des Zertifikats validieren, bevor das Zertifikat für Transaktionsvorgänge verwendet wird.
Referenzen	Zertifikate Verifizierung des HTTP-Client-Hostnamens

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

SSLv2/SSLv3 deaktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.outbound.sslv3.disabled`, um den MID Server zur Verwendung von TLS bei ausgehenden Verbindungen wie REST- und SOAP-Anforderungen zu zwingen. Normalerweise wird für ausgehende Verbindungen einer Instanz die Verwendung von TLS anstelle von SSL erzwungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ausgehend.sslv3.deaktiviert
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Verwendung von TLS für alle ausgehenden Verbindungen von der ServiceNow-Instanz zu erzwingen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Verwendung der TLS-Protokollversion bei der Kommunikation über HTTPS. Wenn Geräte vorhanden sind, die von Kunden/Benutzern der Instanz verwendet werden und die TLS-Kommunikation nicht unterstützen, kann dies zu einem potenziellen Ausfall führen.
Sicherheitsrisiko	(Mittel) Legacy-Versionen von SSL erwiesen sich bei Verwendung für die Implementierung der sicheren HTTP-Shell aufgrund von clientseitigen Angriffen, einschließlich BEAST und SSL-Heartbleed, als unsicher.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verifizierung des HTTP-Client-Hostnamens

Verwenden Sie *com.glide.communications.httpclient.verify_hostname*, um den Hostnamen und die Zertifikatkette zu überprüfen, die von Remote-SSL-Hosts dargestellt werden.

Setzen Sie *com.glide.communications.httpclient.verify_hostname* auf „ **true** “, um sich vor MitM-Angriffen (Man-in-the-Middle) zu schützen, bei denen die Kommunikation zwischen zwei Parteien abgefangen wird. Durch das Festlegen dieser Eigenschaft wird die Eigenschaft *com.glide.communications.trustmanager_trust_all* überschrieben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.communications.httpclient.verify_hostname*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Deaktivieren Sie den Zertifizierungsverifizierungsprozess, der alle Zertifizierungen in der Zertifizierungskette auswertet, indem der Widerrufsstatus überprüft wird.
Typ	wahr | falsch
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Ermöglicht die Verbindung eines nicht validierten Zertifikats mit als unsicherem Host.
Sicherheitsrisiko	(Mittel) Ermöglicht oder verhindert, dass der HTTP-Client ausnahmslos eine Verbindung zu einem potenziell schädlichen Hostnamen herstellt.
Referenzen	Zertifikate Zertifikatvertrauen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Zertifikatverifizierung widerrufen

Verwenden Sie diese Eigenschaft, um den Zertifizierungsverifizierungsprozess zu deaktivieren, der alle Zertifizierungen in der Zertifizierungskette durch Überprüfen des Widerrufstatus auswertet.

API-Aufrufe, die das Hochsicherheits-Plugin verwenden, möchten diese Eigenschaft möglicherweise konfigurieren. Wenn die vollständige Zertifizierungskette nicht im Instanz-Truststore definiert ist oder die verwendeten Zertifikate nicht mit einer OCSP-Widerrufsprüfung (Online Certificate Status Protocol) kompatibel sind, werden möglicherweise Fehler an die API-Aufrufe zurückgegeben.

Die Prüfung der Zertifikatwiderrufung kann deaktiviert werden, indem die Eigenschaft *com.glide.communications.httpclient.verify_revoked_certificate* auf **false festgelegt**wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler, die mit einer Unfähigkeit verbunden sind, die Prüfung durchzuführen, sind NPE, SSLPeerUnverifiedException, Zertifikat und Ausnahme. Diese Fehler können in eine HttpException eingeschlossen werden. Mehrere Faktoren können sich auf eine erfolgreiche Prüfung auswirken:

- Der URI muss für die Instanz zugänglich sein. Beachten Sie, dass die ursprüngliche OCSP-Implementierung möglicherweise keinen Zugriff auf eine Proxy-Verbindung hat.
- Der Referrer-OCSP-Service muss online sein, wenn die Prüfung durchgeführt wird.

Hinweis:
Die Werte für diese Eigenschaften sind Sichere Überschreibung und können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden). Wenn Sie weitere Fragen haben, wenden Sie sich an Kundenservice und Support.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.communications.httpclient.verify_revoked_certif`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Deaktivieren Sie den Zertifikatverifizierungsprozess, der alle Zertifikate in der Zertifikatkette auswertet, indem Sie den Sperrstatus überprüfen. Nur ein selbstsigniertes Serverzertifikat muss in den Instanz-Truststore geladen werden.
Typ	true | false
Standardwert	Wahr
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel)
Sicherheitsrisiko	(Mittel) API-Aufrufe mit dem Plugin „Hochsicherheit“ werden nicht mit einer OCSP-Widerrufsprüfung im Instanz-Truststore überprüft.
Referenzen	Zertifikate

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Best Practices für Sicherheit (Härtung der Instanzsicherheit)

Zusätzlich zu den Sicherheitskonfigurationen ist ein zusätzlicher manueller Aufwand erforderlich, um Now Platform Anwendungen täglich weiter zu sichern. Dieser Abschnitt enthält Sicherheitsaufgaben, die ein Administrator regelmäßig innerhalb eines bestimmten Zeitintervalls ausführen sollte.

Inhaltstypoptionen automatisch festlegen

X-Content-Type-Options-Antwort-HTTP-Header wird vom Server verwendet, um anzugeben, dass die in den Content-Type-Headern angegebenen MIME-Typen (Multifunktions-Internet-Mail-Erweiterungen) befolgt werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch das Festlegen dieser Kopfzeile wird verhindert, dass der Browser Dateien als etwas anderes interpretiert, als durch den Inhaltstyp in den HTTP-Kopfzeilen deklariert wird. Dieser Header kann dazu beitragen, MIME-Verwirrungsangriffe abzuschwächen.

Inhaltstypoptionen automatisch festlegen ist konform, wenn `glide.security.header.auto_set_x_content_type_options` auf „ **true**“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.header.auto_set_x_content_type_options`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verhindert, dass der Browser Dateien als etwas anderes interpretiert als durch den Inhaltstyp in den HTTP-Kopfzeilen deklariert.
Typ	wahr | falsch
Empfohlener Wert	**true**
Funktionale Auswirkung	(Hoch) Dieser Header kann dazu beitragen, MIME-Verwirrungsangriffe abzuschwächen.
Sicherheitsrisiko	(Hoch) Wenn diese Eigenschaft nicht aktiviert ist, kann der Browser den Inhaltstyp in den HTTP-Kopfzeilen falsch interpretieren.
Referenzen	Herunterladbare MIME-Typen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Cache-Control-HTTP-Header-Wert (Härtung der Instanzsicherheit)

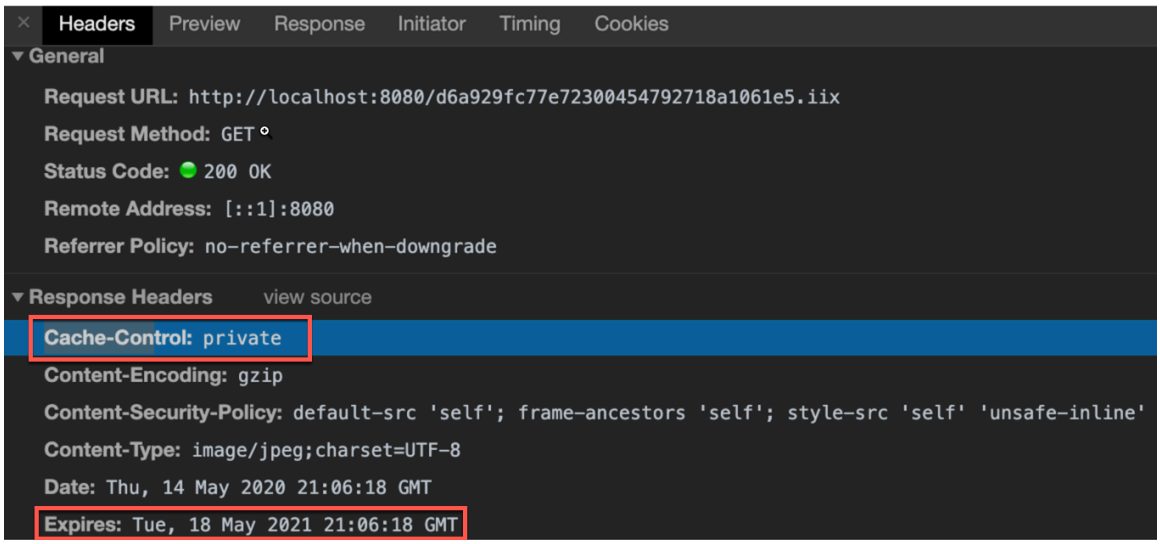
Verwenden Sie die Eigenschaft `glide.http.cache_control`, um den standardmäßigen Cache-Steuerungswert in den HTTP-Antwortkopfzeilen festzulegen, die von Now Platform gesendet werden, wenn statische Inhaltsdaten für eine Seite angefordert werden. Beispiele für statischen Inhalt sind Bilder, CSS und JavaScript, das in für eine Seite gerendert wird.

Die Eigenschaft `glide.http.cache_control` legt den Standardwert für Cache-Control in HTTP-Antwortheadern auf **private** oder **public**fest. Der Standardwert ist **privat**.

Wert	Beschreibung
Privat	Statische Inhalte können auf Browserebene (Client) zwischengespeichert werden, jedoch nicht auf Proxyserverebene.
Öffentlich	Statische Inhalte können auf Browserebene (Client) und auch auf Proxyserverebene zwischengespeichert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Wert für Ablauf in den HTTP-Antwortkopfzeilen steuert, wann der statische Inhalt abläuft. Er hat einen Standardwert von 369 Tagen. Um den Standardwert manuell zu überschreiben, verwenden Sie die Eigenschaft `glide.http.expire.days`.



Hinweis:
Sie können die Eigenschaft `glide.http.cache` verwenden, um festzulegen, ob die Einstellung der Werte für Cache-Steuerung und Ablauf in HTTP-Antwortheadern aktiviert oder deaktiviert werden soll. Der Standardwert ist **true**. Damit können Sie Folgendes festlegen:

- Cache-Control-Wert, Standard unter Verwendung der Eigenschaft `glide.http.cache_control`.
- Läuft standardmäßig mit der Eigenschaft `glide.http.expire.days` ab.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.http.cache_control
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So konfigurieren Sie den Cache-Control-HTTP-Antwortheaderwert für statischen Inhalt.
Empfohlener Wert	Privat
Funktionale Auswirkung	(Mittel) Legt den Standardwert für Cache-Control in einem HTTP-Antwortheader fest.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft auf „ **public**“ festlegen, können Instanzen mit CDN/Proxys statischen Inhalt zwischenspeichern und ohne Authentifizierung rendern. • **private** ist eine geeignetere Einstellung für Instanzen mit CDN/Proxy-Setup. • Wenn für die Instanz kein CDN/Proxy eingerichtet ist, sollte einer der Werte in Ordnung sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sicherheit für Berichte erzwingen

Deaktivieren Sie diese Eigenschaft, um zu verhindern, dass der Benutzer Berichte veröffentlicht oder darauf zugreift. Diese Eigenschaft deaktiviert die Funktion für veröffentlichte Berichte in der Berichterstellung.

Aktivieren Sie das Veröffentlichen von Berichten, indem Sie `glide.report.published_reports.enabled` auf **true**setzen.

Sicherheit für Berichte erzwingen ist konform, wenn `glide.report.published_reports.enabled` auf **false**festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.report.published_reports.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Deaktiviert die Funktion für veröffentlichte Berichte in der Berichterstellung.
Typ	wahr | falsch
Empfohlener Wert	**false**
Funktionale Auswirkung	(Mittel) Der Benutzer kann keine Berichte veröffentlichen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, können Benutzer möglicherweise auf Berichte zugreifen oder diese veröffentlichen, die vertrauliche Daten verfügbar machen. Durch das Veröffentlichen eines Berichts wird eine URL erstellt, über die jeder auf den Bericht zugreifen kann, einschließlich Personen, die keine Benutzer sind. Wenn jemand zur URL navigiert, wird der Bericht mit aktuellen Daten aus der Instanz generiert.
Referenzen	Berichte veröffentlichen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Hochsicherheits-Plugin (Härtung der Instanzsicherheit)

Wenn Sie das Plugin „High Security“ aktivieren, werden Hunderte verschiedener Konfigurationen erstellt oder aktualisiert, um die Sicherheitsstufe in Ihrer Instanz zu steuern. Diese Konfigurationen entschärfen viele der häufigsten OWASP-Angriffe, indem sie eine strikte Zugriffskontrolle, Eingabevalidierung und Ausgabecodierung ermöglichen.

Diese Konfigurationen umfassen:

- Zugriffssteuerung
- Business-Regeln
- Systemeigenschaften

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- UI-Richtlinienaktion
- Skriptaktionen
- Skripteinbindungen

Beispiel

Sehen Sie sich die Beispiele für die folgenden Eigenschaften an:

Eigenschaft	Thema
glide.ui.escape_all_script	Escape Jelly
glide.security.strict.actions	Überprüfen Sie die UI-Aktion vor der Ausführung
glide.security.csrf_ previous.allow	Anti-CSRF-Token
glide.security.csrf.strict.validation.mode	Strenge CSRF-Validierung

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.high_security
Konfigurationstyp	Systemdefinition > Plugins – Entwicklung
Zweck	Dieses Plugin muss aktiviert sein. Sie erhöht die Sicherheitsstufe einer Instanz, wodurch die Angriffsfläche reduziert wird, indem die 10 wichtigsten OWASP-Angriffe wie CSRF, XSS, Cookies für Sicherheitssitzungen und Datei-Uploads abgeschwächt werden.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Hoch) Dieses Plugin aktiviert mehrere Systemsicherheitskonfigurationen, die sich auch auf die Benutzeroberfläche und Funktionalität auswirken können.
Sicherheitsrisiko	(Hoch) Viele Sicherheitskonfigurationen werden unbeabsichtigt offen gelassen, was die Tür für einige der kritischen Schwachstellen öffnen kann.
Referenzen	Strenge Sicherheitseinstellungen werden aktiviert Strenge Sicherheitseinstellungen

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin .

Individuelle Anmelde-IDs (Härtung der Instanzsicherheit)

Stellen Sie sicher, dass alle Benutzer über individuelle Benutzer-IDs verfügen, wodurch alle Benutzeraktivitäten geprüft werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für lokale Benutzerkonten, die nicht verwendet werden, sollte die Kennzeichnung „ **Aktiv** “ auf „falsch“ gesetzt sein.

- Wenn Sie die Kennzeichnung **Aktiv** auf **false** setzen, wird die Kennzeichnung **Gesperrt** automatisch auf **true gesetzt**. Wenn die Kennzeichnung **Gesperrt** auf **true**gesetzt ist, kann sich dieser Benutzeraccount nicht bei der Instanz authentifizieren.
- Wenn Sie die Kennzeichnung **Aktiv** auf **false** setzen, wird ein Benutzer nicht aus dem Now Platformentfernt, aber die Sichtbarkeit für Nicht-Admin-Accounts wird aufgehoben.
- Wenn die Kennzeichnung „ **Aktiv** “ auf „ **false**“ und die Kennzeichnung **„Gesperrt“** ebenfalls auf **„false**“ festgelegt ist, kann sich ein Benutzer weiterhin bei diesem Account anmelden.

Weitere Informationen zu Benutzerkonten finden Sie unter Benutzeradministration .

Mobile-UI-Verschleierung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.m.blur_ui_when_backgrounded*, um alle Felder aus dem Snapshot zu verschleiern, da das Bild während des Hintergrundprozesses gespeichert wird. zu verschleiern.

Auf Android-Geräten erstellt das Android-Betriebssystem einen Screenshot zur Verwendung im Menü „Letzte Aufgabe“, wenn die Anwendung in den Hintergrund gesendet wird. Benutzer können auch manuelle Screenshots der Anwendung erstellen, die öffentlich auf dem Gerät gespeichert werden.

Auf iOS-Geräten ermöglicht das iOS-Betriebssystem Anwendungen auch das Speichern einer Bilddatei. Diese Datei stellt den letzten Bildschirm dar, den der Benutzer gesehen hat, wenn die Anwendung in den Hintergrund gesendet wurde. Dies soll zwar eine bessere Benutzer-Experience bieten, stellt jedoch auch ein Sicherheitsrisiko dar, da die Bilder als PNG-Bilddateien gespeichert werden.

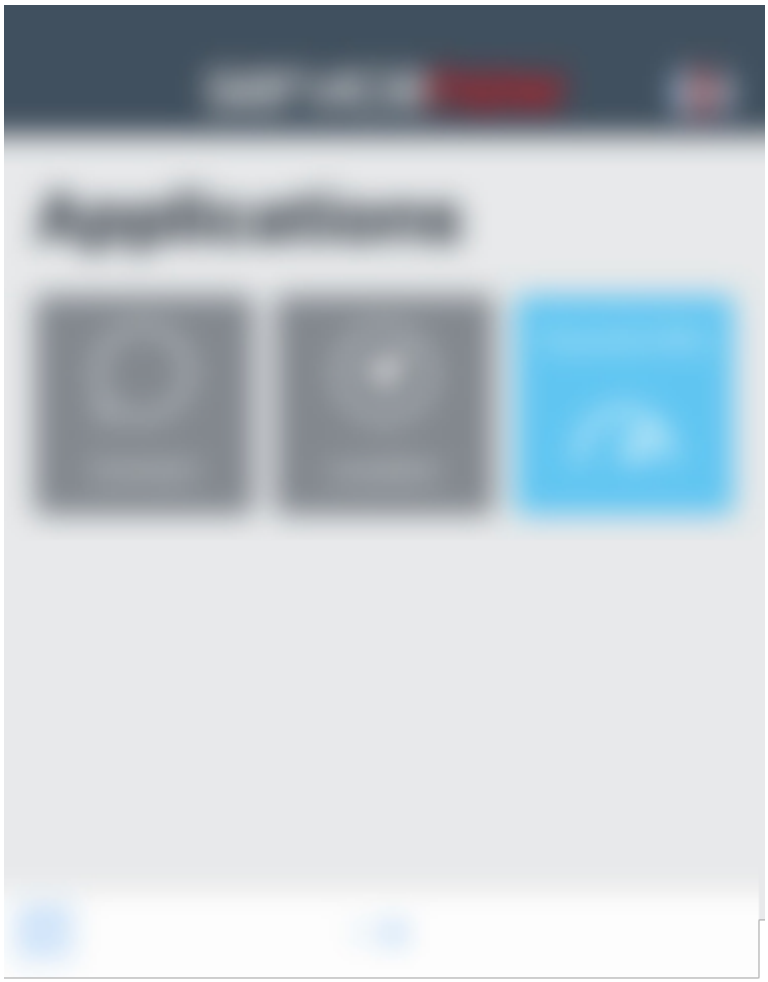
Hinweis:
Diese Einstellung oder Konfiguration ist pro Instanz, daher muss der Benutzer eine Verbindung zur Instanz mit der konfigurierten Eigenschaft herstellen.

Informationen zum Verschleiern aller Felder aus dem Snapshot in der ServiceNow Classic-App finden Sie unter App-Unscharf-Option zur Verbesserung der Sicherheit konfigurieren .

Beispiel

Wenn Sie diese Eigenschaft auf **true**festlegen. Die Hintergrundanwendung ist für iOS-Geräte verschleiert und für Android iOS-Geräte gesperrt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen

Attribut	Beschreibung
Eigenschaft/Plugin-Name	glide.ui.m.blur_ui_when_backgrounded
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	Um alle Felder aus dem Snapshot zu verschleiern, wenn das Bild während des Hintergrundprozesses gespeichert wird.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft `glide.ui.m.blur_ui_when_backgrounded` auf „**true**“ festgelegt ist, verwenden die nativen Apps den auf dem Server definierten Parameter, um den Bildschirm unscharf zu machen, wenn die App in den Hintergrund wechselt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Die von iOS und Android aufgenommenen Screenshots werden unscharf, wenn die App in den Hintergrund wechselt. • Die Benutzer-Experience kann beeinträchtigt werden, da sie den Inhalt nicht sehen können, wenn die App in den Hintergrund gesendet wird.
Sicherheitsrisiko	(Mittel) Ein gefährdetes Gerät (mit Jailbreak) ermöglicht einem Angreifer vollständigen Zugriff auf das Dateisystem und den Zugriff auf Dateien/Snapshots mit eingebetteten vertraulichen Informationen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Patches und Updates (Härtung der Instanzsicherheit)

Stellen Sie sicher, dass auf der Instanz die aktuelle Patch-Ebene ausgeführt wird. Sicherheitsfixes werden regelmäßig für Now Platform im Rahmen vieler Patches und Hotfixes veröffentlicht, die mit Produktfunktions-Updates geliefert werden. Ein Upgrade, wenn neue Patches und Hotfixes verfügbar sind, reduziert das Risiko potenzieller Schwachstellen.

Now Platform durchläuft durchschnittlich zwei Penetrationstests pro Woche.

- Während die meisten dieser Tests keine signifikanten Schwachstellen ergeben, werden regelmäßig Schwachstellen gefunden und behoben.
- Informationen zu Releases, Patches und Hotfixes von Now Platform finden Sie im Abschnitt „Release-Hinweise“ der Produktdokumentation. Weitere Informationen finden Sie in den Versionshinweisen zu Upgrades .

Demodaten entfernen (Härtung der Instanzsicherheit)

Demodaten, insbesondere Demokonten, werden normalerweise beim Erstellen einer Instanz berücksichtigt. Wenn dies der Fall ist, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird.

Öffnen Sie eine Anforderung in HI. Stellen Sie sicher, dass Sie ein Administratorkonto erstellen, bevor Sie die Anforderung senden.

Es wird dringend empfohlen, die Entfernung von Demodaten in der Produktion erfolgreich auf einer Test- und Entwicklungsumgebungsinstanz zu überprüfen, die ein aktueller Klon der Produktionsinstanz ist.

Interne Ressourcen

https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107

https://community.servicenow.com/community?id=community_blog&sys_id=786eaeaddbd0dbc01dcaf3231f961959

Demodaten mit dem Servicekatalog entfernen

Anstatt die Anforderung als Incident zu übermitteln, können bestimmte Benutzer die Entfernung von Demodaten für eine Instanz mithilfe des Servicekatalogs anfordern. Zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diesen Benutzern gehören interne Benutzer und Benutzer mit den Rollen „customer_admin“ oder „partner_admin“.

1. Navigieren Sie zu https://support.servicenow.com/now .
2. Geben Sie die Instanz an, aus der Demodaten entfernt werden sollen.

   Wenn Sie Probleme haben, Ihre Instanz zu finden, stellen Sie dem Instanznamen * voran, um eine Enthält-Abfrage durchzuführen.
3. Klicken **Selfservice** > **Demodaten entfernen** > **.**
4. Geben Sie das Datum und die Uhrzeit zum Entfernen der Demodaten aus der ausgewählten Instanz an.

   Das Datum und die Uhrzeit müssen mindestens vier Stunden nach der aktuellen Uhrzeit liegen.
5. Klicken Sie auf **Absenden**.

Eine neue Change-Anforderung wird erstellt und automatisch angezeigt. Das **geplante Enddatum** wird automatisch basierend auf dem **geplanten Startdatum** plus fünf Stunden berechnet, d. h. die Dauer des Prozesses. Im Change Request. Verwenden Sie die Beobachtungsliste, um weitere Mitglieder Ihres Teams hinzuzufügen, die über den Status der Change-Anforderung Bescheid wissen müssen.

Sicherheitsaufnahmeliste (Härtung der Instanzsicherheit)

Ein „positives“ Sicherheitsmodell (auch als „Aufnahmeliste“ bezeichnet) definiert, was zulässig ist, und lehnt alles andere ab. Dieser Abschnitt enthält Sicherheitskontrollen, die ein Administrator konfigurieren kann, um das Verhalten auf bekannte Aufnahmelisten zu beschränken.

Hinweis:
Eigenschaften der Sicherheitsaufnahmeliste müssen in jeder Instanz manuell eingerichtet werden, da Update Sets die Konfiguration nicht heraufstufen und einen Fehler zurückgeben.

Aufrufe von Allow-Listenmitgliedern überprüfen (Härtung der Instanzsicherheit)

Überprüfen und entfernen Sie die Aufrufeinträge für Aufnahmelistenmitglieder nach Bedarf aus der Tabelle „sys_whitelist_member“.

Mitgliedsaufrufeinträge können auf die Java-Ressourcen auf der Serverseite zugreifen, um anwendungsbasierte Vorgänge ohne entsprechende Validierung auszuführen. Da dies zu unbefugten Offenlegungen oder Änderungen von Kundendaten führen kann, stellt dies ein erhebliches Sicherheitsrisiko dar.

Weitere Informationen

Attribut	Beschreibung
Tabellenname	sys_whitelist_member **Hinweis:** In den letzten Releases können nur ServiceNow-Mitarbeiter auf diese Tabelle zugreifen. nicht einmal Administratoren sind dazu in der Lage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Tabelle
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Überprüfen und Entfernen von Einträgen aus dieser Tabelle.
Empfohlener Wert	In der Tabelle darf kein Datensatz vorhanden sein (die Liste muss leer sein).
Funktionale Auswirkung	(Niedrig) Es sollte keine Auswirkungen geben, solange Sie die Ergebnisse überprüfen und genehmigen, die beim Ausführen des Tools zum Entfernen von Paketaufrufen generiert werden. Um sicherzustellen, dass die Instanz ordnungsgemäß funktioniert, testen Sie die Änderungen in einer Nicht-Produktionsumgebung, bevor Sie sie in der Produktionsumgebung bereitstellen. Weitere Informationen finden Sie unter Tool zur Paketaufrufentfernung.
Sicherheitsrisiko	(Hoch) Clientseitige API-Aufrufe, die zum Datenabruf oder Objektzugriff auf dem Server führen, gelten aus Sicherheitsgründen als gefährlich. Validieren Sie diese Elemente für die Autorisierung und Einschränkung des Zugriffs auf vertrauliche Objekte.

Schritte zum Konfigurieren von

Hinweis:
Die folgenden Schritte ähneln den Schritten, die in den Abschnitten „Schritte zum Konfigurieren“ in beschrieben werden:

- Tool zur Paketaufrufentfernung
- Aktivieren Sie die Allow-Liste für Paketaufrufe

Wenn Sie sie bereits abgeschlossen haben, können Sie diese Schritte überspringen.

1. Aktivieren Sie das Plugin „Packages Call Removal Tool“. Weitere Informationen finden Sie unter Tool zur Paketaufrufentfernung.
2. Navigieren Sie im **Filternavigator zu Pakete Dienstprogramm**zur Entfernung von Aufrufen.
3. Klicken Sie auf jedes Skript von (1) bis (4). Warten Sie auf die Ausgabe, und fahren Sie dann mit der nächsten fort.
4. Sobald Sie das Skript (4) ausgeführt haben, wird eine Liste der betroffenen Felder auf der Seite „Paketaufruf-Elemente“ angezeigt.
5. Lösen Sie alle Elemente in den Abschnitten „Vorgeschlagen“ und „Fehler“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieses Tool meldet möglicherweise einige Paketaufrufe, die in „sa_mapping_ext_commands“ und „sa_custom_operation“verwendet werden. Diese Paketaufrufe gehören zum MID Server. Da keine Klassen vorhanden sind, wird der Code in MID Server ausgeführt. Wenn Sie die folgenden Mitgliedsaufrufe im Abschnitt „Fehler“ finden, markieren Sie sie als „ **Abgelehnt** (Ignoriert)“. Das Tool meldet diesen Mitgliedsanruf nicht mehr.

- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);
- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);
- Packages.com.snc.sw.commands.HttpCallHandler;
- Packages.com.snc.sw.dto.ProviderType.SSH

6. Wenden Sie sich an den ServiceNow -Support, um weitere Korrekturen zu erhalten.

Paketaufrufe für Allow-Liste überprüfen (Härtung der Instanzsicherheit)

Überprüfen und entfernen Sie die Paketaufrufeinträge der Aufnahmeliste nach Bedarf aus der Tabelle „sys_whitelist_package“.

Paketaufrufeinträge können serverseitig auf Java-Ressourcen zugreifen, um anwendungsbasierte Vorgänge ohne entsprechende Validierung auszuführen. Da dies zu unbefugten Offenlegungen oder Änderungen von Kundendaten führen kann, stellt dies ein erhebliches Sicherheitsrisiko dar.

Weitere Informationen

Attribut	Beschreibung
Tabellenname	sys_whitelist_package **Hinweis:** In den letzten Releases kann nur Kundenservice und Support auf diese Tabelle zugreifen. nicht einmal Administratoren sind dazu in der Lage.
Konfigurationstyp	Tabelle
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Überprüfen und Entfernen von Einträgen aus dieser Tabelle.
Empfohlener Wert	In der Tabelle darf kein Datensatz vorhanden sein (die Liste muss leer sein).
Funktionale Auswirkung	(Niedrig) Es sollte keine Auswirkungen geben, solange die Ergebnisse der Ausführung des Tools zum Entfernen von Paketaufrufen überprüft und genehmigt werden. Um sicherzustellen, dass die Instanz ordnungsgemäß funktioniert, testen Sie die Änderungen in einer Nicht-Produktionsumgebung, bevor Sie sie in der Produktionsumgebung bereitstellen. Weitere Informationen finden Sie unter Tool zur Paketaufrufentfernung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Clientseitige API-Aufrufe, die zum Datenabruf oder Objektzugriff auf dem Server führen, gelten aus Sicherheitsgründen als gefährlich. Validieren Sie diese Elemente für die Autorisierung und Einschränkung des Zugriffs auf vertrauliche Objekte.
Workaround	Wenden Sie sich an den Support von ServiceNow, um Unterstützung zu erhalten.

Schritte zum Konfigurieren von

1. Aktivieren Sie das Plugin „Packages Call Removal Tool“. Weitere Informationen finden Sie unter Tool zur Paketaufrufentfernung.
2. Navigieren Sie im **Filternavigator zu Pakete Dienstprogramm**zur Entfernung von Aufrufen.
3. Klicken Sie auf jedes Skript von (1) bis (4). Warten Sie auf die Ausgabe, und fahren Sie dann mit der nächsten fort.
4. Sobald Sie das Skript (4) ausgeführt haben, wird eine Liste der betroffenen Felder auf der Seite „Paketaufruf-Elemente“ angezeigt.
5. Lösen Sie alle Elemente in den Abschnitten „Vorgeschlagen“ und „Fehler“.

   Hinweis:
   Dieses Tool meldet möglicherweise einige Paketaufrufe, die in „sa_mapping_ext_commands“ und „sa_custom_operation“verwendet werden. Diese Paketaufrufe gehören zum MID Server. Da keine Klassen vorhanden sind, wird der Code in MID Server ausgeführt. Wenn Sie die folgenden Paketaufrufe im Abschnitt „Fehler“ finden, markieren Sie sie als **Abgelehnt** (Ignoriert). Das Tool meldet diesen Paketaufruf nicht mehr.

   - Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);
   - Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);
   - Packages.com.snc.sw.commands.HttpCallHandler;
   - Packages.com.snc.sw.dto.ProviderType.SSH

6. Wenden Sie sich an den ServiceNow -Support, um weitere Korrekturen zu erhalten.

URL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.concourse.onmessage_enforce_same_origin*, um die ursprungsübergreifende Kommunikation zwischen iframeszu ermöglichen.

OpenFrame kann nur Nachrichten aus vertrauenswürdigen Domänen verarbeiten, die in der Eigenschaft *glide.ui.concourse.onmessage_enforce_same_origin_whitelist* angegeben sind. Weitere Informationen finden Sie unter UTL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation angeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.concourse.onmessage_enforce_same_origin
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So aktivieren Sie die Aufnahme von vertrauenswürdigen Domänen, damit sie zwischen IFrames für OpenFrame kommunizieren können.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Wenn Sie beabsichtigte Domänen nicht in die Aufnahmeliste aufnehmen, kann die Möglichkeit zum Einbetten anderer Seiten in Now Platform Instanzen eingeschränkt sein.
Sicherheitsrisiko	(Hoch) Wenn eine Webseite Event-Handler enthält, die keine ordnungsgemäße Ursprungsvalidierung durchführen, kann eine Webseite oder ein Skript von einem beliebigen Ursprung mit ihr kommunizieren. Sie kann auch alle vom Event Handler ausgeführten Funktionen initiieren.
Referenzen	OpenFrame-Übersicht

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Relative Links erzwingen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.cms.catalog_uri_relative`*, um relative Links aus dem URI-Parameter für `/ess/catalog.do`zu erzwingen.

- Bei Festlegung auf **true**werden nur relative URLs über die Seite `/ess/catalog.do` mit dem Parameter *`uri`* zugelassen.
- Bei **false**sind alle URLs zulässig, was die Verknüpfung mit externen, nicht autorisierten Inhalten ermöglichen kann.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.cms.catalog_uri_relative
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um Versuche einzuschränken, externe nicht autorisierte Inhalte zu verknüpfen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt die Validierung auf der Katalogseite, sodass nur relative URLs zulässig sind. Vorhandene Links zu externen Webanwendungen werden unterbrochen.
Sicherheitsrisiko	(Hoch) Absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil eines Parameters oder Feldwerts verwendet werden, wodurch die Quellseite auf eine von Angreifern kontrollierte Website umgeleitet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Tool zur Paketaufrufentfernung (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin „Packages Call Removal Tool“ (`com.glide.script.packages_call_removal`), und führen Sie es aus, und überlegen Sie dann, ob jede der vorgeschlagenen Änderungen abgeschlossen oder abgelehnt werden soll.

Das Tool zur Paketaufrufentfernung ist ein Plugin, das:

- Durchsucht Skripts nach Paketaufrufen für Now Platform Java-Klassen.
- Schlägt Änderungen vor, um sie durch bevorzugte GlideScriptable-Namen zu ersetzen.
- Erleichtert die Skriptänderungen.

Hinweis:
Wenn es sich bei diesem Datensatz um einen Basissystemdatensatz handelt, wird das Element bei Verwendung der Empfehlung des Tools als customer_update markiert. Dieses Skript wird in Zukunft möglicherweise nicht mehr aktualisiert. In späteren Releases wird erwartet, dass die Tabellen sys_whtelist_xxx leer sind. Es kann jedoch dennoch nützlich sein, dieses Tool zu verwenden, da es Packages,xxx-Aufrufe kennzeichnet.

Das Tool zur Paketaufrufentfernung meldet möglicherweise einige Paketaufrufe, die in „sa_mapping_ext_commands“ und „sa_custom_operation“verwendet werden. Diese Paketaufrufe gehören zum MID Server. Da keine Klassen vorhanden sind, wird der Code in MID Server ausgeführt. Wenn Sie einen der folgenden aufgelisteten Paketaufrufe im Abschnitt „Fehler“ finden, markieren Sie ihn als Abgelehnt (Ignoriert). Das Tool meldet diesen Paketaufruf nicht mehr.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
- `Packages.com.snc.sw.commands.HttpCallHandler;`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

Weitere Informationen

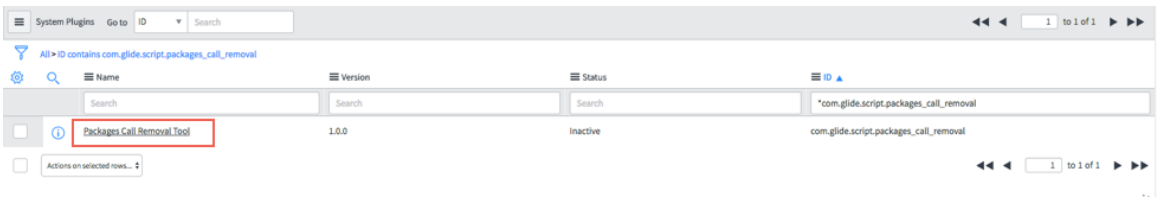
Attribut	Beschreibung
Plugin-Name	com.glide.script.packages_call_removal
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Entfernen/Ersetzen nicht autorisierter Paket-/Mitgliedsaufrufe mit von Glide akzeptierten Namen (GlideScriptable), die nur autorisierten Zugriff auf Daten zulassen.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Paketaufrufe durch `GlideScriptable-` APIs ersetzen und kann sich auf die Anpassungen auswirken, die Paketaufrufe enthalten. Das Tool ersetzt Paketaufrufe nicht automatisch. Stattdessen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

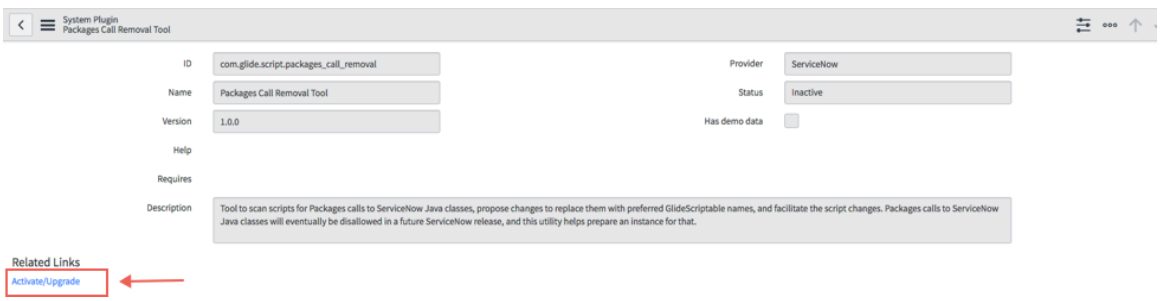
Attribut	Beschreibung
	werden Vorschläge bereitgestellt, die in der Tabelle „packages_call_item“ gespeichert werden. Ihr Administrator kann dann entscheiden, ob er die vorgeschlagene Änderung akzeptiert oder ablehnt.
Sicherheitsrisiko	(Mittel) Clientseitige API-Aufrufe, die zum Datenabruf oder Objektzugriff auf dem Server führen, gelten aus Sicherheitsgründen als gefährlich. Sie sollten auf Autorisierung und Einschränkung für den Zugriff auf vertrauliche Objekte validiert werden.

Schritte zum Konfigurieren von

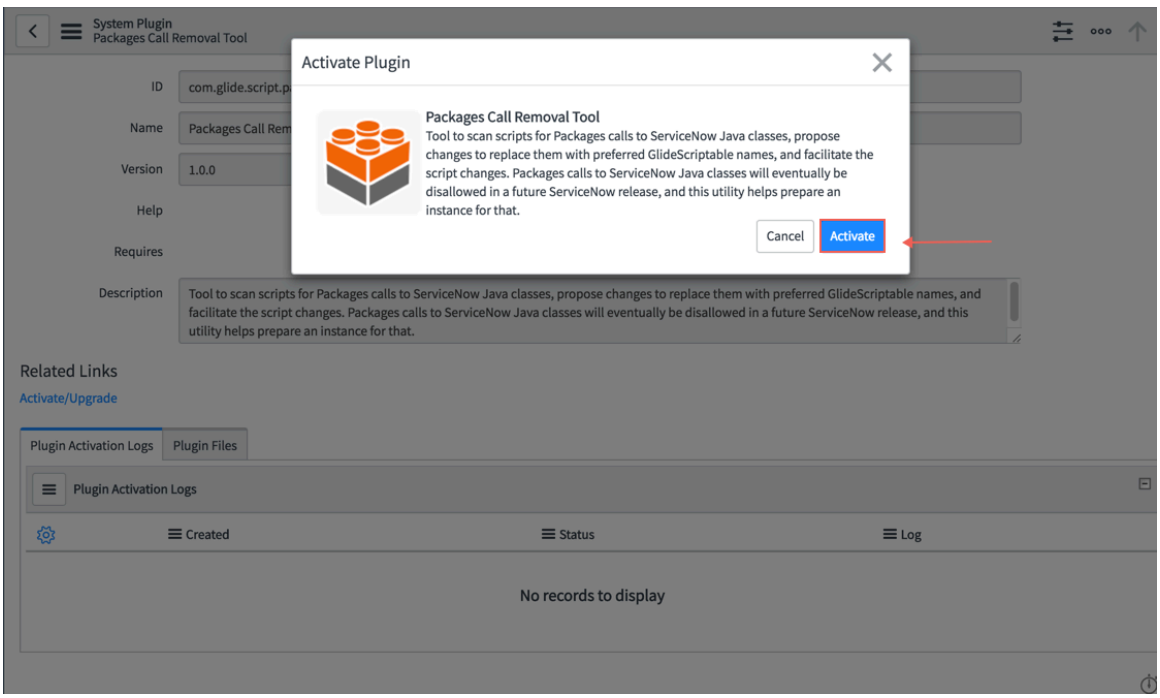
1. Navigieren zu **Systemdefinition** > **Plugins**



2. Suchen Sie nach der Plugin-ID = `com.glide.script.packages_call_removal`.



3. Klicken Sie auf **Aktivieren/Aktualisieren**, um das Plugin zu aktivieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Um Aufrufe von Aufnahmelistenpaketen und Aufnahmelistenmitgliedern zu überprüfen, führen Sie die Aktionen aus, die in den Abschnitten „Schritte zum Konfigurieren“ in den folgenden Themen beschrieben sind:
   - Aktivieren Sie Listenmitgliedsaufrufe zulassen
   - Aktivieren Sie die Allow-Liste für Paketaufrufe

URL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation angeben (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.concourse.onmessage_enforce_same_origin_whitelist`, um die ursprungsübergreifende Kommunikation zwischen IFrames aus vertrauenswürdigen Domänen zu ermöglichen, die Sie in einer Aufnahmeliste angeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.concourse.onmessage_enforce_same_origin_whitelist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Zum Aktivieren der Aufnahmeliste von vertrauenswürdigen Domänen, damit sie zwischen IFrames für OpenFrame kommunizieren können.
Anforderung	Obligatorisch
Funktionale Auswirkung	(Mittel) Wenn Sie beabsichtigte Domänen nicht in die Aufnahmeliste aufnehmen, kann die Möglichkeit zum Einbetten anderer Seiten in den Now Platform -Instanzen eingeschränkt sein.
Sicherheitsrisiko	(Hoch) Wenn eine Webseite Event-Handler enthält, die keine ordnungsgemäße Ursprungsvalidierung durchführen, kann eine Webseite oder ein Skript von einem beliebigen Ursprung mit ihr kommunizieren. Sie kann auch alle vom Event Handler ausgeführten Funktionen initiieren. Die Kommunikation mit IFrames aus anderen Domänen stellt ein Sicherheitsrisiko dar.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

URL-Allow-Liste für Abmeldeumleitungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.security.url.whitelist`, um eine zusätzliche Validierungsebene hinzuzufügen, um sicherzustellen, dass eine eingeführte externe URL Teil der URLs auf der Aufnahmeliste sein soll.

Eine offene Umleitung tritt auf, wenn eine angreifbare Webseite auf eine nicht vertrauenswürdige und schädliche Seite umgeleitet wird, die den Benutzer gefährden kann. Offene Umleitungsangriffe gehen mit einem Phishing-Angriff einher, da der geänderte angreifbare Link mit der ursprünglichen Website identisch ist, was die Erfolgswahrscheinlichkeit des Phishing-Angriffs erhöht.

Diese Eigenschaft ist in den folgenden Fällen anwendbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- /logout.do?sysparm_goto_url={Externe URL}
- /cms_login_redirect.do?sysparm_goto_url={Externe URL}

Benutzer werden zu einer externen vertrauenswürdigen Site weitergeleitet, nachdem sie sich von der Instanz abgemeldet haben:

- /logout_redirect.do?sysparm_url={Externe URL}
- /saml_redirector.do?sysparm_uri={Externe URL}

Wenn SAML aktiviert ist, wird eine Abmelde-URL eines Identitätsanbieters (IDP) aufgerufen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.url.whitelist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Implementieren einer sicheren URL-Umleitung während der Anmeldung, Abmeldung oder anderen Umleitungen. Diese Eigenschaft mindert einen der 10 häufigsten OWASP-Angriffe mit der Bezeichnung „Ungültige Umleitungen und Weiterleitungen“.
Typ	Kommage und Leerzeichen getrennte Zeichenfolge. Beispiel: https://example.com, https://wiki.example.com.
Wert	Die genehmigten URLs Ihrer Organisation [Einige definierte FQDNs (vollständig qualifizierter Domänenname)] Bsp. http://www.servicenow.com]
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Validierung auf der Abmeldeseite. Sie kann funktionale Auswirkungen auf einen Benutzer einer Instanz mit einer SSO/SAML-Konfiguration haben.
Sicherheitsrisiko	(Hoch) Clientseitige offene Umleitung ermöglicht es Angreifern, Opfer/Anwender auf die vom Angreifer kontrollierte Website umzuleiten, und wird als Sicherheitsrisiko angesehen.
Referenzen	Multi-SSO (SAML 2.0) – Fehler und Korrekturen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sicherheitsrichtlinie für in Virtual Agent eingebettete Client-Inhalte (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *com.glide.cs.embed.csp_frame_ancestors*, um die Konfiguration der Richtlinie „frame-ancestors“ nur für https:// zu aktivieren.<your-instance> Seite .service-now.com/sn_va_web_client_app_embed.do

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Virtual Agent-Plugin ermöglicht die Einbettung eines Clients in eine externe Webseite. Damit die Client-Seite in die Webseite eingebettet werden kann, muss die Inhaltssicherheitsrichtlinie die externe Seite als übergeordneten Frame zulassen.

Hinweis:
Vermeiden Sie es, nur „*“ als Inhaltssicherheitsrichtlinie zu verwenden, da dadurch alle Domänen aktiviert würden und die Anwendung potenziell angreifbar für Clickjacking wäre.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.cs.embed.csp_frame_ancestors
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Ermöglicht die Erstellung einer benutzerdefinierten Inhaltssicherheitsrichtlinie für die einbettbare Virtual Agent-Seite.
Empfohlener Wert	Legen Sie vertrauenswürdige Domänen fest
Funktionale Auswirkung	(Hoch) Der einbettbare Virtual Agent-Client lässt nicht zu, dass er in externe Websites eingebettet wird, es sei denn, die Inhaltssicherheitsrichtlinie ist ordnungsgemäß konfiguriert.
Sicherheitsrisiko	(Mittel) Bei falscher Konfiguration (alle übergeordneten Frames werden zugelassen) kann die einbettbare Client-Seite möglicherweise angreifbar für Clickjacking sein.
Referenzen	Betten Sie den Virtual Agent-Webclient in eine externe Webseite ein Weitere Informationen zum Erstellen einer Inhaltssicherheitsrichtlinie für frame-ancestors finden Sie hier.

Schritte zum Konfigurieren von

1. Navigieren zu **/sys_properties_list.do**.
2. Suchen Sie nach der Eigenschaft *com.glide.cs.embed.csp_frame_ancestors*.
3. Weisen Sie eine akzeptable Sicherheitsrichtlinie für Inhalte zu (nur Unternehmens- oder andere akzeptierte Domänen zulassen), und klicken Sie dann auf **Aktualisieren**.

X-Frame-Options des in Virtual Agent eingebetteten Clients (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *com.glide.cs.embed.xframe_options*, um die Konfiguration des X-Frame-Headers nur für https:// zu aktivieren.<your-instance> Seite .service-now.com/sn_va_web_client_app_embed.do

Das Virtual Agent-Plugin ermöglicht die Einbettung eines Clients in eine externe Webseite. Damit die Client-Seite in die Webseite eingebettet werden kann, muss der X-Frame-Options-Header die Einbindung des IFrame in den übergeordneten Frame ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Vermeiden Sie die Verwendung von `allow-from *` als Headerwert für X-Frame-Options, da dadurch alle Domänen aktiviert würden und die Anwendung potenziell angreifbar für Clickjacking wäre.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.cs.embed.xframe_options
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Zum Aktivieren der Spezifikation der Direktive für den X-Frame-Options-Header für die einbettbare Virtual Agent-Seite.
Empfohlener Wert	gleicher Ursprung
Funktionale Auswirkung	(Hoch) Der einbettbare Virtual Agent-Client kann nicht in externe Websites eingebettet werden, es sei denn, der X-Frame-Options-Header ist ordnungsgemäß konfiguriert.
Sicherheitsrisiko	(Mittel) Bei falscher Konfiguration (alle übergeordneten Frames werden zugelassen) kann die einbettbare Client-Seite möglicherweise angreifbar für Clickjacking sein.
Referenzen	Betten Sie den Virtual Agent-Webclient in eine externe Webseite ein

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

X-Frame-Options: SAMEORIGIN (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.set_x_frame_options`*, um den X-Frame-Options-Antwortheader für alle UI-Seiten auf SAMEORIGIN festzulegen.

Verwenden Sie den X-Frame-Options-HTTP-Antwortheader, um anzugeben, ob der Browser eine Seite in <frame> oder <iframe>rendern darf. Websites können diese Funktion verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihr Inhalt nicht in andere Websites eingebettet wird. Ein Angreifer könnte Ihre Seite in seine eigene Seite einbetten und Ihre Seitenelemente in böswilliger Absicht ausführen. Der Endbenutzer denkt möglicherweise, dass die Seite legitim ist, da sie Ihrer Seite ähnelt. Der Endbenutzer kann wie gewohnt auf Elemente klicken, um schädliche Skripts oder Elemente auszuführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.set_x_frame_options
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zur Abwehr von ClickJaking-Angriffen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung für das Rendern einer Now Platform -Anwendung in einer Drittanbieteranwendung in Form eines iFrame. Wenn Sie über eine solche Integration verfügen, wird die Anwendung in der benutzerdefinierten Drittanbieter-App nicht gerendert.
Sicherheitsrisiko	(Mittel) Mit der Richtlinie „Same Origin“ können Sie verhindern, dass eine Domäne ein Skript oder eine Ressource aus einer anderen Domäne abruft. Alle modernen Browser unterstützen diese Funktionalität. Die Richtlinie validiert die Verbindung basierend auf Protokoll, Port und Host. CORS (Cross Origin Request) ist eine Änderung der Richtlinie für denselben Ursprung, die den Zugriff auf Ressourcen/ Skripts aus einer anderen Domäne ermöglicht, wenn dies explizit als Teil des Headerwerts angegeben wird. • In diesem Fall steuert die **X-Frame-Options-** Kopfzeile, ob die Anwendung Now Platform auf der Drittanbieter-Website gerendert werden kann. • Dadurch wird das sensible Risiko reduziert, da der Eigenschaftswert bei Einstellung auf **SAMEORIGIN** das Rendern nicht ermöglicht.
Referenzen	Verfügbare Systemeigenschaften iFrames konfigurieren

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Validierung der externen XML-Entitätsverarbeitung

Diese Eigenschaften ermöglichen die Entitätserweiterung und schränken externe Entitäten (z. B. URLs) ein, wenn sie als Teil der XML-DOCTYPE-Referenz enthalten sind. DTD ist im Grunde ein XML-Schema. Wenn Sie nach einer Lösung für Entitätsdeklarationen suchen, die Potenzial für XXE (externe Entität) haben könnten, aktivieren Sie mithilfe der Systemeigenschaften einen auf der Aufnahmeliste aufgeführten Schutz gegen XXE.

Für XMLDocument- und XMLUtil-Analyse

Wenn Ihre Anpassungen `XMLDocument` oder `XMLUtil` verwenden, legen Sie die folgenden Systemeigenschaften fest. Sie steuern die Entitätserweiterung und ermöglichen die Validierung externer Entitäten, die die Verarbeitung nur von Entitäten in Aufnahmelisten zulassen.

Schwellenwert für Entitätserweiterung festlegen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.xmlutil.max_entity_expansion`*, um die maximale Entitätserweiterungsgrenze in eine kleinere Zahl zu ändern.

Now Platform verarbeitet keine weiteren Entitätserweiterungen, die größer als der in dieser Eigenschaft angegebene zulässige Grenzwert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
3000 ist das von Now Platformvorgegebene Standardminimum, das als sicherer Schwellenwert gilt. Daher betrachtet die Plattform dieses Standardminimum, wenn der von Ihnen eingegebene ganzzahlige Wert unter 3000 liegt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.xmlutil.max_entity_expansion
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich vor XML-Entitätserweiterungs-/Billion-Lach-Angriffen zu schützen.
Empfohlener Wert	3000
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung die Erweiterung großer Entitäten verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann diese Schwachstelle verwenden, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.xml.entity.whitelist.enabled`, um die Validierung einer externen Entität zu aktivieren. Sie lässt nur die Verarbeitung von Entitäten zu, die auf der Aufnahmeliste stehen.

- Wenn Sie diese Eigenschaft auf **true**festlegen, werden nur Entitäten verarbeitet, die in die Aufnahmeliste aufgenommen wurden (empfohlene Einstellung).
- Wenn Sie diese Eigenschaft auf **false**festlegen, wird die Verarbeitung aller externen Entitäten ermöglicht.

Voraussetzungen

Definieren Sie vor dem Festlegen dieser Eigenschaft eine Liste der durch Kommas getrennten FQDNs in der Eigenschaft `glide.xml.entity.whitelist`. Dies sind die einzigen URLs, die über die XML-Entitätsverarbeitung erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.xml.entity.whitelist.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XXE-Angriffe zu schützen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine externe Entität verwendet, die nicht in der Eigenschaft [`glide.xml.entity.whitelist` aufgeführt ist, blockiert Now Platform möglicherweise die weitere Verarbeitung. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann die DTD verwenden, um beliebige HTTP-Anforderungen einzubeziehen, die der Server ausführen kann. Dies kann zu anderen Angriffen führen, die die Vertrauensstellung des Servers zu anderen Entitäten nutzen.
Workaround	Wenn Sie die Erweiterung externer Entitäten nicht verwenden, deaktivieren Sie sie. Weitere Informationen finden Sie unter Entitätserweiterung deaktivieren.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Für XMLDocument2-Parser

Wenn Ihre Anpassungen einen XMLDocument2-Parser verwenden, verwenden Sie die folgenden Systemeigenschaften, um die Validierung externer Entitäten zu aktivieren.

Entitätserweiterung deaktivieren (Härtung der Instanzsicherheit)

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie die Eigenschaft `glide.stax.allow_entity_resolution`, um die Erweiterung externer Entitäten vollständig zu deaktivieren. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

- Wenn Sie diese Eigenschaft auf **true**festlegen, versuchen alle externen Entitäten, abhängig von der Einstellung der Eigenschaft `glide.stax.whitelist_enabled`, Betreffentitäten aufzulösen oder zu erweitern.
- Wenn Sie diese Eigenschaft auf „ **false**“ festlegen, werden alle Entitätsauflösungen und -erweiterungen blockiert. Weitere Informationen finden Sie unter XMLdoc2-Entitätsvalidierung mit Allow-Liste.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaften `glide.xml.entity.whitelist.enabled` und `glide.stax.whitelist_enabled` auf „true“ fest. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste und XMLdoc2-Entitätsvalidierung mit Allow-Liste.
- Definieren Sie eine Liste von durch Kommas getrennten FQDNs in der Eigenschaft `glide.xml.entity.whitelist`. Dies sind die einzigen URLs, die über die XML-Entitätsverarbeitung erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.stax.allow_entity_resolution
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen XML-Entitätserweiterungs-/Billion-Lach-Angriff zu schützen.
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann diese Schwachstelle verwenden, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.
Workaround	Wenn die Anpassung eine Entitätserweiterung erfordert, legen Sie diese Eigenschaft auf „true“ fest, und führen Sie die in XMLdoc2-Entitätsvalidierung mit Allow-Listedokumentierten Schritte aus.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Weitere Informationen zu OWASp-Ressourcen finden Sie unter OWASp .

XMLdoc2-Entitätsvalidierung mit Allow-Liste (Härtung der Instanzsicherheit)

Verwenden Sie eine Eigenschaft, um die Verarbeitung von externen Entitäten, die in der Aufnahmeliste aufgeführt sind, mit XMLDocument2 zu ermöglichen.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaft *glide.xml.entity.whitelist.enabled* auf „Wahr“ fest. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste.
- Definieren Sie eine Liste der durch Kommas getrennten FQDNs in der Eigenschaft *glide.xml.entity.whitelist*. Dies sind die einzigen URLs, die mithilfe der XML-Entitätsverarbeitung erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.stax.whitelist_enabled
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen Angriffe auf externe XML-Entitäten zu schützen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine externe Entität verwendet, die nicht in der Aufnahme aufgeführt ist, blockiert Now Platform möglicherweise die weitere Verarbeitung. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann die DTD beliebige HTTP-Anforderungen enthalten, die der Server ausführen kann. Wenn die Vertrauensstellung des Servers mit anderen Entitäten verwendet wird, kann dies zu weiteren Angriffen führen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Verarbeitung externer XML-Entitäten – Allow-Liste (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft `glide.xml.entity.whitelist`, um bei Bedarf den Zugriff auf eine Liste von durch Kommas getrennten FQDNs zu ermöglichen. Diese URLs sind die einzigen, die über die XML-Entitätsverarbeitung erreicht werden können.

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft `glide.xml.entity.whitelist.enabled` fest, die die Validierung einer externen Entität ermöglicht und nur die Verarbeitung der Aufnahmeliste zulässt, die Sie in der Eigenschaft `glide.xml.entity.whitelist` angeben. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Whitelisting.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.xml.entity.whitelist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So erstellen Sie eine Aufnahmeliste von URLs, auf die die XML-Entitätsverarbeitung zugreifen kann.
Empfohlener Wert	Benutzerdefinierte (z. B. https://google.com)
Funktionale Auswirkung	(Niedrig) Die Verarbeitung externer Entitäten kann blockiert werden, wenn sie nicht in der Aufnahmeliste erwähnt werden. Wenn die Aufnahmeliste aktiviert ist, ist das PUBLIC-Formular einer externen Entitätsdefinition erforderlich.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann die DTD beliebige HTTP-Anforderungen enthalten, die der Server ausführen kann. Dies

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	kann zu anderen Angriffen führen, die die Vertrauensstellung des Servers zu anderen Entitäten nutzen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sitzungsverwaltung (Härtung der Instanzsicherheit)

Die Sitzungsverwaltung hilft, den Datenverkehr, der zu einem bestimmten Benutzer gehört, richtig zu identifizieren. Treffen Sie Vorkehrungen, um sicherzustellen, dass die Vertrauensstellung nicht missbraucht wird.

Webanwendungen können Sitzungen erstellen, um anonyme Benutzer nach der ersten Benutzeranforderung nachzuverfolgen. Ein Beispiel wäre die Beibehaltung der Benutzerspracheinstellung, um Folgendes sicherzustellen:

- Identifizierung des Benutzers bei nachfolgenden Anforderungen.
- Anwendung von Sicherheitszugriffskontrollen.
- Autorisierung des Zugriffs auf die privaten Daten des Benutzers.
- Erhöhung der Benutzerfreundlichkeit der Anwendung.

Daher können aktuelle Webanwendungen Sitzungsfunktionen sowohl vor als auch nach der Authentifizierung bereitstellen.

Authentifizierung und Sitzungsverwaltung

Bei der Authentifizierung wird überprüft, ob eine Person, Entität oder Website die Person ist, für die sie sich ausgibt.

Bei der Authentifizierung wird versucht, die digitale Identität des Absenders einer Kommunikation zu überprüfen. Das Testen des Authentifizierungsschemas bedeutet, dass Sie verstehen, wie der Authentifizierungsprozess funktioniert, und diese Informationen verwenden, um den Authentifizierungsmechanismus zu umgehen. Ein häufiges Beispiel ist der Anmeldevorgang. Die Authentifizierung erfolgt nach der Übermittlung eines Benutzernamens, einer Benutzer-ID und einer oder mehrerer privater Informationen, die nur der Benutzer kennt.

Die Sitzungsverwaltung umfasst sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um sicherzustellen, dass in der Now Platformsichere Sitzungsverwaltungsmechanismen eingerichtet werden.

Absolute Zeitüberschreitung für Sitzung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.user_cookie.max_life_span_in_days`, um eine maximale Lebensdauer für Benutzercookies festzulegen, die erstellt werden, wenn sich Benutzer mit dem Kontrollkästchen „Benutzernamen **speichern** “ anmelden. Wenn das **Cookie** abläuft, müssen sich Benutzer, die das Kontrollkästchen „Benutzernamen speichern“ aktiviert haben, erneut bei der Instanz authentifizieren.

Dadurch bleibt das Benutzer-Cookie für die Dauer der angegebenen Tage gültig, beginnend mit der ersten Ausgabe des Cookies. Der Standardwert beträgt 30 Tage, die maximale Obergrenze liegt bei 365 Tagen.

Hinweis:
Informationen zum Erzwingen einer maximalen Sitzungszeit für aktive Benutzersitzungen finden Sie unter Configure a maximum active time for user sessions .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.user_cookie.max_life_span_in_days`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um Benutzer, die das Kontrollkästchen „Benutzernamen speichern“ aktiviert haben, nach bestimmten Tagen zur **erneuten** Authentifizierung zu zwingen.
Funktionale Auswirkung	(Mittel) Diese Eigenschaft erzwingt eine obligatorische erneute Anmeldung, indem jegliche Art von Cookie-Rotation nach einem bestimmten Zeitraum vermieden wird.
Sicherheitsrisiko	(Mittel) Die Benutzercookies, die für eine unbegrenzte Zeit aktiv sind, stellen ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Ändern Sie die Einstellungen für das Kontrollkästchen Benutzernamen speichern und Cookies

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Anti-CSRF-Token (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.security.use_csrf_token`, um sicherzustellen, dass ein sicheres Token zum Identifizieren und Validieren eingehender Anforderungen verwendet wird, die wiederum zur Verhinderung dieser Angriffe verwendet werden.

Cross-Site Request Forgery (CSRF) ist ein Angriff, der einen Endbenutzer dazu zwingt, unerwünschte Aktionen in einer Webanwendung auszuführen, in der er sich derzeit authentifiziert hat. CSRF-Angriffe zielen speziell auf Anforderungen zur Statusänderung ab, nicht auf den Diebstahl von Daten, da der Angreifer die Antwort auf die gefälschte Anforderung nicht sehen kann.

Die folgenden Eigenschaften können für hinzugefügte Steuerungen für das CSRF-Token aktiviert werden:

- `glide.security.csrf_previous.time_limit`
- `glide.security.csrf_previous.allow`
- `glide.security.csrf.strict.validation.mode`

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.use_csrf_token
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Schutz der Anwendung vor potenziellen CSRF-Angriffen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzbenutzer eine Schreibanforderung an die Instanz sendet. Jede Schreibanforderung enthält ein CSRF-Token (d. h. eine Validierungs-/CSRF-ID, die an die Benutzersitzung gebunden ist). Wenn die Benutzersitzung abläuft, läuft auch das sichere Token ab.
Sicherheitsrisiko	(Hoch) Cross Site Request Forgery stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff starten, indem er das Vertrauen eines Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung in der Instanz übermitteln.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Standardanmeldeinformationen ändern (Härtung der Instanzsicherheit)

Verwenden Sie die **Checkbox Passwortzurücksetzung** in Benutzer und Gruppen, um sicherzustellen, dass ein unberechtigter Benutzer die Standarddaten nicht ausnutzen kann.

Now Platform enthält einige Standarddaten, wenn die Instanz gestartet wird oder wenn Sie eine neue Instanz bereitstellen. Es kann die Demo-Benutzerkonten enthalten, z. B. „Standardadministrator“, „ITIL“ und „Mitarbeiter“. Durch das Festlegen der Eigenschaft ist es erforderlich, die Standard-Administrator-, ITIL- und Mitarbeiter-Anmeldeinformationen zu ändern, wenn Sie sich bei der Anwendung anmelden.

Schritte zum Konfigurieren von

1. Melden Sie sich mit dem Benutzernamen **admin** und dem Passwort **admin**an.
2. Navigieren zu **Systemsicherheit** > **Benutzer** > **Benutzer und Gruppen**
3. Suchen Sie unter Benutzer-ID **admin** und **Nameadministrator**nach dem Benutzer. Klicken Sie auf die **Administrator** -Anwender-ID, um die Einstellungen des Benutzers zu ändern.
4. Ändern Sie das Feld E- **Mail**, um eine gültige E-Mail-Adresse für diesen Benutzer anzugeben.
5. Aktivieren Sie das Kontrollkästchen **Passwort muss zurückgesetzt** werden.
6. Klicken Sie auf **Aktualisieren**.
7. Abmeldung
8. Melden Sie sich erneut an, um aufgefordert zu werden, ein neues Passwort festzulegen.
9. Wiederholen Sie die Schritte 3 bis 7 für ITIL- und Mitarbeiter-Accounts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cookies nur HTTP (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.cookies.http_only`, um das HTTPOnly-Attribut für vertrauliche Cookies zu aktivieren.

Verwenden Sie das Attribut HTTPOnly, um Angriffe wie websiteübergreifendes Skripting zu verhindern, da es keinen Zugriff auf das Cookie mit einem clientseitigen Skript wie JavaScript zulässt. Dadurch werden nicht die Risiken von websiteübergreifendem Skripting eliminiert, aber einige Ausnutzungsvektoren eliminiert.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.cookies.http_only
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um das Risiko eines clientseitigen Skripts zu verringern, das auf das geschützte Cookie zugreift.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt ein zusätzliches HTTPOnly-Flag in Sitzungscookies hinzu und schützt sie so vor Diebstahl. • Wenn Sie über benutzerdefinierte Funktionen verfügen, die JavaScript für den Zugriff auf das Cookie des Benutzers erfordern, wird diese Funktionalität beeinträchtigt. Unter normalen Umständen sollte dies nicht der Fall sein. • Now Platform behandelt die Sitzungsverwaltung, und es sollte keinen Grund geben, warum ein benutzerdefiniertes Skript auf die Cookies des Benutzers zugreift.
Sicherheitsrisiko	(Mittel) Sitzungscookies in der Anwendung authentifizieren einen Endbenutzer und stellen implizite Zugriffsberechtigungen für die Anwendung bereit. Das bedeutet, dass sie vor Diebstahl oder Export geschützt werden müssen. Kennzeichnungen vom Typ „Nur HTTP“ schützen die Sitzungscookies vor JavaScript-Injektionen oder websiteübergreifenden Skripting-Schwachstellen, die sie stehlen.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Strikte CSRF-Validierung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.security.csrf.strict.validation.mode`, um die strikte Validierung des CSRF-Tokens zu aktivieren. Wenn das CSRF-Token nicht übereinstimmt, wird die erneute Übermittlung der Anforderung verhindert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.csrf.strict.validation.mode
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingt die strikte Validierung des CSRF-Tokens und verhindert dessen Wiederverwendung.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzbenutzer eine Schreibanforderung an die Instanz sendet. Es wird überprüft, ob das aktuelle CSRF-Token zuvor verwendet wurde. Wenn Ja, wird die Übermittlung weiterer Schreibanforderungen verhindert.
Sicherheitsrisiko	(Mittel) Cross Site Request Forgery stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzbenutzer starten, indem er das Vertrauen des Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine falsch formatierte Anforderung an die Instanz senden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Passwortlose Authentifizierung deaktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.login.no_blank_password`, um zu verhindern, dass sich Benutzer mit leeren Passwörtern bei Now Platform anmelden oder indem Sie das Feld **Passwort** leer lassen.

Selbst wenn der Administrator absichtlich einen leeren Wert oder ein leeres Passwort in Benutzerdatensätzen zuweist, kann sich ein Benutzer nicht anmelden, ohne einen Wert im Feld **Passwort** anzugeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.login.no_blank_password
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine starke Authentifizierung sicherzustellen, da der Benutzername innerhalb einer Organisation manchmal leicht zu erraten ist.
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Vorgänge sollten keine leeren Passwörter verwenden, da dies als kritisches Sicherheitsrisiko angesehen wird. Wenn jedoch ein gültiger Fall für eine solche Verwendung vorliegt, besteht die Möglichkeit eines Ausfalls. Benutzer mit leeren Passwörtern können sich nicht bei der Instanz anmelden.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann sich bei der Instanz mit den Standardbenutzernamen oder einer bestimmten Person/Gruppe (normalerweise vorname.nachname) ohne Passwort anmelden. Dies wird als kritisches Sicherheitsrisiko angesehen, da ein öffentlicher Benutzer die Vertraulichkeit und Integrität der Instanzdaten verletzen könnte.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Multifaktor-Authentifizierung (MFA) aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.authenticate.multifactor*, um die Multifaktor-Authentifizierung (MFA) in der Instanz zu aktivieren. MFA ist eine Sicherheitsanforderung, bei der ein Benutzer mehr als einen Satz von Anmeldeinformationen eingeben muss, um sich bei einer Instanz zu authentifizieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.authenticate.multifactor
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verstärken Sie die Instanzsicherheit, indem Sie die Multifaktor-Authentifizierung für interaktive Benutzeranmeldungen einführen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft wird die Experience des Benutzers verbessert. Sie fungiert als zusätzliche Schutz- und Sicherheitsebene gegen gefährdete Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Systemeigenschaften der Multifaktor-Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Legen Sie Kriterien für die rollenbasierte Multifaktor-Authentifizierung fest

Verwenden Sie die Eigenschaft *glide.authenticate.multifactor*, um die rollenbasierte Multifaktor-Authentifizierung (MFA) für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den dem Benutzer zugewiesenen Rollen. Wenn einem Anwender in der Multifaktor-Rollenliste die Rollen „admin“, „security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

- Legen Sie diese Eigenschaft auf **„true** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf „ **false** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer zu deaktivieren, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.authenticate.multifactor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer, die bestimmten Rollen zugewiesen sind.
Typ	wahr/falsch
Empfohlener Wert	`true`
Sicherheitsabhängigkeiten	Aktivieren **Sie die rollenbasierte Multifaktor-Authentifizierung** in der **Tabelle „Multifaktor-Kriterien“**.
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft wird die Experience des Benutzers verbessert. Sie fungiert als zusätzliche Schutz- und Sicherheitsebene gegen gefährdete Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Richtlinienprüfungen für Passwortzurücksetzung aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft **glide.enable.password_policy**, um Passwortrichtlinienprüfungen zu aktivieren, wenn ein Benutzer sein Passwort über die Benutzeroberfläche ändert.

Informationen zum Definieren der Passwortrichtlinie, die nach Aktivierung dieser Eigenschaft verwendet werden soll, finden Sie unter Passwortrichtlinien für Ihre Instanz aktivieren.

Hinweis:
glide.enable.password_policy gilt nicht, wenn ein Administrator ein Passwort ändert oder einen Benutzer über ein Skript hinzufügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.enable.password_policy
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Zweck	Zum Anwenden der Passwortrichtlinie zum Zeitpunkt der Passwortänderung.
Empfohlener Wert	true (für Passwörter mit höherer Sicherheit)
Funktionale Auswirkung	(Mittel) Wenn die Eigenschaft auf „true“ festgelegt wird, werden Passwortrichtlinienprüfungen aktiviert, wenn ein Benutzer sein Passwort zurücksetzt.
Sicherheitsrisiko	(Mittel) Ohne eine Passwortrichtlinie kann ein Benutzer ein schwaches Passwort erstellen, was die Wahrscheinlichkeit erhöht, dass ein Angreifer Zugriff auf die Instanz erhält.

Schritte zum Konfigurieren von

Wenn Sie diese Einstellung auf der Seite „Härtungs-Compliance-Konfiguration“ im Instanz-Sicherheitszentrum konfigurieren:

1. Wählen Sie unter **Mittel**die Option **Sitzungsverwaltung**aus.
2. Wählen Sie in der Einstellung **Enable Password Reset Policy Check** (Richtlinienprüfung für Passwortzurücksetzung aktivieren) **Mittel** für Passwörter mit mittlerer Stärke oder **Stark** für robustere Passwörter mit höherer Stärke aus. Wenn Sie eine dieser Optionen auswählen, wird die Eigenschaft **glide.enable.password_policy** auf „true“ festgelegt und ein Workflow gestartet, der Ihre Passwortrichtlinie automatisch aktualisiert.

Darüber hinaus können Sie die Systemeigenschaft `glide.apply.password_policy.on_login` festlegen, um Passwortrichtlinienprüfungen zum Zeitpunkt der Anmeldung zu aktivieren.

Fehlgeschlagene Anmeldeversuche verwalten (Härtung der Instanzsicherheit)

Es sind zwei Skriptaktionen verfügbar, mit denen ein Site-Administrator verwalten kann, wie oft ein Benutzer ein falsches Passwort eingeben kann, bevor er von Now Platformausgesperrt wird. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldeversuche zu verwalten.

Weitere Informationen

Attribut	Beschreibung
Eigenschaft/Plugin-Name	N/V
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Zum Erzwingen einer strikten Richtlinie für fehlgeschlagene Anmeldeversuche, um ein Brute-Forcing von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur ermöglicht es dem Administrator der Instanz, jeden böswilligen Benutzerzugriff zu überwachen und zu melden. Keine Auswirkungen auf die Funktionalität, nur Änderung der Benutzer-Experience.
Sicherheitsrisiko	(Mittel) Wenden Sie eine definierte Protokollierungs- und Auditing-Strategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.
Referenzen	

Schritte zum Konfigurieren von

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen *`*SNC User`*.
3. Um die Verwaltung fehlgeschlagener Anmeldeversuche zu aktivieren, ändern Sie den Status Aktiv der Skriptaktionen *`SNC User Lockout Check with Auto Unlock`* oder *`SNC User Lockout Check`* von **false** in **true**.
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie die Skriptaktion *`SNC User Clear`* aktivieren.

Automatisches Ausfüllen des Passwortfelds (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.login.autocomplete`*, um Browsern die Verwendung der automatischen Vervollständigung für Passwortfelder in Anmeldeformularen zu ermöglichen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.login.autocomplete
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So deaktivieren Sie den Browser, um die automatische Vervollständigung für ein Passwortfeld zu versuchen.
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Diese Korrektur führt dazu, dass die Kennzeichnung für die automatische Vervollständigung des **Passwortfelds deaktiviert** wird, sodass der Cache des Passwortverlaufs nach Browser nicht im Feld angezeigt wird. Es sollte keine Auswirkungen auf die Funktionalität geben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Niedrig) Benutzerauthentifizierungsfelder sollten validiert werden und dürfen niemals die clientseitige Zwischenspeicherung zulassen.
Referenzen	https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Anmeldeinformationen von der Willkommensseite entfernen (Härtung der Instanzsicherheit)

Ändern Sie den Standardinhalt auf der Willkommensseite, um die Standardanmeldeinformationen zu entfernen.

Hinweis:
Zwei Datensätze zur Vorgehensweise bei der Anmeldung sind Teil der Demodaten für das CMS-Plugin. Wenn Sie die Demodaten für eine Instanz nicht installieren, sind diese Datensätze nicht vorhanden. In diesem Fall wird die Konfiguration gemäß den empfohlenen Sicherheitspraktiken als sicherheitskonform betrachtet. Weitere Informationen finden Sie unter Best Practices für Sicherheit.

Schritte zum Konfigurieren von

1. Navigieren zu **System-UI** > **Inhalt der Willkommensseite** > **.**
2. Suchen Sie die beiden Abschnitte mit einer Kurzbeschreibung der **Anmeldung**.
3. Ändern Sie den Status Aktiv für jeden von **true** in **false**.

Erinnerung entfernen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.forgetme`, um das Kontrollkästchen „Benutzernamen speichern“ von der **Anmeldeseite** zu entfernen, um zu verhindern, dass Anmeldeinformationen zwischengespeichert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.forgetme
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um sicherzustellen, dass keine Authentifizierungsinformationen zwischengespeichert werden.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Benutzer-Experience ändern, indem sie automatisch von der Instanz abgemeldet wird, wenn ihre Sitzung abläuft. Der Ablauf der Sitzung hängt ausschließlich von dem Wert ab, der in der Systemeigenschaft festgelegt ist, wie unter Benutzersitzungen verwalten beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Mittel) Wenn Sie bei der **Anmeldung** das Kontrollkästchen Benutzernamen speichern aktivieren, wird ein zusätzliches Cookie auf dem Computer des Benutzers gespeichert. • Ihr Zweck besteht darin, die Sitzung für die nachfolgenden Besuche des angemeldeten Benutzers automatisch wiederherzustellen. • Dies stellt ein Sicherheitsrisiko dar, da die Benutzersitzung so lange aktiv bleiben kann, bis sie sich absichtlich abmeldet. Die Wahrscheinlichkeit eines Angriffs in diesem Szenario steigt, wenn der Endbenutzer den Browser unbeaufsichtigt gelassen hat oder wenn er durch einen anderen Angriff gefährdet ist.
Referenzen	Entfernen Sie das Kontrollkästchen Benutzernamen speichern

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

HTTP-Sitzungsbezeichner rotieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.rotate_sessions`, um die Rotation der HTTP-Sitzungsbezeichner zu aktivieren, um Sicherheitsschwachstellen zu reduzieren.

Wenn sich die Sitzungs-ID eines nicht authentifizierten Benutzers nach der Authentifizierung nicht ändert, ist eine Webanwendung angreifbar für einen Sitzungsfixierungsangriff . Ein böswilliger Benutzer könnte eine nicht authentifizierte Sitzung starten und die zugehörige Sitzungs-ID an das Opfer weitergeben. Sobald sich das Opfer authentifiziert hat, gibt der böswillige Benutzer diese authentifizierte Sitzung frei.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.rotate_sessions
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Durch diese Korrektur wurde die SessionID geändert, wenn der Benutzer von einer nicht authentifizierten Seite zu authentifizierten Seiten navigiert. • Wenn Sie einen Proxy verwenden oder die SessionID hartcodieren, wenn sich ein Benutzer zum ersten Mal anmeldet, oder aus irgendeinem Grund, kann dies potenzielle Auswirkungen auf die Funktionalität haben. • Wenn Sie das SAML 2.0-Plugin für die Single Sign-on-Authentifizierung verwenden, kann dies die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigen. In einem solchen Fall können Sie diese Eigenschaft auf „false“ festlegen.
Sicherheitsrisiko	(Spät) SessionID wird verwendet, um den Instanzbenutzer zu verarbeiten und zu authentifizieren, indem der Sitzungsstatus im Browser beibehalten wird. Daher gilt SessionID als vertrauliche Daten und sollte standardmäßig sicher sein. Die Sitzungsrotation ist eine Sicherheitskontrolle, die die Änderung der Sitzungs-ID erzwingt, wenn der Benutzer von nicht authentifizierten Seiten zu authentifizierten Seiten navigiert.
Referenzen	Authentifizierung mit SAML

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Cookies für sichere Sitzung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.secure_cookies`, um ordnungsgemäß formatierte Cookies zu erfordern

Wenn Sie die Eigenschaft auf „true“ festlegen, lehnt Ihre Instanz eine Sitzung ab, wenn das zugeordnete Cookie nicht das erwartete Format aufweist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.secure_cookies
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft auf „true“ festgelegt ist, werden falsch formatierte Cookies abgelehnt. Wenn ein solches Cookie abgelehnt wird, muss sich der Benutzer erneut anmelden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sicherheitsverweisungsrichtlinie (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `com.glide.security.referrerpolicy`, um zu steuern, welche Referrer-Daten in HTTP-Antwortheadern gesendet werden sollen, wenn Seiten von Now Platform Datenanforderungen senden. Der Wert Referrer-Policy in einem HTTP-Header steuert, welche Referrer-Informationen in Datenanforderungen enthalten sein sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

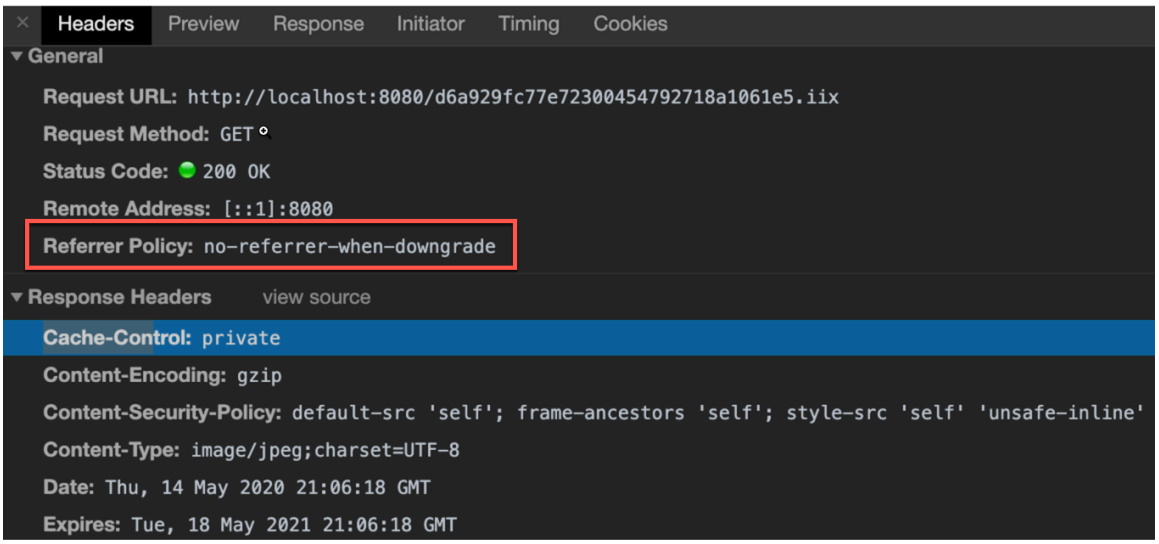
Werte der Sicherheitsreferenzrichtlinie

Legen Sie die Eigenschaft *com.glide.security.referrerpolicy* auf einen der folgenden Werte fest.

Wert	Beschreibung
Standard	Die InstanzNow Platform verwaltet die Ebene der Informationen, die in Referrer-Headern gesendet werden, die für die spezifische Seitenanforderung von Now Platform geeignet sind.
gleicher Ursprung	Now Platform -Seiten senden eine vollständige Referrer-URL innerhalb der Instanz und derselben Domäne und keinen Referrer-Header nach außerhalb des Ursprungs. Diese Einstellung gewährleistet ein gutes Maß an Instanzsicherheit.
origin	Now Platform -Seiten senden die Basis-URL im Referrer-Header innerhalb der Instanz und derselben Domäne sowie nach außen. Diese Einstellung gewährleistet ein gutes Maß an Instanzsicherheit.
Ursprung-wenn-übergreifend	Now Platform -Seiten senden die gesamte URL im Referrer-Header innerhalb der Instanz und derselben Domäne und senden nur die Basis-URL nach außen. Diese Einstellung gewährleistet ein gutes Maß an Instanzsicherheit.
no-referrer-when-downgrade	Now Platform -Seiten senden den Ursprung, den Pfad und die Abfragezeichenfolge in der URL, solange kein Downgrade in einem Sicherheitsprotokoll erfolgt. **Hinweis:** Diese Einstellung gewährleistet kein gutes Maß an Instanzsicherheit in Now Platform und sollte nicht verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Referrer-Richtlinie und Werteübersicht



Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.security.referrerpolicy
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Steuert, wie viele eingehende Daten über den Header „referrer“ gesendet werden, wenn eine Now Platform -Seite eine Datenanforderung sendet.
Empfohlener Wert	Standard
Funktionale Auswirkung	(Niedrig) Bei Festlegung auf „Standard“ verwaltet die Instanz Now Platform die Ebene der in Referrer-Headern gesendeten Informationen.
Sicherheitsrisiko	(Hoch) Das Festlegen dieses Eigenschaftswerts auf „no-referrer-when-downgrade“ stellt kein gutes Sicherheitsniveau für Ihre Instanz sicher.
Referenz	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy https://developer.mozilla.org/en-US/docs/Glossary/origin

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitüberschreitung der Sitzungsaktivität (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.session_timeout`, um den Zeitüberschreitungswert der Aktivität in Minuten anzugeben.

Das Festlegen dieser Eigenschaft hat mehrere funktionale Auswirkungen:

- Je länger die angegebene Sitzungszeitüberschreitung ist, desto mehr Arbeitsspeicher wird während einer Verarbeitungssitzung verwendet. Das Basissystem verwendet eine Apache Tomcat-Standardzeitüberschreitungsdauer von 30 Minuten.
- Mit Now Platform werden Benutzer weiterhin mit „Benutzernamen speichern“ abgemeldet. Nach 30 Minuten Inaktivität in der Anwendung meldet die Plattform den Benutzer automatisch ab, es sei denn, das Kontrollkästchen Benutzernamen speichern auf der **Anmeldeseite** ist aktiviert. Der Unterschied zu besteht darin, dass sie sich nicht erneut anmelden, um fortzufahren.
- Wenn es auf den Homepages der Benutzer Anzeigen oder Inhalte gibt, die automatisch aktualisiert werden, wird diese Zeitüberschreitung möglicherweise nie erreicht.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.session_timeout
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen einer Sitzungszeitüberschreitung.
Empfohlener Wert	Benutzerdefinierte Zeitüberschreitung in Minuten. Der empfohlene Wert beträgt 30 Minuten. Dieser Wert kann jedoch je nach Funktionalität und Sicherheitsanforderung variieren. Legen Sie diesen Wert nicht auf mehr als einen Tag fest.
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt den rechtzeitigen Ablauf des Benutzerkontos. Keine Auswirkungen auf die Funktionalität, die Benutzer-Experience wird jedoch geändert.
Sicherheitsrisiko	(Mittel) Benutzersitzungen, die auf unbestimmte Zeit aktiv sind, stellen ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Benutzersitzungen verwalten

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Zeitüberschreitung für Sitzungsfenster (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.ui.user_cookie.life_span_in_days`, um den Ablaufzeitraum für das Erinnerungscookie festzulegen. Der Standardwert beträgt 15 Tage, die maximale Obergrenze liegt bei 30 Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.user_cookie.life_span_in_days
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	So aktivieren Sie den standardmäßigen Ablauf des Cookies „Benutzernamen speichern“.
Empfohlener Wert	Benutzerdefinierter ganzzahliger Wert (Anzahl der Tage) [Beispiel: 15]
Funktionale Auswirkung	(Mittel) Diese Eigenschaft wird vom Endbenutzer aktiviert, wenn der Endbenutzer das Kontrollkästchen Benutzernamen speichern auf der **Anmeldeseite** aktiviert und sich bei Now Platformanmeldet.
Sicherheitsrisiko	(Mittel) Die Benutzercookies, die für eine unbegrenzte Zeit aktiv sind, stellen ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Ändern Sie die Einstellungen für das Kontrollkästchen Benutzernamen speichern und Cookies

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Konfigurieren Sie Passwörter für automatisch erstellte Benutzerkonten

Verwenden Sie die Systemeigenschaften `glide.email.inbound.use_default_password` und `glide.user.default_password`, um zu definieren, wie Passwörter für neue Benutzer erstellt werden, die aus eingehenden E-Mails erstellt werden.

Die in diesem Dokument beschriebenen Systemeigenschaften definieren, wie die Instanz Passwörter für Benutzerkonten behandelt, die aus eingehenden E-Mails generiert werden. Ihre Instanz muss so konfiguriert sein, dass sie E-Mails empfangen und die automatische Benutzererstellung aktivieren kann. Im folgenden Abschnitt finden Sie Details zu diesen Konfigurationen.

Nachdem Ihre Instanz so konfiguriert wurde, dass Konten automatisch erstellt werden, können Sie mithilfe der Eigenschaften bestimmen, ob ein Standardpasswort verwendet werden soll, und dieses Passwort bei Bedarf definieren.

Voraussetzungen

Um diese Eigenschaften zu verwenden, muss Ihre Instanz so konfiguriert sein, dass neue Benutzerkonten automatisch erstellt werden.

- Sie müssen Ihren eigenen POP3-Server konfigurieren, um E-Mails für Ihre Instanz zu speichern und zu empfangen. Dann müssen Sie die Systemeigenschaft `glide.email.read.active` auf „true“ festlegen. Weitere Informationen zum Konfigurieren eines POP3-Servers in Ihrer Instanz finden Sie unter Verwenden Ihres eigenen POP3-Servers aktivieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie die Eigenschaft `glide.pop3readerjob.create_caller` auf „Wahr“ fest. Mit dieser Eigenschaftsänderung kann Ihre Instanz automatisch Benutzer aus eingehenden E-Mails erstellen. Weitere Informationen finden Sie unter Automatische Benutzererstellung aktivieren .

Hinweis:
Überspringen Sie die Eigenschaft `glide.user.default_password`, wenn die Eigenschaft `glide.pop3readerjob.create_caller` auf **false**festgelegt ist.

Wie Ihre Instanz Passwörter definiert

In Quebec und früheren Releases von ServiceNowerstellt Ihre Instanz neue Benutzerkonten aus eingehenden E-Mails mit einem komplexen Passwort, das in der Systemeigenschaft `glide.user.default_password` definiert ist. Benutzer verwenden dieses Passwort bei der ersten Anmeldung. Anschließend werden sie von der Instanz zur Eingabe eines neuen Passworts aufgefordert. Wenn Sie Ihre Instanz auf Rome oder spätere Releases aktualisiert haben, bleibt dieser Prozess unverändert. Als Administrator können Sie Ihre Instanz aktualisieren, um die unten beschriebene neue Methode zu verwenden.

In neuen Instanzen ab Release Rome haben Benutzerkonten, die aus eingehenden E-Mails erstellt wurden, kein Passwort. Wenn ein Benutzer zum ersten Mal mit seinem neuen Account auf die Instanz zugreift, muss er seinen Benutzernamen eingeben und auf **Passwort vergessen?** klicken. Schaltfläche, um ein anfängliches Passwort zu erstellen.

In Rome und späteren Releases können Sie auswählen, welchem Prozess Ihre Instanz folgt, indem Sie einen Wert in der Systemeigenschaft `glide.email.inbound.use_default_password` festlegen. Um das oben beschriebene Standardverhalten zu ändern, erstellen Sie diese Systemeigenschaft anhand der folgenden Informationen:

Feld „Systemeigenschaf	Wert
Name	glide.email.inbound.use_default_password
Typ	Wahr|Falsch
Wert	Wählen Sie einen Wert basierend auf Ihrem gewünschten Verhalten aus: **Wahr** Für neue Konten wird ein Standardpasswort verwendet, das in der Systemeigenschaft `glide.user.default_password` definiert ist. **false** Neue Accounts haben kein Standardpasswort. Benutzer müssen ein Passwort definieren, wie weiter oben in diesem Abschnitt beschrieben.

Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaften hinzufügen .

Definieren Sie ein Standardpasswort

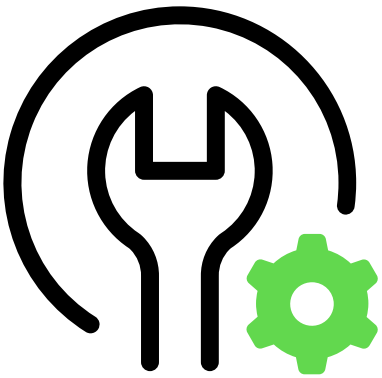
Wenn Ihre Instanz für die Verwendung eines Standardpassworts konfiguriert ist, müssen Sie dieses Passwort mit der Systemeigenschaft `glide.user.default_password` definieren. Erstellen Sie diese Eigenschaft anhand der folgenden Informationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld „Systemeigenschaf	Wert
Name	glide.user.default_password
Typ	Kennwort 2
Wert	Geben Sie ein eindeutiges Passwort ein, das als Standard verwendet werden soll. Verwenden Sie eine starke Passwortkomplexität, um die Sicherheit Ihrer Instanz zu gewährleisten.

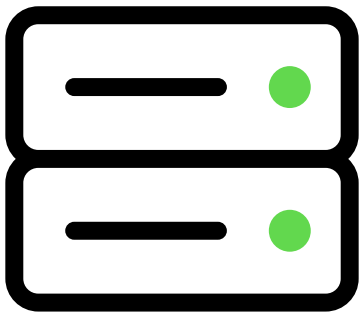
Andere Einstellungen und Sicherheitsressourcen

Dieser Abschnitt enthält Sicherheitseigenschaften, die Sie außerhalb des Instanz-Sicherheitszentrums festlegen, sowie andere sicherheitsbezogene Ressourcen.



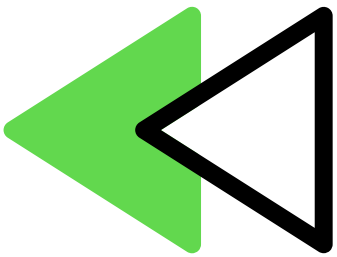
Eigenschaften des Sicherheitssystems

Sicherheitseinstellungen bieten mehrere Eigenschaften, um die Sicherheitsstufe in Ihrer Instanz zu steuern.



Leitfaden zur MID Server-Bereitstellung

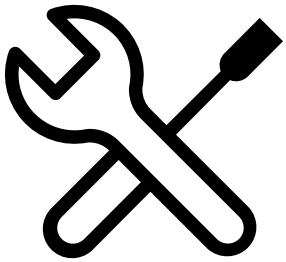
Der MID-Server (ServiceNow Management, Integration, and Discovery) ist eine schlanke Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf Standardhardware ausgeführt wird, einschließlich virtueller Computer.



Umkehrbares Verhalten

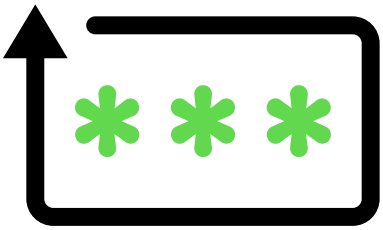
Es gibt Systemeigenschaften, die entweder als „safe_overrides“ oder „no_db_override“ kategorisiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



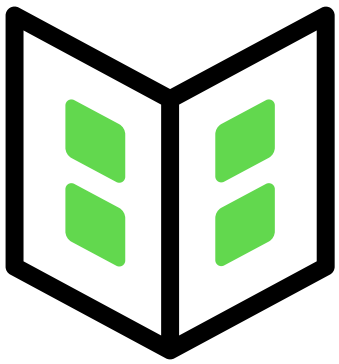
Veraltete Sicherheitseigenschaften

Diese Sicherheitseigenschaften waren in früheren Releases veraltet.



Verwenden der Javascript-Inhaltszugriffssteuerung

Sie können die JavaScript-Inhaltszugriffssteuerung verwenden, um die Liste der blockierten JavaScript-URLs von Drittanbietern in Ihrer Instanz zu ändern.



Andere Sicherheitshärtungsressourcen

Zusätzliche Informationsquellen zur Härtung von Sicherheitskontrollen im Zusammenhang mit der Now Platform.

Protokollierung, Auditing und Fehler (Härtung der Instanzsicherheit)

Wenden Sie eine Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Weitere Informationen darüber, was in der Instanz protokolliert werden kann, finden Sie unter Systemprotokolle. Stellen Sie sicher, dass es einen Zeitplan für die Überwachung von Systemereignissen wie Anmeldungen und fehlgeschlagenen Anmeldungen gibt, indem Sie verwenden **Systemprotokolle** > **Ereignisse**.

SQL-Fehlermeldungen deaktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft `glide.db.loguser`, um die Darstellung von SQL-Fehlermeldungen in einem Browser zu deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.db.loguser
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	So deaktivieren Sie die Anzeige von SQL-Fehlermeldungen im Browser.
Typ	Wahr|Falsch
Empfohlener Wert	false

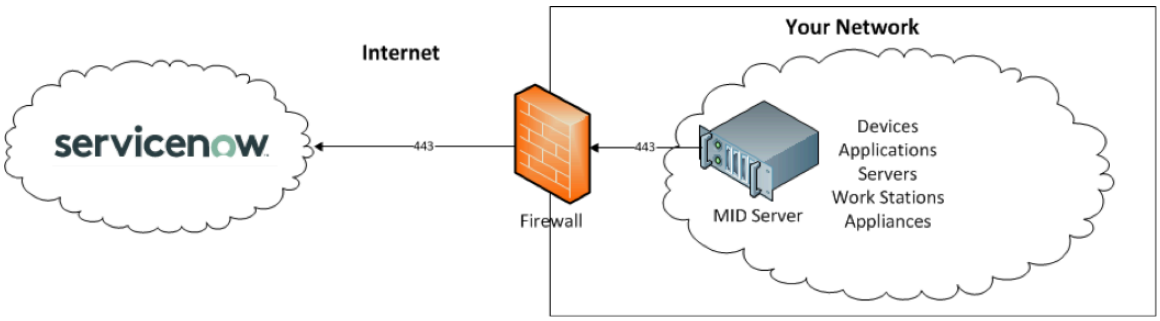
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Dies hat keine Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Mittel) Keine vertraulichen SQL-Informationen, die einem Angreifer helfen könnten, sollten als Teil der Fehlermeldung auf einer Webseite angezeigt werden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Leitfaden zur sicheren MID Server-Bereitstellung (Härtung der Instanzsicherheit)

Der MID-Server ServiceNow Management, Integration, and Discovery ist eine einfache Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf Standardhardware ausgeführt wird, einschließlich virtueller Computer.



Es authentifiziert sich sicher bei Ihrer Instanz in der ServiceNow Cloud mit seinen eigenen Anmeldeinformationen und erleichtert die Datenübertragung mit Ihren Anwendungen, Datenquellen und Services. Mehrere MID Server können in verschiedenen Netzwerksegmenten bereitgestellt werden, um zusätzliche Skalierbarkeit zu bieten.

Berücksichtigen Sie die folgenden Faktoren in Bezug auf die Sicherheit Ihres MID Servers:

Physische Sicherheit

Sichern Sie die physische Hardware, die den MID Server oder den Hypervisor für virtualisierte MID Server hostet.

- Bewahren Sie die Hardware an einem sicheren Ort auf, der die Hardware vor nicht autorisiertem Zugriff schützt.
- Schützen Sie den Zugang zu diesem Standort mit einem elektronischen Kartenleser und Videoüberwachung.
- Platzieren Sie die physische Hardware in einem abgeschlossenen Gehäuse oder einem Rack mit physischer Schlüsselzugriffskontrolle.

Sicherheit der virtuellen Infrastruktur

Verwenden Sie die Virtualisierung von vmit der Flexibilität, mehrere MID Server in virtualisierten Betriebssystemen und Netzwerken in gemeinsam genutzter physischer Hardware zu installieren.

Der Zugriff auf den Hypervisor und die Verwaltungskonsolen der virtuellen Infrastruktur muss geschützt werden, um ein nicht autorisiertes Klonen des virtualisierten MID Servers zu verhindern:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Beschränken Sie den Zugriff auf den Hypervisor und die Verwaltungskonsolen der virtuellen Infrastruktur durch wenige vertrauenswürdige Administratoren.
- Lassen Sie nur Verbindungen zum internen vertrauenswürdigen Netzwerk für die Managementkonsole wie ESX Server und VirtualCenter zu.
- Verwenden Sie VLANs, um Netzwerkangriffe zu verhindern.
- Befolgen Sie die Sicherheitsrichtlinien, die in den Leitfäden zur Virtualisierungshärtung der Anbieter veröffentlicht wurden.

Betriebssystemsicherheit

Erfahren Sie, wie der MID Server seinen Now Platform -Benutzernamen und sein Passwort in seiner Konfigurationsdatei mit dem Namen config.xmlfür die sichere Authentifizierung bei der Instanz speichert.

Der MID Server muss in einem sicheren und gesicherten Betriebssystem bereitgestellt werden, um Schutz vor nicht autorisiertem Zugriff auf die Anmeldeinformationen zu bieten:

- Beschränken Sie den Zugriff auf das Betriebssystem auf wenige, vertrauenswürdige Administratoren.
- Überwachen Sie die Betriebssystemprotokolle, um nicht autorisierten Zugriff zu erkennen, insbesondere Versuche, auf die Datei config.xml zuzugreifen, da diese Datei wichtige MID Server-Konfigurationsinformationen enthält.
- Installieren Sie regelmäßig Sicherheitspatches für das Betriebssystem mit der neuesten Antivirensoftware, und aktualisieren Sie die Antivirus-Definitionen regelmäßig.
- Der MID Server benötigt ein aktuelles Java-Framework, um ausgeführt werden zu können. Halten Sie Java regelmäßig auf dem neuesten Stand.
- Entfernen oder deaktivieren Sie nicht benötigte Services und Anwendungen.
- Installieren Sie eine BS-Firewall, um den Zugriff auf nicht autorisierte Ports zu beschränken.
- Befolgen Sie die Sicherheitsrichtlinien, die in den Härtungsleitfäden für Betriebssysteme der Anbieter veröffentlicht wurden.

Netzwerksicherheit

Der MID Server kommuniziert über Port 443 über SSL mit der Instanz und erfordert keine eingehenden Verbindungen.

Gehen Sie wie folgt vor, um Ihren MID-Server in einem Netzwerk ordnungsgemäß zu sichern:

- Installieren Sie den MID Server auf einem gesicherten Server hinter einer Unternehmensfirewall, um sich vor nicht autorisiertem Zugriff aus dem Internet zu schützen.
- Konfigurieren Sie die Firewall auf dem MID Server so, dass keine anderen eingehenden Verbindungen akzeptiert werden als die, die für die Unternehmensverwaltung des Betriebssystems und der Hardware erforderlich sind.
- Das System, das den MID Server hostet, muss auf die Download-Site ServiceNow unter **install.servicenow.com**zugreifen können.

> **Hinweis:**
> Diese URL führt zur Download-Site ServiceNow, auf die über dieses Thema nicht zugegriffen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der MID Server-Hostcomputer muss auf diese Site zugreifen können, um das Installationspaket herunterzuladen. Er kontaktiert **install.servicenow.com** alle 60 Minuten, um zu sehen, ob eine neuere Version verfügbar ist, und führt in diesem Fall ein automatisches Upgrade durch. Ein MID Server-Upgrade findet auch statt, wenn Sie eine Instanz aktualisieren.

Firewall

Konfigurieren Sie Ihre Firewall so, dass ausgehender Netzwerkverkehr vom MID Server zu Ihrer Instanz und dem Auto-Upgrade-Server zugelassen wird.

Verwenden Sie zum Konfigurieren Ihrer Firewall die folgenden Beispielsyntaxen:

- `<source IP> AN<instance_name> .service-now.com AN PORT 443`
- `<source IP> AN install.service-now.com AN PORT 443`

Administration und Management

In diesem Abschnitt werden die Sicherheitspraktiken und -richtlinien für die Verwaltung des MID Servers in Ihrer Umgebung beschrieben.

Erstellen Sie ein Konto mit einer mid_server-Rolle

Erstellen Sie ein Benutzerkonto in der Instanz, die eine mid_server-Rolle enthält.

Befolgen Sie beim Erstellen eines Benutzeraccounts die folgenden Richtlinien:

- Verwenden Sie in der Instanz für den MID Server kein Administratorkonto.
- Verwenden Sie für das MID Server-Konto eine ausreichende Länge und Komplexität des Passworts.
- Das Passwort muss aus mindestens 12 Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.
- Verwenden Sie verschiedene MID Server-Konten mit eindeutigen Passwörtern für verschiedene MID Server in einer Instanz.
- Verwenden Sie die strikte SOAP-Sicherheitsfunktion, um alle Tabellen mit Zugriffssteuerungslisten (ACL) zu schützen, indem Sie *`Enforce strict security on incoming SOAP requests`* in aktivieren **Systemeigenschaften** > **Webservices**.
- Ändern Sie die MID Server-Passwörter in einer Häufigkeit, die der Passwortrichtlinie Ihrer Organisation entspricht.

Hinweis:
Weitere Informationen finden Sie unter MID Server-Benutzer erstellen und Rolle gewähren .

Einrichten eines MID-Servers auf einem Windows-Host

Wenn Sie den MID Server auf einem Windows-Host installieren, wird ein Windows-Dienst erstellt. Standardmäßig wird dieser Service als lokales Windows-Systemkonto ausgeführt. Ändern Sie nach Abschluss der Installation den neu erstellten Windows-Dienst in ein Konto mit der geringsten Anzahl von Berechtigungen, die zum Ausführen des MID Servers auf dem Windows-Host erforderlich sind.

1. Navigieren zu **Computerverwaltung** > **Services und Anwendungen** > **Services**.
2. Klicken Sie mit der rechten Maustaste auf **ServiceNow MID Server**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Popup-Fenster **auf die Registerkarte Anmelden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf das Optionsfeld neben **Dieser Account**.
5. Geben Sie den entsprechenden Benutzernamen und das Passwort des Kontos ein, unter dem der Service ausgeführt werden soll.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster Services mit der rechten Maustaste auf **ServiceNow MID Server**, und klicken Sie dann auf Neu **starten**.
8. Vergewissern Sie sich, dass der MID Server erfolgreich neu gestartet und eine Verbindung zur Instanz hergestellt werden konnte.

Anmeldeinformationen für Windows Discovery und Orchestration

Richten Sie auf den Zielsystemen mit der geringsten Anzahl erforderlicher Berechtigungen ein lokales Windows- oder Active Directory-Konto ein. Es ist möglicherweise nicht erforderlich, Anmeldeinformationen des Domänenadministrators zu verwenden.

Die folgenden Seiten der Produktdokumentation enthalten Anleitungen dazu, welcher Kontotyp verwendet werden soll und welche Berechtigungen erforderlich sind.

- Windows-Anmeldeinformationen
- Windows-Probes und -Berechtigungen
- Microsoft Just Enough Administration (JEA) für Discovery

Anmeldeinformationen für Linux Discovery und Orchestration

Verwenden Sie bei der Erkennung und Orchestrierung ein Nicht-Root-Konto mit eingeschränkten sudo-Berechtigungen auf Linux-Zielsystemen.

Verwenden Sie die folgenden Richtlinien:

- Verwenden Sie für das Linux-Konto eine ausreichende Länge und Komplexität des Passworts. Das Passwort muss aus mindestens 12 Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.
- Bei der Konfiguration von sudo-Berechtigungen können sich die lokalen Pfade zu ausführbaren Binärdateien je nach ausgeführter Linux-Distribution unterscheiden. Weitere Informationen finden Sie unter Berechtigte MID Server-Befehle .

Verschlüsseln Sie die Anmeldeinformationen für den MID-Server

Standardmäßig werden die Anmeldeinformationen für den MID Server in der Datei config.xml verschlüsselt.

Stellen Sie beim Bearbeiten der Datei config.xml und beim Angeben des Passworts sicher, dass das Attribut `encrypt="true"` vorhanden ist, indem Sie die folgende Syntax verwenden:

```
<parameter name="MID.instance.username" value="MIDsrvadmin" />
```

```
<parameter name="MID.instance.password" encrypt="true" value="$ECUREpassw0rd"/>
```

Hinweis:
Durch die Verschlüsselung von MID Server-Anmeldeinformationen wird kein unsicherer Serverhost durch schlechte physische Sicherheit und Netzwerksicherheit ersetzt. Das in der Datei config.xml gespeicherte Passwort wird beim ersten Start des MID Servers oder, falls es sich um einen vorhandenen MID Server handelt, beim Neustart verschlüsselt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die Mindestgröße der DH-Gruppe auf 2048 Bit fest

Das National Standard Institute of Technology (NIST) hat die Verwendung des Diffie-Hellman (DH) 1024-Bit-Schlüssels nach dem Jahr 2013 verboten. Legen Sie stattdessen die Mindestgröße der DH-Gruppe auf 2048 Bit fest.

1. Navigieren Sie in der -Instanz zu **MID-Server** > **Server**.
2. Klicken Sie auf den Namen des MID Servers, für den Sie diese Funktionalität deaktivieren möchten.
3. Klicken Sie in der MID Server-Konfiguration auf die Schaltfläche **Neu** neben Konfigurationsparameter.
4. Konfigurieren Sie unter MID Server-Konfigurationsparameter die folgenden Parametereinstellungen:
   - **Parametername** mid.ssh.dh_group_length_min
   - **Wert** 2048

Deaktivieren Sie ausgehende SSL

Sie können SSLv2 und SSLv3 im Now Platformdeaktivieren. Durch das Festlegen dieser Eigenschaft wird der MID Server gezwungen, TLS zu verwenden und die erhöhte Sicherheit bei ausgehenden Verbindungen wie REST- und SOAP-Anforderungen zu nutzen.

1. Navigieren Sie in der -Instanz zu **MID-Server** > **Eigenschaften**.
2. Fügen Sie einen Konfigurationsparameter hinzu, und legen Sie seinen Wert wie folgt fest:
   - **Nennen** Sie glide.outbound.sslv3.disabled
   - **Wert „** true“.

Deaktivieren Sie schwächere Algorithmen

Sie können die schwächeren Algorithmen deaktivieren, sodass Anforderungen an einen nicht TLS 1.2-konformen HTTP-Server dort fehlschlagen, wo sie früher funktionierten.

Bearbeiten Sie die Datei jre/lib/security/java.security im Agent-Ordner mit der folgenden Syntax:

jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, [other schwache Algorithmen…]

Hinweis:
Beachten Sie, dass diese Datei beim Upgrade überschrieben wird. Daher sollten Sie über einen Prozess verfügen, um diese Datei nach jedem Upgrade erneut zu aktualisieren.

PowerShell-Benutzer sollten ihren Windows -Administrator konsultieren, um niedrigere Versionen von TLS zu deaktivieren. Um Details dazu zu erhalten, welche Versionen von TLS in PowerShell verwendet werden, verwenden Sie den Befehl [enum]::GetNames([Net.SecurityProtocolType]).

Umkehrbares Verhalten

Es gibt Systemeigenschaften, die entweder als „safe_overrides“ oder „no_db_override“ kategorisiert sind.

Sichere Überschreibung

Die Werte für diese Eigenschaften können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Administratoren können die Eigenschaft „Sichere Überschreibung“ nicht umbenennen oder löschen.

Attribut	Kategorie
Standardmäßig verweigern	Zugriffssteuerung
Aktivieren der AJAXGlideRecord-ACL-Überprüfung	Zugriffssteuerung
Datenschutz für vom Client aufrufbare Skripteinbindungen	Zugriffssteuerung
Vom Client generierte Skripts in der Sandbox	Eingabevalidierung
Überschreibung des Sammlungsmodus (veraltet)	Sicherheitsaufnahmeliste

Keine DB-Überschreibung

Die vorhandenen Werte für diese Eigenschaften können nicht geändert oder überschrieben werden.

Attribut	Kategorie
Aktivieren Sie Einschränkungen beim Dateidownload	Anlagen

Veraltete Sicherheitseigenschaften

Diese Sicherheitseigenschaften waren in früheren Releases veraltet.

Überschreibung des Sammlungsmodus (veraltet)

Die Eigenschaft `glide.whitelist.manager.collection_mode.override` wurde entwickelt, um die Abwärtskompatibilität für stark angepasste Instanzen zu gewährleisten. Es wurden Paketaufrufe verwendet, die in einer Version vor Calgary erstellt wurden, und sind seitdem veraltet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.whitelist.manager.collection_mode.override
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Durch Deaktivieren der Eigenschaft „Sammlungsmodus“ wird die Sicherheitslücke geschlossen, die beim Importieren von Java-Paketaufrufen in eine Instanz vorhanden ist.
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Es sollte keine Auswirkungen geben, solange die Ergebnisse aus Abschnitt 10.6 überprüft und genehmigt werden. Um sicherzustellen, dass die Instanz ordnungsgemäß funktioniert, testen Sie die Änderungen in einer Nicht-Produktionsumgebung, bevor Sie sie in der Produktionsumgebung bereitstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Clientseitige API-Aufrufe, die zum Datenabruf oder Objektzugriff auf dem Server führen, gelten aus Sicherheitsgründen als gefährlich. Validieren Sie sie auf Autorisierung und Einschränkung für den Zugriff auf vertrauliche Objekte.
Referenzen	https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483

SMTP-Authentifizierung (veraltet)

Die Eigenschaft *glide.smtp.auth* gibt an, ob für einen SMTP-Server Benutzernamen- und Passwortauthentifizierungseinträge erforderlich sein sollen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.smtp.auth
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Erzwingt die SMTP-Authentifizierung
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Fehlerkorrektur erzwingt die Authentifizierung beim externen E-Mail-Server, bevor der Inhalt in Form einer E-Mail übermittelt wird. Wenn die Automatisierung für die Bereitstellung von E-Mail-Inhalten eingerichtet ist, kann dies Auswirkungen haben, bis Sie die Eigenschaft festlegen und einen relevanten Benutzernamen/ein relevantes Passwort für den E-Mail-Serverzugriff angeben.
Sicherheitsrisiko	(Niedrig) Aktivieren Sie die SMTP-Authentifizierung, bevor der Inhalt an den externen E-Mail-Server gesendet wird. Die Authentifizierung sollte immer erfolgen, bevor Transaktionen an/von der Instanz stattfinden.
Referenzen	E-Mail-Eigenschaften

Verwenden der JavaScript-Inhaltszugriffssteuerung

Wenn Sie ein Upgrade-Kunde sind, können Sie die JavaScript-Inhaltszugriffssteuerung verwenden, um die Liste der blockierten JavaScript-URLs von Drittanbietern in Ihrer Instanz zu ändern.

Vorbereitungen

Wenn Sie ein Upgrade-Kunde sind, haben Sie Lese- und Schreibzugriff auf die Tabelle.

Wenn Sie ein neuer Kunde sind, werden alle Datensätze ausgeblendet. Wenden Sie sich an den Support von ServiceNow®, um Unterstützung zu erhalten.

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Suchen Sie im Anwendungsnavigator nach `sys_js_content_provider_rule.list`.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Regel für JavaScript-Inhaltsanbieter

Feld	Beschreibung
Aktiv	Option, bei der die Regel aktiv wird, wenn sie ausgewählt wird. Wenn diese Option deaktiviert ist und keine anderen Regeln übereinstimmen, wird die **Pfad** -URL zugelassen.
Pfad	Absolute URL zu einer JavaScript-Datei. **Hinweis:** Jeder Pfad hat vier Variationen. Zum Beispiel blockiert der Pfad `/scripts/lib/jquery/jquery-1.8.2.min.js` die folgenden URLs: ○ /scripts/lib/jquery/jquery-1.8.2.min.js ○ /scripts/lib/jquery/jquery-1.8.2.min.jsx ○ /lib/jquery/jquery-1.8.2.min.js ○ /lib/jquery/jquery-1.8.2.min.jsx
Aktion	Option zu ○ **Verweigern**: Der Server gibt die Antwort **404 Nicht gefunden** für die **Pfad** -URL oder eine ihrer Variationen zurück. ○ **Zulassen**: Der Server gibt den Inhalt der Datei für die **Pfad** -URL oder eine ihrer Variationen zurück. ○ **Umleiten**: Der Server gibt den Inhalt einer alternativen Datei zurück, wie im Feld Umleitungspfad angegeben.
Anwendung	Option, die den Umfang der Regel angibt. **Global** ist die Standardeinstellung. **Hinweis:** Diese Funktionalität ist nicht bereichs-/anwendungs- oder domänenabhängig.
Umleitungspfad	Feld, das den Pfad für die Umleitung angibt. Wenn **Aktion** auf **Umleiten**festgelegt ist, wird einer Anforderung für die **Pfad** -URL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	stattdessen der Inhalt von dieser URL zugestellt.

4. Klicken Sie auf **Absenden**.

Andere Sicherheitshärtungsressourcen

Im Folgenden finden Sie zusätzliche Informationsquellen zur Härtung von Sicherheitskontrollen im Zusammenhang mit Now Platform.

Ressource	Beschreibung
Sicherheitstestportal	Sicherheitsservices-Portfolio auf HI
KB0538598	Penetrationstests für Kundenanwendungen | Richtlinie und Verfahren
KB0546756	Deaktivieren des Zugriffs auf das öffentliche Content Management System (CMS).
KB0550071	ServiceNow, Inc. Überprüfung der Instanzzugriffskontrolle
KB0550613	IP-Adressbeschränkungen erkennen und aktivieren
KB0550828	Audit und Überprüfung von GlideAjax-Transaktionen
KB0550837	Skript-Sandboxing-Korrektur
KB0551031	Sicherheitskorrektur für die Passwortzurücksetzungs-UI
KB0552835	Fehlerkorrektur für Demo-Benutzerkonten
KB0529232	ServiceNow, Inc. Monitoring – Übersicht und Einblick
KB0564232	Verwenden der Mobile-App ServiceNow, Inc. mit externer Authentifizierung
Sicherheit und Risiko	ServiceNow, Inc. Community

Härtungseinstellungen

Der Inhalt der Härtungseinstellungen ServiceNow, Inc. Security Center enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins in Now Platform. Sie können diese Eigenschaften mit der App für Härtungseinstellungen im Security Center festlegen.

Übersicht und Zweck

Das Sicherheitscenter berechnet eine tägliche Compliance-Punktzahl, ausgedrückt als Prozentsatz, der darauf basiert, wie konform Ihre aktuellen Instanz-Sicherheitseinstellungen mit den Compliance-Werten in den Härtungseinstellungen von Security Center sind.

Sie können die spezifischen Sicherheitskonfigurationseinstellungen, die sich auf die Punktzahl für Ihre Instanz auswirken können, direkt im Sicherheitscenter verwalten.

Die Konfigurationen der Härtungseinstellungen werden mit mehreren Attributen erläutert, die in der Tabelle beschrieben sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdetails der Härtungseinstellungen

Konfigurationsattribut	Beschreibung
Übersicht	Bietet einen allgemeinen Überblick über die Empfehlung.
Konfigurationsname	Eigenschaft oder Plugin-Name.
Konfigurationstyp	Beschreibt, wo die Eigenschaft außerhalb des Sicherheitscenters konfiguriert werden kann, z. B. in den Systemeigenschaften (*sys_properties_list.do*).
Datentyp	Beschreibt den Typ des für die Konfiguration erforderlichen Werts. Beispiele sind true/false boolean, Installation, Plugin, Zeichenfolge usw.
Empfohlener Wert	Der vom Sicherheitscenter empfohlene Wert zur Verbesserung der Sicherheits-Compliance in Ihrer Instanz.
Standardwert	Der Wert, auf den die Konfiguration im Basissystem festgelegt ist.
Kategorie	Der Name und der Link zur Kategorie für die Härtungseinstellung.
Sicherheitsrisiko	**Schweregradpunktzahl**: Die Punktzahl gibt das potenzielle Sicherheitsrisiko für Ihre Instanz in Abhängigkeit von der Wahrscheinlichkeit der Ausnutzung der Schwachstelle an. Die Sicherheitsschwachstelle wird einzeln betrachtet und anhand der CVSS-Punktzahl (Common Vulnerability Scoring System) auf einer Skala von **0,0** bis **10,0**bewertet. Weitere Informationen finden Sie unter https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator .
	Schweregradbewertung pro CVSS-Punktzahl: • Kritisch: 9,0–10,0 • Hoch: 7,0–8,9 • Mittel: 4,0–6,9 • Niedrig: 0,01–3,9 • Keine: 0,0
	Details zum Sicherheitsrisiko: Beschreibt die Bedeutung der Einstellungskonfiguration und das Risiko, die empfohlene Konfiguration nicht zu verwenden.
Abhängigkeiten und Voraussetzungen	Zugehörige Einstellungen oder Konfigurationen, die vor oder in Verbindung mit der Härtungskonfiguration erforderlich sind.
Funktionale Auswirkung	Die Auswirkungen dieser Härtungseinstellung auf den Betrieb Ihrer Instanz.
Referenzen	Links zu Konfigurationsdokumentation oder anderen hilfreichen Informationen.

Hinweis:
Einige der Konfigurationen können nur von Kundenservice und Support abgeschlossen werden und werden als solche angegeben.

Weitere Informationen dazu, wie Sie sicherstellen können, dass Ihre Instanzen die Härtungsanforderungen erfüllen, finden Sie unter Sicherheitshärtung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere Ressourcen

Zur Benutzerreferenz enthält Now Platform ausführliche Informationen zu Konfigurationsfunktionen in der Produktdokumentation. Sie greifen auf die meisten Sicherheitsinhalte über die Links in Instanz sichernzu. Siehe auch:

- Verfügbare Systemeigenschaften
- Eigenschaften der allgemeinen Sicherheitseinstellungen
- Strenge Sicherheitseinstellungen

Baseline der Härtungseinstellungen

Erkunden Sie, wie unterschiedliche Baselineversionen für Härtungseinstellungen mit verschiedenen Familien- und Store-Releases übereinstimmen.

Security Center funktioniert, indem eine Teilmenge von Systemeigenschaften aus einer Instanz erfasst und ihre Konfigurationsdetails zusammen mit den Sicherheitsauswirkungen der Nichteinhaltung innerhalb der App angezeigt werden. Die Baseline dient als Referenzpunkt für die Systemeigenschaften, die mit jedem Release der Security Center-App erfasst werden.

Übersicht über die Baseline der Härtungseinstellungen

Security Center-Version	Baselineversion der Härtungseinstellung	Unterstützte Familien	Store-Releasedatum	Wird standardmäßig mit installiert
SSC v1.1	Baseline v1.0	Utah, Vancouver	Mai 2023	Familie Vancouver
SSC v1.2	Baseline v1.0	Utah, Vancouver	August 2023	Nur speichern
SSC v1.3	Baseline v2.0	Vancouver, Washington	November 2023	Familie Washington
SSC v1.4	Baseline v4.0	Washington, Xanadu	Mai 2024	Xanadu

Neue Härtungseinstellungen

Hier ist eine Liste aller neuen Härtungseinstellungen, die mit der Security Center Version 2.0-Baseline veröffentlicht wurden.

- Verwendung des Alias für Anmeldeinformationen erzwingen [Aktualisiert in Security Center 1.5]
- OCSP-Prüfung bei Netzwerkfehlern erzwingen [Neu in Security Center 1.3]
- Zertifikatkette und Hostname überprüfen [Neu in Security Center 1.3]
- Zertifikatwiderruf überprüfen [Neu in Security Center 1.3]
- Sicherheitsrichtlinie für sichere Inhalte für SVG-Dateien festlegen [Neu in Security Center 1.3]
- Verwendung des Vorgangs zum sicheren Einfügen mehrerer Elemente innerhalb der Import Set-API
- Plugin „Protected Tables“ aktivieren [Neu in Security Center 1.3]
- Sichere Referrerrichtlinie erzwingen [Neu in Security Center 1.3]
- Rollen für Zeitüberschreitungsausnahmen für aktive Sitzungen definieren [Neu in Security Center 1.3]
- Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1.3]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MIME-Typ der Datei im SOAP Web Service „AttachmentCreator“ validieren [Neu in Security Center 1.3]
- Zertifikatsbasierte Authentifizierung nicht erzwungen
- Sitzungsaudit-Ereignisse protokollieren [Neu in Security Center 1.3]
- Authentifizierung für Event Management-HTTP-Prozessor erforderlich [Neu in Security Center 1.3]
- Sicherheitsregeln für die Freigabe von Dashboards erzwingen – Neu in Security Center 1.3]
- Klonen von Zielen nicht zulassen [Neu in Security Center 1.3]
- Bereichssicherheit für digitale Services des öffentlichen Sektors erzwingen [Neu in Security Center 1.3]
- Bereichsbezogenen ACL-Zugriff für Informationsanforderungs-Playbooks erzwingen – Neu in Security Center 1.3]
- Lebensdauer aktiver Sitzungen des Gasts begrenzen [Neu in Security Center 1.3]
- Größe des HTTP-Antworttexts begrenzen [Aktualisiert in Security Center 1.5]
- Lebensdauer aktiver Sitzungen von Integrationen begrenzen [Neu in Security Center 1.3]
- Zugriff auf Knowledge Bases beschränken [Neu in Security Center 1.3]
- Benutzerkommentare zu Artikeln ausblenden [Neu in Security Center 1.3]
- oauth-Parameter auf Post-Text beschränken [Neu in Security Center 1.3]
- Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen [Aktualisiert in Security Center 1.5]
- Sicherstellen, dass das Erstellen/Löschen von Dashboards eine Zugriffsprüfung erfordert [Neu in Security Center 1.3]
- Legacy-Verhalten für GlideRecord-Umfangsbegrenzung aktivieren [Neu in Security Center 1.3]
- Einschränkungen des Anwendungsbereichs erzwingen [In Security Center 1.5 entfernt]
- Schreibzugriff erfordern, um auf die Seite „Element hinzufügen“ im Servicekatalog zuzugreifen [Neu in Security Center 1.3]
- Validierungszeit für Anti-CSRF-Token [Neu in Security Center 1.3]
- Sicherstellen, dass ACLs für Archivtabellen aktiviert sind [Neu in Security Center 1.3]
- Geschützten Java-Sicherheitsmanager aktivieren [Neu in Security Center 1.3]
- Strikte Erhöhungsberechtigung erzwingen [Neu in Security Center 1.3]
- Leeren der Zwischenablage anfordern, wenn mobile Anwendung im Hintergrund ausgeführt wird [Neu in Security Center 1.3]
- Anforderungen für Geräteverschlüsselung und Passcode erzwingen [Neu in Security Center 1.3]
- Lebensdauer aktiver UI-Sitzungen begrenzen [Neu in Security Center 1.3]
- MID-Auditprotokoll aktivieren [Aktualisiert in Security Center 1.5]
- Erforderliche JMS-Verbindungsfactorys [Aktualisiert in Security Center 1.5]
- Captcha für Gast-Walk-up-Experience in der Kundenserviceanwendung anfordern [Aktualisiert in Security Center 1.5]
- Identitätswechsel bei ACL-Auswertung in HR-App überprüfen [Aktualisiert in Security Center 1.5]
- HR-Fallaktualisierungen aus persönlichen E-Mails beschränken [Aktualisiert in Security Center 1.5]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisierte Härtungseinstellungen

Diese Liste enthält die Härtungseinstellungen, die in Security Center Baselineversion 2.0 aktualisiert wurden.

Dokumentation	Updates
Beschränken Sie JSONP-Anforderungen auf vertrauenswürdige URLs	• Neue Kurzbeschreibung: JSONP-Anforderungen auf vertrauenswürdige URLs beschränken • Alte Kurzbeschreibung: Aufnahmeliste für JSONP-Anforderungen
Minimieren Sie die zulässige Anhangsgröße	• Neue Kurzbeschreibung: Zulässige Anhangsgröße minimieren • Alte Kurzbeschreibung: Max. zulässige Anhangsgröße
Zertifikatvertrauen erzwingen [In Security Center 1.5 entfernt]	• Neue Kurzbeschreibung: Zertifikatvertrauen erzwingen • Alte Kurzbeschreibung: Certificate Trust
Xframe-Optionen festlegen, um das Einbetten von Websites von Drittanbietern zu verhindern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Legen Sie die Xframe-Optionen so fest, dass das Einbetten von Websites von Drittparteien verhindert wird • Alte Kurzbeschreibung: Xframe-Optionen
HTML-Bereinigung in Virtual Agent aktivieren	• Neue Kurzbeschreibung: HTML-Bereinigung in Virtual Agent aktivieren • Alte Kurzbeschreibung: Aktivieren Sie die HTML-Bereinigung
Lesezugriff für delegierte Entwickler beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Lesezugriff für delegierte Entwickler beschränken • Alte Kurzbeschreibung: Delegierte Entwickler – Allow-Liste für Lesezugriff
Bewertung und Filterung von E-Mail-Spam aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Aktivieren Sie die Bewertung und Filterung von E-Mail-Spam • Alte Kurzbeschreibung: Bewertung und Filterung von E-Mail-Spam

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Hochsicherheits-Plugin [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Hochsicherheits-Plugin aktivieren • Alte Kurzbeschreibung: Hochsicherheits-Plugin
Plugin für kontextbezogene Sicherheit aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Aktivieren Sie das Contextual Security Plugin • Alte Kurzbeschreibung: Contextual Security Plugin
HTML-Bereinigung erzwingen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: HTML-Bereinigung erzwingen • Alte Kurzbeschreibung: Nicht bereinigten HTML-Code überprüfen
Gastbenutzer für SOAP-Anforderungen festlegen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Gastbenutzer für SOAP-Anforderungen festlegen • Alte Kurzbeschreibung: Gastbenutzer für SOAP-Anforderungen
Aktivieren Sie das SNC-Zugriffssteuerungs-Plugin	• Neue Kurzbeschreibung: SNC-Zugriffssteuerungs-Plugin aktivieren • Alte Kurzbeschreibung: SNC Access Control-Plugin
Sicherheits-Jump-Start-Plugin aktivieren (ACL-Regeln) [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Sicherheits-Jump-Start-Plugin aktivieren • Alte Kurzbeschreibung: Sicherheits-Jump-Start-Plugin (ACL-Regeln)
Legacy-AngularJS-Verhalten deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Legacy AngularJS-Verhalten deaktivieren • Alte Kurzbeschreibung: Legacy AngularJS Behavior
Begrenzen Sie gleichzeitige interaktive Sitzungen	• Neue Kurzbeschreibung: Gleichzeitige interaktive Sitzungen begrenzen • Alte Kurzbeschreibung: Glide Authenticate Limit Gleichzeitige interaktive Sitzungen begrenzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Gleichzeitige Sitzungen auf allen Knoten beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Gleichzeitige Sitzungen auf allen Knoten begrenzen • Alte Kurzbeschreibung: Glide Authenticate Limit Gleichzeitige Sitzungen auf allen Knoten authentifizieren
Anzahl gleichzeitiger interaktiver Sitzungen minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Anzahl gleichzeitiger interaktiver Sitzungen minimieren • Alte Kurzbeschreibung: Glide Authenticate Max. gleichzeitige interaktive Sitzungen
Rollenbasierte Multifaktor-Authentifizierung aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Aktivieren Sie die rollenbasierte Multifaktor-Authentifizierung • Alte Kurzbeschreibung: Rollenbasierte Multifaktor-Authentifizierung
Aktualisierte Version des Multi-SSO-Plugins aktivieren [In Security Center 1.5 aktualisiert]	• Neue Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins aktivieren • Alte Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins ist aktiviert
Dauer der SAML-Einschränkung „notBefore“ oder „notOnOrAfter“ minimieren [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: SAML-Einschränkungsdauer „notBefore“ oder „notOnOrAfter“ minimieren • Alte Kurzbeschreibung: SAML-Einschränkung „notBefore“ oder „notOnOrAfter“.
Autorisierung für API-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für API-Anforderungen erforderlich • Alte Kurzbeschreibung: API-Anforderungsautorisierung
Autorisierung für CSV-Anforderungen anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für CSV-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von CSV-Anforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Autorisierung für Daten-Broker-REST-API anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für Daten-Broker-REST-API erforderlich • Alte Kurzbeschreibung: Datenbroker-REST-API-Autorisierung
Autorisierung für Excel-Anforderungen anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für Excel-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von Excel-Anforderungen
Autorisierung für Importanforderungen anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für Importanforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von Importanforderungen
Autorisierung für JSONv2-Anforderung anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für JSONv2-Anforderung erforderlich • Alte Kurzbeschreibung: Autorisierung von JSONv2-Anforderungen
Autorisierung für PDF-Anforderungen anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für PDF-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von PDF-Anforderungen
Autorisierung für RSS-Anforderungen anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für RSS-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von RSS-Anforderungen
Autorisierung für SCHEMA-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für SCHEMA-Anforderungen erforderlich • Alte Kurzbeschreibung: SCHEMA-Anforderungsautorisierung
Autorisierung für SOAP-Anforderungen erfordern [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Autorisierung für SOAP-Anforderungen erforderlich • Alte Kurzbeschreibung: SOAP-Anforderungsautorisierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Berechtigung für Entladeanforderungen anfordern	• Neue Kurzbeschreibung: Autorisierung für Entladeanforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von Entlade-Anforderungen
Autorisierung für WSDL-Anforderung anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für WSDL-Anforderung erforderlich • Alte Kurzbeschreibung: WSDL-Anforderungsautorisierung
Berechtigung für XML-Anforderungen anfordern	• Neue Kurzbeschreibung: Autorisierung für XML-Anforderungen erforderlich • Alte Kurzbeschreibung: XML-Anforderungsautorisierung
Berechtigung für XML-Ausgabeanforderungen erfordern	• Neue Kurzbeschreibung: Autorisierung für XML-Ausgabeanforderungen erforderlich • Alte Kurzbeschreibung: XML-Ausgabeautorisierung
Kennzeichnung für „Nur-HTTP-Cookie“ aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Aktivieren Sie die Kennzeichnung für „Nur-HTTP-Cookie“. • Alte Kurzbeschreibung: Kennzeichnung für „Nur-HTTP-Cookie“
Deaktiviert die Ausführung der Rohdatenbankabfrage	• Neue Kurzbeschreibung: Ausführung von Rohdatenbankabfragen deaktivieren • Alte Kurzbeschreibung: Anforderungen für Zugriffssteuerung auf Vorgangsebene
SQL-Fehlermeldungen deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: SQL-Fehlermeldungen deaktivieren • Alte Kurzbeschreibung: SQL-Fehlermeldungen werden deaktiviert
Eingehende E-Mail-Bilder in Anhänge konvertieren [In Security Center 1.5 entfernt]	• Neue Kurzbeschreibung: Eingehende E-Mail-Bilder in Anhänge konvertieren • Alte Kurzbeschreibung: Eingehende E-Mail in HTML konvertieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
SMTP-Empfängeranzahl minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: SMTP-Empfängermenge minimieren • Alte Kurzbeschreibung: Max. SMTP-Empfänger
Excel-Formeln mit Escape-Zeichen versehen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Excel-Formeln mit Escape-Zeichen versehen • Alte Kurzbeschreibung: Excel-Formel mit Escape-Zeichen versehen
HTML-Bereinigung aktivieren [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: HTML-Bereinigung aktivieren • Alte Kurzbeschreibung: HTML-Bereinigung
Cache-Control-HTTP-Header-Wert [Entfernt in Security Center 1.5]	• Neue Kurzbeschreibung: Cache-Steuerung HTTP-Header-Wert • Alte Kurzbeschreibung: Cache-Control-HTTP-Header-Wert
Verhalten von Produktionsinstanzen erzwingen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Verhalten der Produktionsinstanz erzwingen • Alte Kurzbeschreibung: Verhalten der Produktionsinstanz
Definieren zulässiger ServiceNow interner IP-Adressen [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Zulässige interne ServiceNow-IP-Adressen definieren • Alte Kurzbeschreibung: Allow-Liste für IP-Adressenzugriff
Legacy-JQuery-Verhalten deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Legacy-JQuery-Verhalten deaktivieren • Alte Kurzbeschreibung: Legacy-JQuery-Verhalten
Anfänglicher eindeutiger LDAP-Name aufheben [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Anfänglichen eindeutigen LDAP-Namen aufheben • Alte Kurzbeschreibung: Anfänglicher eindeutiger LDAP-Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Zugriff auf benutzerdefinierte Journaleinträge beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Zugriff auf benutzerdefinierte Journaleinträge beschränken • Alte Kurzbeschreibung: Sichere benutzerdefinierte Journaleinträge
Einmalige Lebensdauer der Verifizierung außerhalb des Bereichs minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Einmalige Lebensdauer der Verifizierung außerhalb des Bereichs minimieren • Alte Kurzbeschreibung: Kurze einmalige Lebensdauer der Verifizierung außerhalb des Bereichs
Ausgehende SSLv2-/SSLv3-Verbindungen deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Ausgehende SSLv2/SSLv3-Verbindungen deaktivieren • Alte Kurzbeschreibung: SSLv2/SSLv3 wird deaktiviert
Erstellung von Anwendern aus eingehenden E-Mails deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Erstellung von Anwendern aus eingehenden E-Mails deaktivieren • Alte Kurzbeschreibung: E-Mails nach Domäne beschränken
Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Standardauthentifizierung für vom Client aufrufbare Skripteinbindungen anfordern • Alte Kurzbeschreibung: Datenschutz für vom Client aufrufbare Skripteinbindungen
Standardauthentifizierung für vom Client aufrufbare Skripteinbindungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Standardauthentifizierung für vom Client aufrufbare Skripteinbindungen anfordern • Alte Kurzbeschreibung: Datenschutz für vom Client aufrufbare Skripteinbindungen
AJAXGlideRecord-ACL-Überprüfung anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: AJAXGlideRecord-ACL-Überprüfung erforderlich • Alte Kurzbeschreibung: AJAXGlideRecord-ACL-Überprüfung wird aktiviert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Sandbox für vom Client generierte Skripts erzwingen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Sandbox für vom Client generierte Skripts erzwingen • Alte Kurzbeschreibung: Vom Client generierte Skripts-Sandbox
Strikte Validierung des CSRF-Tokens erzwingen [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Strikte Validierung des CSRF-Tokens erzwingen • Alte Kurzbeschreibung: Strikte CSRF-Validierung
Hochgeladene MIME-Typen beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Hochgeladene MIME-Typen beschränken* Kurzbeschreibung • Alte Kurzbeschreibung: MIME-Typeinschränkung für Uploads, STANDARDWERT VON WAHR IN FALSCH GEÄNDERT
Aktivieren Sie ACLs für bereichsbezogene Administratoranwendungen	• Neue Kurzbeschreibung: ACLs für bereichsbezogene Administratoranwendungen aktivieren • Alte Kurzbeschreibung: ACLs für bereichsbezogene Administratoranwendungen verwalten
Anti-CSRF-Token aktivieren [In Security Center 1.5 entfernt]	• Neue Kurzbeschreibung: Anti-CSRF-Token aktivieren • Alte Kurzbeschreibung: Anti-CSRF-Token
Implementieren Sie die Sicherheitskopfzeile x-frame-options: SAMEORIGIN	• Neue Kurzbeschreibung: Implementiert die X-Frame-Options: SAMEORIGIN-Sicherheitskopfzeile • Alte Kurzbeschreibung: X-Frame-Optionen: SAMEORIGIN
Verschleierung der Mobile-App-UI erforderlich machen	• Neue Kurzbeschreibung: Verschleierung der Mobile-App-UI erforderlich • Alte Kurzbeschreibung: Mobile-App-UI-Verschleierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Standardmäßig mit leeren ACLs verweigern	• Neue Kurzbeschreibung: Standardmäßig verweigern mit leeren ACLs • Alte Kurzbeschreibung: Sicherheitsmanager-Standardverweigerung
Validieren Sie den SOAP-Inhaltstyp	• Neue Kurzbeschreibung: SOAP-Inhaltstyp validieren • Alte Kurzbeschreibung: SOAP-Inhaltstypprüfung
Erzwingen Sie strikte Sicherheit für SOAP-Anforderungen	• Neue Kurzbeschreibung: Strikte Sicherheit für SOAP-Anforderungen erzwingen • Alte Kurzbeschreibung: Strikte Sicherheit für SOAP-Anforderungen
Accountwiederherstellung aktivieren [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Accountwiederherstellung aktivieren • Alte Kurzbeschreibung: Accountwiederherstellung
Erfordert XMLdoc2-Entitätsvalidierung mit allowlistDisable-Entitätserweiterung	• Neue Kurzbeschreibung: XMLdoc2-Entitätsvalidierung mit allowlistDisable-Entitätserweiterung erforderlich • Alte Kurzbeschreibung: XMLdoc2-Entitätsvalidierung mit allowlistDisable-Entitätserweiterung
Domänentrennung auf Punkt-zu-Punkt-Felder anwenden [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Domänentrennung auf Punkt-zu-Punkt-Felder anwenden • Alte Kurzbeschreibung: Domänentrennung anwenden
Beschränken Sie herunterladbare MIME-Typen	• Neue Kurzbeschreibung: Herunterladbare MIME-Typen beschränken • Alte Kurzbeschreibung: Deny-Liste des herunterladbaren MIME-Typs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Eingeschränkte herunterladbare MIME-Typen definieren [In Security Center 1.5 entfernt]	• Neue Kurzbeschreibung: Eingeschränkte herunterladbare MIME-Typen definieren • Alte Kurzbeschreibung: Herunterladbare MIME-Typen
Escape-Jelly-Skript	• Neue Kurzbeschreibung: Jelly-Skript mit Escape-Zeichen • Alte Kurzbeschreibung: Escape Jelly
HTML in Listenansichten mit Escape-Zeichen versehen	• Neue Kurzbeschreibung: HTML in Listenansichten mit Escape-Zeichen versehen • Alte Kurzbeschreibung: Escape-HTML
Escape-Skripts in Scratchpad	• Neue Kurzbeschreibung: Escape-Skripts in Scratchpad • Alte Kurzbeschreibung: Escape-Scratchpad
XML-Markup mit Escape-Zeichen versehen	• Neue Kurzbeschreibung: Escape-XML-Markup • Alte Kurzbeschreibung: Escape-XML
Verschleierung der klassischen Mobile-App-UI erforderlich machen	• Neue Kurzbeschreibung: Verschleierung der Benutzeroberfläche der Classic Mobile-App erforderlich • Alte Kurzbeschreibung: UI-Verschleierung der klassischen mobilen App
Öffentlicher Zugriff auf Favoriten	• Neue Kurzbeschreibung: Öffentlichen Zugriff auf Favoriten deaktivieren • Alte Kurzbeschreibung: Öffentlicher Zugriff auf Favoriten
Strikte Sicherheit von Sitzungscookies erzwingen	• Neue Kurzbeschreibung: Strikte Sicherheit von Sitzungscookies erzwingen • Alte Kurzbeschreibung: Cookies für sichere Sitzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Deaktivieren Sie eingebetteten HTML-Code	• Neue Kurzbeschreibung: Eingebetteter HTML-Code deaktivieren • Alte Kurzbeschreibung: Eingebetteter HTML-Code
Deaktivieren Sie JavaScript-Tags in eingebettetem HTML	• Neue Kurzbeschreibung: JavaScript-Tags in eingebettetem HTML deaktivieren • Alte Kurzbeschreibung: Javascript-Tags in eingebettetem HTML zulassen
Minimieren Sie die Zeitüberschreitungsdauer der Sitzungsaktivität	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer der Sitzungsaktivität minimieren • Alte Kurzbeschreibung: Zeitüberschreitung für Sitzungsaktivität
Beschränken Sie herunterladbare Dateitypen in statischen Inhalten	• Neue Kurzbeschreibung: Herunterladbare Dateitypen in statischem Inhalt beschränken • Alte Kurzbeschreibung: Dateityp-Downloadbeschränkungen aus statischem Inhalt
Minimieren Sie die Zeitüberschreitungsdauer des Sitzungsfensters	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer des Sitzungsfensters minimieren • Alte Kurzbeschreibung: Zeitüberschreitung für Sitzungsfenster
Minimieren Sie die absolute Zeitüberschreitungsdauer der Sitzung	• Neue Kurzbeschreibung: Absolute Zeitüberschreitungsdauer der Sitzung minimieren • Alte Kurzbeschreibung: Absolute Zeitüberschreitung für Sitzung
Maximieren Sie die Zeitüberschreitungsdauer beim Entsperren der fehlgeschlagenen Anmeldung	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer bei Entsperren bei fehlgeschlagener Anmeldung maximieren • Alte Kurzbeschreibung: Zeitüberschreitung beim Entsperren nach fehlgeschlagenen Anmeldungen verwalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Beschränken Sie externe XML-Entitäten	• Neue Kurzbeschreibung: Externe XML-Entitäten beschränken • Alte Kurzbeschreibung: URL-Zulassungsliste für XML-Entitätsvalidierung
Schwellenwert für Entitätserweiterung minimieren [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Schwellenwert für Entitätserweiterung minimieren • Alte Kurzbeschreibung: Schwellenwert für Entitätserweiterung wird festgelegt
Minimieren Sie die Ablaufdauer der Anforderung zum Zurücksetzen des Passworts	• Neue Kurzbeschreibung: Ablaufdauer der Anforderung für Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Ablauf der Anforderung zum Zurücksetzen des Passworts
Minimieren Sie den maximalen zulässigen Versuch für die Anforderung zum Zurücksetzen des Passworts	• Neue Kurzbeschreibung: Maximale Versuche für Anforderung zur Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Maximale Versuche für Anforderung zum Zurücksetzen des Passworts
Fensterdauer für maximale Versuche für Anforderung zum Zurücksetzen des Passworts minimieren	• Neue Kurzbeschreibung: Fensterdauer für maximale Versuche bei Anforderung einer Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Fenster für max. Versuche für Anforderung zum Zurücksetzen des Passworts
Maximieren Sie die Dauer des Wiederholungsfensters für die Anforderung zum Zurücksetzen des Passworts	• Neue Kurzbeschreibung: Fensterdauer für Wiederholungsanforderung für Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Fenster für Wiederholungsanforderung für Passwortzurücksetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Minimieren Sie die Dauer des Fensters für die erfolgreiche Anforderung einer Passwortzurücksetzung	• Neue Kurzbeschreibung: Fensterdauer bei erfolgreicher Anforderung einer Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Fenster „Passwortzurücksetzungsanforderung erfolgreich“.
Maximieren Sie die Dauer des Entsperrungsfensters für die Anforderung zum Zurücksetzen des Passworts	• Neue Kurzbeschreibung: Fensterdauer für Entsperrungsanforderung für Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Anforderung zum Zurücksetzen des Passworts Entsperren Fenster
Maximieren Sie die SMS-Komplexität beim Zurücksetzen des Passworts	• Neue Kurzbeschreibung: SMS-Komplexität für Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Passwort zurücksetzen SMS-Komplexität
Minimieren Sie die Ablaufdauer der SMS für die Passwortzurücksetzung	• Neue Kurzbeschreibung: SMS-Ablaufdauer für Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: SMS-Ablauf Passwort zurücksetzen
Minimieren Sie die maximale Anzahl von SMS pro Tag für die Passwortzurücksetzung	• Neue Kurzbeschreibung: Max. SMS pro Tag für Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Passwort zurücksetzen – max. SMS pro Tag
Maximieren Sie die Dauer des SMS-Pause-Fensters für die Passwortzurücksetzung	• Neue Kurzbeschreibung: Fensterdauer für SMS-Pause für Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Fenster „Passwort zurücksetzen SMS-Pause“.
Aktivieren Sie die SMS-Codebenachrichtigung für die Registrierung und Verifizierung	• Neue Kurzbeschreibung: SMS-Codebenachrichtigung für Registrierung und Verifizierung aktivieren • Alte Kurzbeschreibung: SMS-Codebenachrichtigung für Registrierung und Verifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Maximieren Sie die Verzögerungsdauer der Verifizierung der Passwortzurücksetzung	• Neue Kurzbeschreibung: Verzögerungsdauer der Verifizierung der Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Verzögerung der Verifizierung der Passwortzurücksetzung
Benutzer während des Prozesses zum Zurücksetzen/Ändern des Passworts benachrichtigen [In Security Center 1.5 entfernt]	• Neue Kurzbeschreibung: Benutzer während des Prozesses zur Passwortzurücksetzung/-änderung benachrichtigen • Alte Kurzbeschreibung: Benachrichtigungsprozess für Passwortzurücksetzung/-änderung
E-Mail-Domänen für die Registrierung externer Benutzer beschränken [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: E-Mail-Domänen für externe Benutzerregistrierung beschränken • Alte Kurzbeschreibung: E-Mail-Domänen-Allow-Liste für externe Benutzerregistrierung
Minimieren der Ablaufdauer des Links für die Registrierung externer Benutzer [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Ablaufdauer des Links zur Registrierung externer Benutzer minimieren • Alte Kurzbeschreibung: Link für externe Benutzerregistrierung abgelaufen
Beschränken zulässiger Java-Pakete	• Neue Kurzbeschreibung: Zulässige Java-Pakete beschränken • Alte Kurzbeschreibung: Allow-Liste für Java-Pakete

Härtungseinstellungen gelöscht

Diese Liste enthält die Härtungseinstellungen, die in Security Center Baselineversion 2.0 entfernt wurden.

- Codesignatur für Anwendungskonfigurationsdaten und Skripte aktivieren
- Glide KMF-Verschlüsseler aktivieren
- Verwendung des Verschlüsselers auf Instanzebene deaktivieren
- Alle ausgehenden HTTP-Anforderungsfelder protokollieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerung

Die Zugriffskontrollkategorie prüft den Prozess des Schutzes von Ressourcen vor nicht autorisiertem Zugriff durch Gewähren und Verweigern von Anforderungen basierend auf einem Berechtigungsmodell. Dazu gehört es sicherzustellen, dass eine Entität, die auf eine Ressource zugreift, über gültige Anmeldeinformationen verfügt, ein wohl definierter Satz von Rollen oder Berechtigungen erstellt und geschützt wird und sichergestellt wird, dass Rollen- oder Berechtigungssteuerungen vor Wiedergabe und Manipulation geschützt sind.

Zugriffskontrollen bestimmen, ob der Zugriff auf eine bestimmte Ressource gewährt oder verweigert werden soll. Ermöglicht den Zugriff auf Ressourcen nur für die Benutzer, die berechtigt sind, sie zu verwenden.

Validierungszeit für Anti-CSRF-Token [Neu in Security Center 1.3]

Die Eigenschaft *glide.security.csrf_previous.time_limit* gibt die Zeit in Sekunden an, nach der ein sicheres Token abläuft.

Wenn eine Benutzersitzung abläuft, läuft das sichere Token mit ihr ab, es sei denn, die Eigenschaft, die **die Wiederverwendung abgelaufener Token zulässt**, ist aktiviert und liegt innerhalb des durch diese Eigenschaft beschriebenen Zeitrahmens. Dieses Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.csrf_previous.time_limit*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	86400
Standardwert	86.400 Sekunden oder 1 Tag
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt wird, wird die Tokenvalidierung deaktiviert, die verwendet wird, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft bestimmt die Dauer in Sekunden, für die ein sicheres Token gültig bleibt. Das sichere Token läuft ab, wenn die Benutzersitzung abläuft, es sei denn, die Eigenschaft, die **die Wiederverwendung abgelaufener Token** ermöglicht, ist aktiviert und das Token befindet sich innerhalb des in dieser Eigenschaft angegebenen Zeitrahmens. Dieses Token verhindert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Site-übergreifende Angriffe durch gefälschte Anforderungen. Er hat einen Standardwert von 86.400 Sekunden oder 1 Tag.

Domänentrennung auf Punkt-zu-Punkt-Felder anwenden [Aktualisiert in Security Center 1.5]

Die Eigenschaft `glide.sys.domain.include_domain_condition_on_join` steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie die Domänentrennungsfunktion für Punkt-zu-Punkt-Felder anwenden.

Diese Eigenschaft `glide.sys.domain.include_domain_condition_on_join` steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie die Domänentrennungsfunktion für Punkt-zu-Punkt-Felder anwenden. Wenn `glide.sys.domain.include_domain_condition_on_join` in einer Instanz mit Domänentrennung nicht auf den empfohlenen Wert „true“ festgelegt ist, können vertrauliche Informationen offengelegt werden, die nicht mit einer bestimmten Domäne geteilt werden sollen.

Hinweis:
Wenn das Plugin „Domain Separation“ installiert ist, wird ein sys_properties-Datensatz für diese Eigenschaft installiert, dessen Wert auf **true**festgelegt ist, was dem Standardwert entspricht. Andernfalls, in dem Basissystem ohne installierte Domänentrennung, ist der Eigenschaftsdatensatz nicht vorhanden, und er hat seinen nicht standardmäßigen Wert.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sys.domain.include_domain_condition_on_join`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	„True“, wenn die Domänentrennung installiert ist, andernfalls ist die Eigenschaft nicht vorhanden.
Standardwert	false
Kategorie	Zugriffssteuerung
Zweck	Steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie die Domänentrennungsfunktion für Punkt-zu-Punkt-Felder anwenden.
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn `glide.sys.domain.include_domain_condition_on_join` nicht auf den empfohlenen Wert **true**festgelegt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	ist, können vertrauliche Informationen offengelegt werden, die nicht mit einer bestimmten Domäne geteilt werden sollen.
Referenzen	Domänentrennung für Service Provider

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktivieren Sie ACLs für bereichsbezogene Administratoranwendungen

`glide.security.scoped_administration.honor_global_acl` bestimmt, ob eine Anwendungsverwaltungs-App die Regeln der globalen Zugriffssteuerungsliste (ACL) erben kann.

Diese Eigenschaft ist besonders nützlich, wenn keine bereichsbezogenen Administratoranwendungs-ACLs für den Datensatzbereich definiert sind.

Legen Sie `glide.security.scoped_administration.honor_global_acl` auf „true“ fest, um zu verhindern, dass ein Benutzer mit geringen Berechtigungen mit Berechtigungen für die Anwendung potenziell auf vertrauliche Datensätze zugreift.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.scoped_administration.honor_global_acl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Steuert die ACL-Zugriffsregel in der bereichsbezogenen Administratoranwendung.
Empfohlener Wert	Wahr
Standardwert	Wahr
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) Wenn der Eigenschaftswert „wahr“ ist und keine bereichsbezogenen Administratoranwendungs-ACLs für den Datensatzbereich definiert sind, werden die globalen ACLs berücksichtigt. Bei Festlegung auf „falsch“ werden ACL-Prüfungen ignoriert, wenn für den Datensatzbereich keine bereichsbezogenen Administratoranwendungs-ACLs definiert sind.
Sicherheitsrisikobewertung	3.8
Referenzen	Access control rules in application administration apps

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin

Zugriff für delegierten Entwickler blockieren

Diese Konfiguration wirkt sich auf den Zugriff für delegierte Entwickler aus, die Benutzerrollen über ein Skript aktualisieren. Wenn die Konfiguration konform ist, kann der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entwickler keine Datensätze aktualisieren oder in die Tabelle sys_user_has_role einfügen, ohne auch die Rolle „user_admin“ zu haben.

Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf. Wenn die Eigenschaft Rollen enthält, können nur diese Rollen Skriptmodule ausführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.sys.security.delegateddev.block_grant_roles`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf.
Typ	Umschalter
Empfohlener Wert	Wahr
Sicherheitsabhängigkeiten	Keine
Sicherheitsrisikobewertung	6.7
Funktionale Auswirkung	(Hoch) Wenn ein Benutzer mit der Rolle „delegated_developer“ versucht, einen Datensatz in der Tabelle „sys_user_has_role“ zu ändern, aktiviert diese Eigenschaft zusätzliche Sicherheitsprüfungen für den Vorgang. Die zusätzlichen Sicherheitsprüfungen überprüfen, ob dem Benutzer die Rolle user_admin] zugewiesen wurde, wenn er versucht, die Tabelle „sys_user_has_role“ [zu erstellen oder zu aktualisieren. Wenn sie nicht über die Rolle user_admin verfügen, wird der Zugriff verweigert. Wenn die Eigenschaft „false“ ist, werden diese zusätzlichen Prüfungen nicht validiert.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung können nicht autorisierte Benutzer auf vertrauliche Inhalte/Daten in der Instanz zugreifen.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Abgelaufene CSRF-Token blockieren [Aktualisiert in Security Center 1.5]

Blockieren Sie abgelaufene CSRF-Token, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.

Übersicht

Siteübergreifende Anforderungsfälschungen sind eine Art von böswilligem Exploit, bei dem nicht autorisierte Befehle im Namen eines authentifizierten Benutzers ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdetails

Attribut	Beschreibung
Übersicht	Steuert die Verwendung eines abgelaufenen sicheren Tokens zum Identifizieren und Validieren eingehender Anforderungen. Legen Sie den Wert auf „ **false** “ fest, um zu verhindern, dass ein zuvor abgelaufenes Token eine eingehende Anforderung validiert.
Konfigurationsname	`glide.security.csrf_previous.allow`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	**false**
Standardwert	**true**
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	**Schweregradpunktzahl**: 6,5
	Schweregradbewertung pro CVSS-Punktzahl: Mittel
	Details zum Sicherheitsrisiko: Erzwingt einen robusten Anti-CSRF-Mechanismus zum Schutz authentifizierter Funktionen, und effektive Anti-Automatisierungs- oder Anti-CSRF-Funktionen schützen nicht authentifizierte Funktionen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Anti-CSRF-Token aktivieren [In Security Center 1.5 entfernt], websiteübergreifende Anforderungsfälschung .

Überprüfen Sie die Bedingungen der UI-Aktion vor der Ausführung

Verwenden Sie die Eigenschaft `glide.security.strict.actions`, um die Überprüfung der Bedingungen für UI-Aktionen in Formularen und Listen zu aktivieren, bevor sie ausgeführt werden. Wenn Sie diese Eigenschaft auf wahrfestlegen, wird den Tabellen-UI-Aktionen eine zusätzliche Validierungsebene hinzugefügt, bevor sie ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.strict.actions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um eine zusätzliche Validierungsebene für die Tabellen-UI-Aktionen sicherzustellen, bevor sie ausgeführt werden.
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Sicherheitsrisikobewertung	3.3

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt nur eine zusätzliche Validierungsebene hinzu, um nach UI-Aktionen in der Zieltabelle/-seite in der Instanz zu suchen. Solange die Zugriffskontrollen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Niedrig) Zugriffsanforderung wird immer überprüft, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang validiert alle UI-Aktionen, bevor das Formular für den Endbenutzer gerendert wird.
Referenzen	Hochsicherheits-Plugin

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Administratorrollen für Event Management-Zuweisungsgruppen konfigurieren [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft *evt_mgmt.connector_assignment_group_admin_roles*, um festzulegen, welche Rollen für den Administratorzugriff über das Zuweisungsgruppenfeld in Connector-Instanzen berechtigt sind.

Die Eigenschaft *evt_mgmt.connector_assignment_group_admin_roles* enthält eine durch Kommas getrennte Zeichenfolge, die die Rollennamen angibt, die Administratorzugriff über das Zuweisungsgruppenfeld in Connector-Instanzen haben. Durch das Ändern der Standardrollen in dieser Liste können nicht autorisierte Benutzer Event-Integrationen in der Instanz ändern. Um den nicht autorisierten Zugriff auf Rollen zu verhindern, legen Sie *evt_mgmt.connector_assignment_group_admin_roles* auf den Wert admin,evt_mgmt_admin,sn_sow_srm.srm_admin fest. Überprüfen Sie alle zusätzlichen Rollen in der empfohlenen Wertzeichenfolge, um sicherzustellen, dass die Rolle enthalten sein sollte.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*evt_mgmt.connector_assignment_group_admin_roles*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	admin, evt_mgmt_admin, sn_sow_srm.srm_admin
Standardwert	admin, evt_mgmt_admin, sn_sow_srm.srm_admin
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3.1 • CVSS-Punktzahl: Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Durch das Ändern der Standardrollen können nicht autorisierte Benutzer Event-Integrationen in der Instanz ändern.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Creating groups

Internen Zugriff auf explizite externe Rollen verweigern [Aktualisiert in Security Center 1.5]

Mehrere Eigenschaften bilden zusammen die Konfiguration für die Härtungseinstellung **„Explizite Rollen aktivieren" für die interne Deny-Liste**. Die Eigenschaft `glide.security.explicit_roles.enable_internal_user_blacklist` verhindert, dass externen Benutzern die Rolle „snc_internal" zugewiesen wird, und ermöglicht die Eigenschaft `glide.security.explicit_roles.internal_user_blacklist`, um die Rolle „snc_external" zuzuweisen.

Glide.security.explicit_roles.enable_internal_user_blacklist

Sie können internen Benutzern und externen Benutzern Zugriff auf Ihre Instanz gewähren. Um die Sicherheit zu erhöhen, muss jeder Benutzer mindestens eine Rolle besitzen, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Legen Sie die Eigenschaft `glide.security.explicit_roles.enable_internal_user_blacklist` auf den empfohlenen Wert **true** fest, um die Zuweisung der Rolle snc_external zu aktivieren.

Legen Sie den Wert auf **false** fest, um die Möglichkeit zum Zuweisen der Rolle snc_external zu deaktivieren. Allen Benutzern wird standardmäßig die Rolle snc_internal zugewiesen

Hinweis:
Instanzen ohne installierte explizite Rollen sind nicht betroffen. Ab dem Paris-Release erhalten Neuinstallationen von expliziten Rollen die Eigenschaft mit dem Standardwert true.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.explicit_roles.enable_internal_user_blackl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Ermöglicht die Zuweisung angegebener Benutzerklassen zur Rolle „snc_external" anstelle der Rolle „snc_internal".
Empfohlener Wert	True (Standard).
Konfigurationstyp	Boolescher Wert.
Sicherheitsrisiko	(Mittel) Das Deaktivieren der Eigenschaft kann zu einer unangemessenen Standardrollenzuweisung führen.
Sicherheitsrisikobewertung	5.4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Explizite Rollen in CSM ,

Glide.security.explicit_roles.internal_user_blacklist

Der Wert `glide.security.explicit_roles.internal_user_blacklist` bestimmt, welchen Benutzerklassen (Tabellen, die sys_user erweitern) die Rolle snc_external anstelle der Rolle snc_internal zugewiesen werden soll. Der Standardwert csm_consumer_user,customer_contact ist so definiert, dass er den Anwendungsfällen in den Plugins „Customer Service Management“ entspricht.

Der Eigenschaftswert muss nur geändert werden, wenn zusätzliche oder andere Benutzerklassen vorhanden sind, denen standardmäßig die Rolle snc_external anstelle der Rolle snc_internal zugewiesen werden muss. Wenden Sie sich an den Support, um diese Werte zu ändern.

Attribut	Beschreibung
Eigenschaftsname	`glide.security.explicit_roles.internal_user_blacklist`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Ermöglicht die Zuweisung von zugewiesenen Benutzern standardmäßig die Rolle „snc_external“ anstelle der Rolle „snc_internal“.
Empfohlener Wert	`csm_consumer_user`, `customer_contact`
Konfigurationstyp	Zeichenfolge
Funktionale Auswirkung	
Sicherheitsrisiko	(Mittel) Das Deaktivieren der Eigenschaft kann zu einer unangemessenen Standardrollenzuweisung führen.
Sicherheitsrisikobewertung	5.4
Referenzen	Explizite Rollen, Zuweisungen externer Benutzerrollen korrigieren

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Verhindern, dass sich inaktive Benutzer anmelden [Neu in Security Center 1.5]

Konfigurieren Sie diese Eigenschaft, um zu steuern, ob sich inaktive Benutzer bei Ihrer Instanz authentifizieren können.

Wenn die Einstellung `glide.authenticate.only.allow.active.user.login` nicht auf den empfohlenen Wert true festgelegt ist, können sich Benutzer in der Tabelle sys_user, die als inaktiv markiert sind, weiterhin bei der Instanz anmelden. Benutzer können als inaktiv markiert werden, wenn sie nicht mehr zur Anmeldung berechtigt sind, z. B. wenn ihnen ein Unternehmen gekündigt wird. Wenn die Einstellung auf „falsch“ konfiguriert ist, können Benutzer weiterhin auf die Instanz und die Daten zugreifen, auf die sie zuvor Zugriff hatten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.only.allow.active.user.login`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, können inaktive Benutzer wie ein gekündigter Mitarbeiter weiterhin auf die Instanz und alle Daten zugreifen.
Abhängigkeiten und Voraussetzungen	Keine

Verweigern Sie den nicht autorisierten Zugriff auf Anforderungselemente

Die Eigenschaft `glide.sc.req_for.roles.default` definiert ein Standardverhalten für die `abrufenAddress` -API.

Diese Eigenschaft funktioniert nur, wenn `glide.sc.req_for.roles` keine Werte hat. Wenn `glide.sc.req_for.roles` Werte aufweist, hat diese Eigenschaft keine Bedeutung, und Benutzer mit nur definierten Rollen erhalten Zugriff auf die API.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sc.req_for.roles.default`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Wenn in der Eigenschaft keine Rollen angegeben sind, kann die vom Client aufrufbare `Skripteinbindung ScriptServiceCatalogGetLocation` von jedem nicht privilegierten angemeldeten Benutzer aufgerufen werden und die Adresse anderer Benutzer im System abrufen. Diese Eigenschaft schützt diese API vor unprivilegierten Benutzern.
Empfohlener Wert	verweigern
Standardwert	verweigern
Konfigurationstyp	Auswahlliste (allow | deny)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsrisiko	(Mittel) Wenn `glide.sc.req_for.roles.default` nicht auf den empfohlenen Wert von „ **verweigern** “ (allow) festgelegt ist und der Wert von `glide.sc.req_for.roles` leer ist, kann jeder Benutzer Elemente für andere Benutzer anfordern, die nicht autorisierten Ressourcenzugriff zulassen.
Referenzen	Vom Client aufrufbare Skripteinbindungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Anti-CSRF-Token aktivieren [In Security Center 1.5 entfernt]

Verwenden Sie die Eigenschaft `glide.security.use_csrf_token`, um sicherzustellen, dass ein sicheres Token zum Identifizieren und Validieren eingehender Anforderungen verwendet wird, die wiederum zur Verhinderung dieser Angriffe verwendet werden.

Cross-Site Request Forgery (CSRF) ist ein Angriff, der einen Endbenutzer dazu zwingt, unerwünschte Aktionen in einer Webanwendung auszuführen, in der er sich derzeit authentifiziert hat. CSRF-Angriffe zielen speziell auf Anforderungen zur Statusänderung ab, nicht auf den Diebstahl von Daten, da der Angreifer die Antwort auf die gefälschte Anforderung nicht sehen kann.

Die folgenden Eigenschaften können für hinzugefügte Steuerungen für das CSRF-Token aktiviert werden:

- `glide.security.csrf_previous.time_limit`
- `glide.security.csrf_previous.allow`
- `glide.security.csrf.strict.validation.mode`

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.use_csrf_token`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Zum Schutz der Anwendung vor potenziellen CSRF-Angriffen.
Sicherheitsrisikobewertung	8.1
Empfohlener Wert	Wahr
Standardwert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzbenutzer eine Schreibanforderung an die Instanz sendet. Jede Schreibanforderung enthält ein CSRF-Token (d. h. eine Validierungs-/CSRF-ID, die an die Benutzersitzung gebunden ist). Wenn die Benutzersitzung abläuft, läuft auch das sichere Token ab.
Sicherheitsrisiko	(Hoch) Cross Site Request Forgery stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff starten, indem er das Vertrauen eines Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung in der Instanz übermitteln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sicherstellen, dass ACLs für Archivtabellen aktiviert sind [Neu in Security Center 1.3]

Die Eigenschaft `glide.security.enable_archive_table_acls` steuert, ob Zugriffskontrolllisten (ACLs) der ursprünglichen Tabelle, der Tabelle, aus der die Archivtabelle erstellt wurde, als „false“ ausgewertet werden.

Die Eigenschaft `glide.security.enable_archive_table_acls` sollte nicht auf „false“ festgelegt werden, da die ACLs der ursprünglichen Tabelle unabhängig von ihrem Wert ausgewertet werden. Sie können zusätzliche ACLs für eine Archivtabelle vermeiden, indem Sie sie nicht hinzufügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.enable_archive_table_acls`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „falsch“ festgelegt ist, werden zu archivierten Tabellen hinzugefügte ACLs ignoriert. Dies ist eine Aktion, die kontraintuitiv ist und daher zu einer Autorisierungsumgehung führen kann.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden alle aktiven Lese-ACLs in Archivtabellen berücksichtigt. Wenn keine aktiven Lese-ACLs vorhanden sind oder die Eigenschaft auf „falsch“ festgelegt ist, wird die ursprüngliche Tabelle (Tabelle, aus der Daten archiviert wurden) auf die Archivtabelle angewendet. **Hinweis:** In Archivtabellen werden nur Lese-ACLs unterstützt. Andere Vorgänge in Archivtabellen werden intern durch einen Zugriffs-Handler gesteuert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin für kontextbezogene Sicherheit aktivieren [Aktualisiert in Security Center 1.3]

Aktivieren Sie das Plugin „Contextual Security Plugin“ (*com.glide.role_management*), um die kontextbezogene Sicherheit zu aktivieren, die einen Datensatz/Informationen mithilfe der Funktionen zum Erstellen, Lesen, Schreiben und Löschen sichert.

Nach der Installation und Aktivierung werden die Wörterbuchrollen (erstellt von Simple Security Manager) nicht mehr getestet. Stattdessen sucht Now Platform nach ACL-Regeln für Felder und Tabellen. Sie sichert die Daten mithilfe von ACL-Regeln anstelle herkömmlicher, rollenbasierter Dictionary-Regeln, die von einem einfachen Sicherheitsmanager implementiert werden. Auch wenn Sie das Wörterbuchformular konfigurieren und einem Wörterbucheintrag Rollen hinzufügen, werden die Rechte nicht geändert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	*com.glide.role_management*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Im Gegensatz zum einfachen Sicherheitsmanager kennt der kontextbezogene Sicherheitsmanager die Systemtabellenhierarchie. Sie können möglicherweise unterschiedliche Sicherheitsregeln für ein Feld haben, je nachdem, wo es in der Hierarchie angezeigt wird.
Empfohlener Wert	Aktiv (Plugin standardmäßig aktiviert)
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Funktionsebene der Zugriffskontrollen, wodurch die Anwendung die Zugriffsbeschränkungen nur basierend auf der ACL-Tabelle bestimmen kann.
Sicherheitsrisiko	(Hoch) Zugriffskontrollen auf funktionaler Ebene müssen vor der Ausführung von CRUD-Vorgängen serverseitig erzwungen werden, um die entsprechende Zugriffsebene für Instanzbenutzer sicherzustellen.
Referenzen	Contextual Security Manager

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin .

Aktivieren der AJAXGlideRecord-ACL-Überprüfung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.script.secure.ajaxgliderecord*, um eine Validierung der Zugriffskontrollregel (ACL) durchzuführen, wenn auf serverseitige Datensätze, z. B. Tabellen, mit GlideAjax-APIs in einem Client-Skript zugegriffen wird.

Von Client-Skripts ist es möglich, beliebige Daten vom Server abzufragen, indem AJAXGlideRecord () verwendet wird.GlideAjax Client)-API, indem Sie eine Syntax wie einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

serverseitigen Glide-Datensatz verwenden. Es ist ein leistungsstarkes und nützliches Tool in vielen Bereitstellungen.

Wenn Sie Zugriffskontrolllisten (ACLs) auf Aufrufe der GlideAjax-API anwenden, können Sie nur Daten abfragen, auf die der aktuell verbundene Benutzer Zugriff hat. Wenn beispielsweise ein ESS-Benutzer angemeldet ist, der keine Rechte zum Lesen der Tabelle „cmn_location“ hat, schlägt ein Aufruf der GlideAjax-API für diese Tabelle fehl.

Wenn Now Platform ohne Überprüfung des Aufrufs der GlideAjax-ACL ausgeführt wird, kann eine API Informationen zurückgeben, auf die der aktuell angemeldete Benutzer andernfalls nicht zugreifen könnte.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.secure.ajaxgliderecord
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Stellt sicher, dass Sicherheits-ACLs auch dann überprüft und validiert werden, wenn auf die Datensätze über clientseitige APIs zugegriffen wird.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die ACL-Beziehung zu serverseitigen Datensätzen, wenn die Anforderungen mithilfe der AJAXGlideRecord-API-Aufrufe gestellt werden. Wenn die ACL-Konfiguration nicht ordnungsgemäß konfiguriert ist, kann dies Auswirkungen haben. Weitere Informationen zu ihren Auswirkungen und ihrer Identifizierung finden Sie im Artikel Audit and review client-side GlideRecord (AJAXGlideRecord)Transaktionen [KB0550828] im HI Knowledge Base .
Sicherheitsrisiko	(Hoch) Über Client-Skripts ist es möglich, beliebige Daten vom Server über die GlideAjax-API abzufragen. Auf serverseitige Ressourcen kann ohne entsprechende Autorisierung zugegriffen werden. Daher hilft die Verwendung der ACL-Validierung der Anwendung, die Anforderung basierend auf der konfigurierten Autorisierung zu validieren.
Workaround	Stellen Sie sicher, dass die richtigen ACLs für Skripteinbindungen, Prozessoren und andere Entitäten erstellt werden, die von einer GlideAjax-API (AJAXGlideRecord) verwendet werden, damit sie mit der richtigen Autorisierung ausgeführt wird. Implementieren Sie Methoden wie `canRead ()`, `canWrite ()`, `canCreate ()`und `canDelete ()`, um eine Benutzerautorisierung durchzuführen, bevor Sie mit GlideRecord auf Tabellendatensätze zugreifen. Eine andere Methode ist die Verwendung von GlideRecordSecure. Die Klasse wird vom

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	GlideRecord-Server geerbt, der dieselben Funktionen wie GlideRecord ausführt und auch ACLs erzwingt.
Referenzen	ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz) Diese Eigenschaft gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • `glide.script.use.sandbox`: Siehe vom Client generierte Skripts in der Sandbox. • `glide.script.allow.ajaxevaluate`: Siehe AJAXEvaluate aktivieren.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Strikte Validierung des CSRF-Tokens erzwingen [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft `glide.security.csrf.strict.validation.mode`, um die strikte Validierung des CSRF-Tokens zu aktivieren. Wenn das CSRF-Token nicht übereinstimmt, wird die erneute Übermittlung der Anforderung verhindert.

Die Eigenschaft `glide.security.csrf.strict.validation.mode` aktiviert die strikte Validierung des CSRF-Tokens, die die Wiederverwendung von CSRF-Token verhindert. Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt ist, können CSRF-Token wiederverwendet werden, was CSRF-Angriffen Tür und Tor öffnet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.csrf.strict.validation.mode`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Erzwingt die strikte Validierung des CSRF-Tokens und verhindert dessen Wiederverwendung.
Empfohlener Wert	Wahr
Standardwert	Wahr
Sicherheitsrisikobewertung	(Mittel) Cross Site Request Forgery stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzbenutzer starten, indem er das Vertrauen des Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine falsch formatierte Anforderung an die Instanz senden.
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzbenutzer eine Schreibanforderung an die Instanz sendet. Es wird überprüft, ob

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	das aktuelle CSRF-Token zuvor verwendet wurde. Wenn Ja, wird die Übermittlung weiterer Schreibanforderungen verhindert.
Sicherheitsrisiko	(Mittel) Cross Site Request Forgery stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzbenutzer starten, indem er das Vertrauen des Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine falsch formatierte Anforderung an die Instanz senden.

Kehren Sie zu Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch zurück, um Ihren umschlossenen Schlüssel hochzuladen.

Lesezugriff für delegierte Entwickler beschränken [Aktualisiert in Security Center 1.3]

Wenn *com.glide.dd_allow_global_access_tables* nicht den empfohlenen Wert von wf_aktivität, wf_aktivität_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget und sp_page enthält, können diese Tabellen von einem delegierten Entwickler gelesen werden. Dies könnte dem delegierten Entwickler Lesezugriff auf vertrauliche Informationen gewähren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.dd_allow_global_access_tables*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	wf_aktivität, wf_aktivität_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Standardwert	wf_aktivität, wf_aktivität_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Stellen Sie sicher, dass *com.glide.dd_allow_global_access_tables* auf wf_aktivität, wf_aktivität_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page festgelegt ist.

Deaktivieren Sie eingehende E-Mails für ausgesperrte Benutzer

Verwenden Sie die Eigenschaft *glide.pop3.process_locked_out*, um Aktionen bei eingehender E-Mail für ausgesperrte, aktive Benutzer zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie diese Eigenschaft auf „ **false** “ fest, um eingehende E-Mails für ausgesperrte Benutzer zu deaktivieren.

Hinweis:
Berücksichtigen Sie die Sicherheitsauswirkungen, wenn Benutzer aus nicht vertrauenswürdigen Domänen zugelassen werden, und warum sie ausgesperrt wurden, bevor E-Mails von ihnen Aktionen für eingehende E-Mails auslösen können.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.pop3.process_locked_out`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Diese Eigenschaft steuert Aktionen bei eingehender E-Mail für ausgesperrte Benutzer.
Empfohlener Wert	false
Standardwert	false
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft auf „ **true**“ festlegen, kann es zu einer Offenlegung von Informationen kommen, da eingehende E-Mails von Benutzern mit gesperrten Accounts empfangen werden.
Sicherheitsrisikobewertung	7.5

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Überprüfen Sie eingehende Transaktionen noch einmal

Verwenden Sie die Eigenschaft `glide.security.strict.updates`, um die doppelte Überprüfung der Sicherheit bei eingehenden Transaktionen während der Formularübermittlung zu ermöglichen. Wenn Sie diese Eigenschaft auf **true**setzen, wird eine zusätzliche Ebene der Tabellenvalidierung hinzugefügt, bevor ein Formular im Browser gerendert wird.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.security.strict.updates`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um eine zusätzliche Überprüfungsebene der Benutzerberechtigungen sicherzustellen, bevor das Formular im Browser angezeigt wird.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur fügt eine zusätzliche Validierungsebene hinzu, um nach Benutzerberechtigungen für die Zieltabelle/-seite in der Instanz zu suchen. Solange die Zugriffskontrollen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Hoch) Sie sollten die Zugriffsanforderung immer überprüfen, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang prüft auf Berechtigungen, wenn das Formular angefordert wird und bevor das Formular gerendert wird.
Referenzen	Eigenschaften der Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktivieren Sie ACLs, um Live-Profildetails zu steuern

Verwenden Sie die Eigenschaft `glide.live_profile.details`, um anzugeben, ob ein Benutzer in der Lage sein soll, alle Detailfelder wie Firmenname und Telefonnummern in einem Live-Profil anzuzeigen.

Abhängig von der Einstellung der Eigenschaft `glide.live_profile.details` geschieht Folgendes:

- Wenn der Wert auf Anzeigen festgelegt ist, wird der Zugriff auf die Live-Profilinformationen unabhängig von den für das Benutzerprofil erstellten ACLs gewährt.
- Wenn der Wert auf ACL festgelegt ist, ist der Zugriff auf die Live-Profilinformationen gemäß den für das Benutzerprofil erstellten ACLs eingeschränkt.
- Wenn der Wert auf Ausblenden festgelegt ist, ist der Zugriff auf die Live-Profilinformationen unabhängig von den für das Benutzerprofil erstellten ACLs eingeschränkt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.live_profile.details`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Der Zweck besteht darin, nur autorisierten Benutzern den Zugriff auf die Details eines Live-Profils (z. B. Firmenname, Telefonnummern) zu ermöglichen.
Empfohlener Wert	Sys-Sicherheits-ACL
Sicherheitsrisikobewertung	4.3

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Benutzer auf die Live-Profildetails aller anderen Benutzer zugreifen.
Sicherheitsrisiko	(Mittel) API-Anforderungen sollten Tabellen-ACLs immer berücksichtigen. Die Einschränkung muss angewendet werden, um zu verhindern, dass nicht autorisierte Benutzer auf Details eines Live-Profils zugreifen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktivieren Sie ACLs für die Berichtsansicht

Verwalten Sie eine Prüfung für report_view-ACLs veröffentlichter Berichte.

Verwenden Sie die Eigenschaft the `glide.report.report_view.check_published`, um eine Prüfung von report_view-ACLs für veröffentlichte Berichte zu verwalten. Wenn die Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, wird die Überprüfung von report_view-ACLs auf veröffentlichte Berichte deaktiviert.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.report.report_view.check_published`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: Hoch • CVSS-Punktzahl: 7,5 • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „ **true**“ festgelegt ist, ist die Überprüfung von report_view-ACLs auf veröffentlichte Berichte deaktiviert.
Abhängigkeiten und Voraussetzungen	Keine

Aktivieren Sie die URL-Allow-Liste für die ursprungsübergreifende IFrame-Kommunikation

Verwenden Sie die Eigenschaft `glide.ui.concourse.onmessage_enforce_same_origin`, um die ursprungsübergreifende Kommunikation zwischen iframeszu ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OpenFrame kann nur Nachrichten aus vertrauenswürdigen Domänen verarbeiten, die in der Eigenschaft `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` angegeben sind. Weitere Informationen finden Sie unter UTL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation angeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.concourse.onmessage_enforce_same_origin`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Zum Aktivieren der Aufnahmeliste von vertrauenswürdigen Domänen, damit sie zwischen IFrames für OpenFrame kommunizieren können.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	4.2
Funktionale Auswirkung	(Mittel) Wenn Sie beabsichtigte Domänen nicht in die Aufnahmeliste aufnehmen, kann die Möglichkeit zum Einbetten anderer Seiten in Now Platform Instanzen eingeschränkt sein.
Sicherheitsrisiko	(Hoch) Wenn eine Webseite Event-Handler enthält, die keine ordnungsgemäße Ursprungsvalidierung durchführen, kann eine Webseite oder ein Skript von einem beliebigen Ursprung mit ihr kommunizieren. Sie kann auch alle vom Event Handler ausgeführten Funktionen initiieren.
Referenzen	OpenFrame-Übersicht

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Authentifizierung für rollenlose ACL erzwingen

Verwenden Sie die Eigenschaft `glide.security.enforce_auth_roleless_acl`, um sicherzustellen, dass nur authentifizierte Benutzer Prüfungen auf leere ACLs bestehen.

Wenn die Eigenschaft `glide.security.enforce_auth_roleless_acl` nicht auf „true“ festgelegt ist, gewährt GlideRecordSecure nicht authentifizierten Benutzern Zugriff, wenn in einer zugrunde liegenden Zugriffssteuerungsliste (ACL), die Daten schützt, eine Rolle oder Bedingungen fehlen.

ACLs werden häufig von Entwicklern leer gelassen, um allen authentifizierten Benutzern in einer Instanz Zugriff zu gewähren. Das bedeutet, dass jeder Benutzer eine Prüfung für eine leere ACL besteht. Diese Eigenschaft stellt sicher, dass nur authentifizierte Benutzer Prüfungen auf leere ACLs bestehen. Die öffentliche Rolle muss explizit verwendet werden, um nicht authentifizierten Benutzern Zugriff zu gewähren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.enforce_auth_roleless_acl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „true“ festgelegt ist, besteht die Möglichkeit eines nicht authentifizierten Datenverlusts, der sich auf die Vertraulichkeit auswirkt.
Abhängigkeiten und Voraussetzungen	Keine

Einschränkungen des Anwendungsbereichs erzwingen [In Security Center 1.5 entfernt]

Verwenden Sie die Eigenschaft `glide.record.legacy_cross_scope_access_policy_in_script`, um die Berechtigungen von bereichsbezogenen Apps zu steuern.

Wenn die Eigenschaft `glide.record.legacy_cross_scope_access_policy_in_script` auf „true“ festgelegt ist, können bereichsbezogene Apps APIs aufrufen, die nur für globale Apps verfügbar sein sollten. Diese Eigenschaft umgeht die beabsichtigten Zugriffskontrollen zum Erstellen und Aktualisieren von Entwicklern für diese bereichsbezogenen Apps.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.record.legacy_cross_scope_access_policy_in_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt ist, können bereichsbezogene Apps und delegierte Entwickler für diese bereichsbezogenen Apps Datensätze in globalen Tabellen wie „Incident“ erstellen und aktualisieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Sicherheitsregeln für die Freigabe von Dashboards erzwingen – Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.cms.dashboards.sharing_with_secure_search`, um zu steuern, ob Benutzer Dashboards freigeben können.

Wenn die Eigenschaft `glide.cms.dashboards.sharing_with_secure_search` nicht auf **true**festgelegt ist, können Benutzer Dashboard-Gruppen und -Rollen freigeben, auf die sie keinen Zugriff haben. Durch Aktivieren dieser Eigenschaft werden Zugriffssteuerungslisten (ACLs) beim Durchsuchen der Tabellen „sys_user“, „sys_user_role“ und „sys_user_group“ während des Dashboard-Freigabeprozesses erzwungen. Die übermäßige Freigabe eines Dashboards kann dazu führen, dass Benutzer, Gruppen oder Rollen auf Daten zugreifen, für die sie keine Anzeigeberechtigung haben sollten, wodurch vertrauliche Informationen möglicherweise gefährdet werden. Daher wird empfohlen, `glide.cms.dashboards.sharing_with_secure_search` auf „true“ zu setzen, damit Dashboards nur für diejenigen freigegeben werden, die über die entsprechenden Berechtigungen verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.cms.dashboards.sharing_with_secure_search`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt wird, werden Zugriffssteuerungslisten beim Durchsuchen der Tabellen „sys_user“, „sys_user_role“ und „sys_user_group“ nicht erzwungen. Dies kann dazu führen, dass Dashboards für nicht autorisierte Benutzer freigegeben werden und vertrauliche Informationen verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Access control
Funktionale Auswirkung	Diese Eigenschaft wendet Sicherheitsregeln auf die Liste der Benutzer, Benutzergruppen und Rollen an, die beim Freigeben von Dashboards sichtbar sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereichssicherheit für digitale Services des öffentlichen Sektors erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.enforce_security_scope.sn_gsm*, um zu steuern, wie auf die Anwendungsdaten aus der Anwendung „Public Sector Digital Services“ zugegriffen wird.

Mit der Anwendung ServiceNow Public Sector Digital Services können Sie Anwendungen für den öffentlichen Sektor entwickeln, die digitale Services für Bürger, Unternehmen und Behörden bereitstellen.

Wenn *glide.enforce_security_scope.sn_gsm* auf „falsch“ festgelegt ist, kann der Zugriff auf die Anwendungsdaten in den globalen Tabellen der App „Public Sector Digital Services“ basierend auf den Zugriffssteuerungslisten (ACLs) dieser globalen Tabellen zugänglich sein. Wenn diese Eigenschaft auf „true“ festgelegt ist, wird der Zugriff auf Daten in globalen Tabellen nur basierend auf den ACLs ausgewertet, die direkt in der App „Public Sector Digital Services“ enthalten sind. Das Festlegen dieser Eigenschaft auf „falsch“ kann zur Offenlegung von Informationen aus zu weitreichenden ACLs führen.

Um dieses Sicherheitsrisiko zu beheben, legen Sie *glide.enforce_security_scope.sn_gsm* auf „true“ fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.sn_gsm*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt wird, kann dies zur Offenlegung von Informationen durch zu weitreichende ACLs führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	

Bereichsbezogenen ACL-Zugriff für Informationsanforderungs-Playbooks erzwingen – Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.enforce_security_scope.sn_gsm_info_req*, um den Zugriff auf Playbook-Daten für die Playbook-Funktion „Informationsanforderung“ zu steuern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit der Anwendung Information Request Playbook können Endbenutzer des öffentlichen Sektors Anforderungen für öffentliche Datensätze übermitteln und nachverfolgen und Behördenmitarbeitern einen vordefinierten Prozess für die Bearbeitung und Lösung dieser Anforderungen bereitstellen. Wenn `glide.enforce_security_scope.sn_gsm_info_req` nicht auf „wahr“ festgelegt ist, kann unerwarteter Zugriff auf Playbook-Daten für die Playbook-Anwendung „Information Request“ gewährt werden. Legen Sie diese Eigenschaft auf „true“ fest, um beim Gewähren des Zugriffs nur ACLs aus dem Bereich sn_gsm_info_req zu berücksichtigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_gsm_info_req`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „falsch“ festgelegt ist, werden ACLs aus allen Bereichen berücksichtigt, wenn Zugriff auf Playbook-Daten in der Bereichshaupttabelle gewährt wird. Dadurch würden Playbook-Daten für Informationsanforderungen verfügbar gemacht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• Using Information Request Playbook • Configure Information Requests service channel

Strikte Erhöhungsberechtigung erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.security.strict_elevate_privilege`, um zu steuern, ob als privilegiert markierte Rollen manuell erhöht werden müssen, damit dem Benutzer die Fähigkeiten der Rolle gewährt werden.

Legen Sie diese Eigenschaft auf „true“ fest, um eine zusätzliche Ebene der Sicherheitsvalidierung hinzuzufügen, wenn ein privilegierter Benutzer seine Rolle erweitert.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.strict_elevate_privilege`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,7 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn *glide.security.strict_elevate_privilege* auf „false“ festgelegt ist, werden Rollen, die als privilegiert markiert sind, bei einer neuen Sitzung des Administratorbenutzers automatisch erhöht und müssen nicht manuell erhöht werden (mit Ausnahme von security_admin).
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft erfordert unbedingt, dass Benutzer mit Administratorrolle die Berechtigungen bei Bedarf erhöhen.

AJAXGlideRecord-ACL-Überprüfung anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.script.secure.ajaxgliderecord*, um eine Validierung der Zugriffskontrollregel (ACL) durchzuführen, wenn auf serverseitige Datensätze, z. B. Tabellen, mit GlideAjax-APIs in einem Client-Skript zugegriffen wird.

Von Client-Skripts ist es möglich, beliebige Daten vom Server abzufragen, indem AJAXGlideRecord () verwendet wird.GlideAjax Client)-API, indem Sie eine Syntax wie einen serverseitigen Glide-Datensatz verwenden. Es ist ein leistungsstarkes und nützliches Tool in vielen Bereitstellungen.

Wenn Sie Zugriffskontrolllisten (ACLs) auf Aufrufe der GlideAjax-API anwenden, können Sie nur Daten abfragen, auf die der aktuell verbundene Benutzer Zugriff hat. Wenn beispielsweise ein ESS-Benutzer angemeldet ist, der keine Rechte zum Lesen der Tabelle „cmn_location“ hat, schlägt ein Aufruf der GlideAjax-API für diese Tabelle fehl.

Wenn Now Platform ohne Überprüfung des Aufrufs der GlideAjax-ACL ausgeführt wird, kann eine API Informationen zurückgeben, auf die der aktuell angemeldete Benutzer andernfalls nicht zugreifen könnte.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.script.secure.ajaxgliderecord*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Stellt sicher, dass Sicherheits-ACLs auch dann überprüft und validiert werden, wenn auf die Datensätze über clientseitige APIs zugegriffen wird.
Empfohlener Wert	Wahr
Standardwert	Wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die ACL-Beziehung zu serverseitigen Datensätzen, wenn die Anforderungen mithilfe der AJAXGlideRecord-API-Aufrufe gestellt werden. Wenn die ACL-Konfiguration nicht ordnungsgemäß konfiguriert ist, kann dies Auswirkungen haben. Weitere Informationen zu ihren Auswirkungen und ihrer Identifizierung finden Sie im Artikel Audit and review client-side GlideRecord (AJAXGlideRecord)Transaktionen [KB0550828] im HI Knowledge Base .
Sicherheitsrisiko	(Hoch) Über Client-Skripts ist es möglich, beliebige Daten vom Server über die GlideAjax-API abzufragen. Auf serverseitige Ressourcen kann ohne entsprechende Autorisierung zugegriffen werden. Daher hilft die Verwendung der ACL-Validierung der Anwendung, die Anforderung basierend auf der konfigurierten Autorisierung zu validieren.
Workaround	Stellen Sie sicher, dass die richtigen ACLs für Skripteinbindungen, Prozessoren und andere Entitäten erstellt werden, die von einer GlideAjax-API (AJAXGlideRecord) verwendet werden, damit sie mit der richtigen Autorisierung ausgeführt wird. Implementieren Sie Methoden wie `canRead ()`, `canWrite ()`, `canCreate ()`und `canDelete ()`, um eine Benutzerautorisierung durchzuführen, bevor Sie mit GlideRecord auf Tabellendatensätze zugreifen. Eine andere Methode ist die Verwendung von GlideRecordSecure. Die Klasse wird vom GlideRecord-Server geerbt, der dieselben Funktionen wie GlideRecord ausführt und auch ACLs erzwingt.
Referenzen	ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz) Diese Eigenschaft gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *`glide.script.use.sandbox`*: Siehe vom Client generierte Skripts in der Sandbox. • *`glide.script.allow.ajaxevaluate`*: Siehe AJAXEvaluate aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

ACLs auf Feldebene in GlideRecordSandbox erzwingen

Verwalten Sie ACLs auf Feldebene in GlideRecordSandbox in Ihrer Instanz.

Verwenden Sie die Eigenschaft the *glide.sandbox.fields.check_acl* , um ACLs auf Feldebene in GlideRecordSandbox zu erzwingen. Diese Eigenschaft wird beispielsweise angewendet, wenn ein Benutzer ein Skript bereitstellen kann, wie in *sysparm_query*. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können ACL-Beschränkungen umgangen werden, wodurch vertrauliche Daten gefährdet werden können, z. B. *sys_user.user_password* von einem nicht autorisierten Benutzer.

Warnung:
Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sandbox.fields.check_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **falsch** “ festgelegt wird, können ACL-Beschränkungen umgangen werden, die vertrauliche Daten verfügbar machen könnten.
Abhängigkeiten und Voraussetzungen	Keine

Verwendung des Alias für Anmeldeinformationen erzwingen [Aktualisiert in Security Center 1.5]

Erfahren Sie, wie Sie Ihre Anmeldeinformationen vor nicht autorisierter Verwendung schützen, indem Sie die MID Server-Eigenschaft konfigurieren.

Der MID Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon in Ihrem lokalen Netzwerk ausgeführt wird. MID Server-Eigenschaften werden in der Tabelle [ecc_agent_property] aufgelistet. Sie können in Ihrer Instanz darauf zugreifen, indem Sie zu navigieren **MID-Server** > **Eigenschaften**. Mit Aliassen für Anmeldeinformationen kann ein Administrator bestimmte Anmeldeinformationen für Erkennungszeitpläne verwenden. Aliasse für Anmeldeinformationen bieten eine detailliertere Kontrolle darüber, welche Anmeldeinformationen eine Discovery-Tabelle verwenden darf. Um diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsschwachstelle zu beheben, legen Sie *alias_filtering_behavior* auf „strikt“ fest, um eine unnötige Offenlegung von Anmeldeinformationen mit erhöhten Berechtigungen zu verhindern. Unter MID Server properties finden Sie weitere Details.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*alias_filtering_behavior*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	strict
Standardwert	locker
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Härtungseinstellung nicht auf „strikt“ festgelegt ist, werden alle Anmeldeinformationen unabhängig von ihren Aliassen für Discovery-Tabellen verwendet, was die Wahrscheinlichkeit eines nicht autorisierten Zugriffs erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• MID Server • Anmeldeinformationsaliasse für Discovery

GroupBy-ACLs erzwingen

Konfigurieren Sie Ihre Instanz so, dass ACL-Prüfungen für groupby-Spalten durchgeführt werden.

Verwenden Sie diese Eigenschaft, um Ihre Instanz so zu konfigurieren, dass ACL-Prüfungen für groupby-Spalten durchgeführt werden. Wenn diese Eigenschaft auf den empfohlenen Wert **true**festgelegt ist, wird das Attribut *groupby_acl_check* einer Tabelle so festgelegt, dass groupby-ACLs berücksichtigt werden. Wenn die Eigenschaft auf **false**festgelegt ist, findet keine ACL-Prüfung für groupby-Spalten in einer Tabelle statt, was zu Informationsverlusten führen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.groupby_acl_check*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **falsch** “ festgelegt wird, wird die ACL-Prüfung für „groupby“-Spalten deaktiviert, was zu Informationsverlusten führen kann.
Abhängigkeiten und Voraussetzungen	Keine

Sicherstellen, dass das Erstellen/Löschen von Dashboards eine Zugriffsprüfung erfordert [Neu in Security Center 1.3]

Die Eigenschaft `glide.processors.check_access_before_process` ermöglicht die Erzwingung der Zugriffssteuerungsliste (ACL) zum Erstellen oder Löschen von Dashboards, wenn ein Benutzer angemeldet ist. Diese Eigenschaft muss immer auf „true“ festgelegt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.processors.check_access_before_process`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft deaktivieren, indem Sie sie auf „falsch“ setzen, wird eine ACL-Umgehung in Dashboards aktiviert. Dadurch können alle authentifizierten Benutzer mit geringen Berechtigungen Dashboards löschen und hinzufügen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft steuert die Möglichkeit, neue sys_dashboards zu erstellen und vorhandene Dashboards zu löschen, wenn ein Benutzer nicht über die erforderlichen Zugriffsrechte verfügt. Wenn der Wert auf „false“ festgelegt ist, können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Benutzer mit unangemessenen Rollen sys_dashboard-Einträge hinzufügen und löschen (obwohl die GlideRecord-Ebene die vorhandenen ACLs erneut überprüfen sollte). Ein Wert von true schränkt Hinzufügen- und Löschvorgänge für Benutzer ohne die erforderlichen Zugriffsrechte ein.

Validierung des oauth-Statusparameters erzwingen

Konfigurieren Sie die Eigenschaft undund *glide.oauth.state.parameter.required*, um Ihre Instanz vor CSRF-Angriffen (Cross-Site Request Forgery) zu schützen.

Die Eigenschaft *glide.oauth.state.parameter.required* ermöglicht es, dass der Parameter State in einer OAuth-Anforderung für den Autorisierungscode-Flow erforderlich ist. Der State-Parameter ist ein Zeichenfolgenwert, der keine Sonderzeichen enthalten oder leer sein darf. Wenn diese Eigenschaft auf „ **true** “ festgelegt wird, wird sichergestellt, dass ein Angreifer während der Authentifizierung keine CSRF-Angriffe (Cross-Site Request Forgery) ausführen kann, wodurch Ihre Instanz vor Angriffen eines Benutzers geschützt wird, dessen Identität Sie annehmen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.oauth.state.parameter.required*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Legen Sie diese Eigenschaft auf „ **true** “ fest, um sicherzustellen, dass CSRF-Angriffe verhindert werden.
Abhängigkeiten und Voraussetzungen	Keine

Strikten Upload von Anwenderbildern erzwingen

Verwenden Sie die Eigenschaft *glide.security.strict.user_image_upload*, um die Zugriffssteuerung für das Hochladen/Aktualisieren eines Profilbildes zu aktivieren, wenn sie für einen Benutzerdatensatz ausgeführt wird.

Diese Einstellung ermöglicht es einem nicht autorisierten Benutzer, ein Bild in das Profil eines anderen Benutzers hochzuladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie diese Eigenschaft auf **true**festlegen, werden die Tabellen-ACLs beim Hochladen von Fotos erzwungen, sodass nur autorisierte Benutzer ein Bild hochladen können.
- Wenn Sie die Option auf **false**festlegen, werden ACLs beim Hochladen von Bildern in das Feld Foto nicht erzwungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.strict.user_image_upload`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	So beschränken Sie das Hochladen von Benutzerbildern nur auf autorisierte Benutzer.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	3.7
Funktionale Auswirkung	(Niedrig) Keine Auswirkungen auf die Funktionalität, da autorisierte Benutzer weiterhin Bilder in ihr Benutzerprofil hochladen können.
Sicherheitsrisiko	(Niedrig) Wenn Sie diese Eigenschaft auf „ **false**“ festlegen, kann ein authentifizierter Benutzer ein Bild ohne Autorisierung in das Konto eines anderen Benutzers hochladen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

E-Mail-Domänen für die Registrierung externer Benutzer beschränken [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft `sn_ext_usr_reg.allowed_email_domains`, um zulässige externe E-Mail-Domänen aufzulisten.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`sn_ext_usr_reg.allowed_email_domains`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do), Communities Eigenschaften
Kategorie	Zugriffssteuerung
Zweck	Listen Sie E-Mail-Domänen auf, um Benutzer-E-Mails für die Registrierung zuzulassen.
Empfohlener Wert	Als nicht leeren Wert festlegen
Konfigurationstyp	Zeichenfolge
Sicherheitsrisiko	(Hoch) Böswillige Akteure könnten die Registrierung mit E-Mail-Adressen aus unerwünschten Domänen durchführen. Stellen Sie sicher, dass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	`sn_ext_usr_reg.allowed_email_domains` nicht auf einen leeren Wert festgelegt ist.
Sicherheitsrisikobewertung	7.5
Referenzen	Communities

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Benutzerkommentare zu Artikeln ausblenden [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.knowman.show_user_feedback`, um zu steuern, ob Feedbackkommentare sichtbar sind.

Wenn `glide.knowman.show_user_feedback` nicht auf nie festgelegt ist, sind Feedback-Kommentare in Knowledge Base-Artikeln für Benutzer mit Rollen sichtbar, die in der Glide-Eigenschaft `glide.knowman.show_user_feedback.roles`definiert sind. Da Feedback-Kommentare vertrauliche Informationen enthalten können, möchten Sie möglicherweise nicht, dass das Feedback sichtbar ist. Wenn diese Eigenschaft nicht auf „nie“ festgelegt ist, kann dies Auswirkungen auf die Vertraulichkeit haben, wenn vertrauliche Informationen im Feedback offengelegt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.knowman.show_user_feedback`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Auswahlliste
Empfohlener Wert	nie
Standardwert	onload
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „nie“ festgelegt wird, kann dies dazu führen, dass vertrauliche Informationen in Feedback-Kommentaren offengelegt werden.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Zeigt Benutzerkommentare zu KB-Artikeln basierend auf den in der Konfiguration genannten Auswahlmöglichkeiten an.

Hochsicherheits-Plugin [Aktualisiert in Security Center 1.3]

Wenn Sie das Plugin „High Security“ aktivieren, werden Hunderte verschiedener Konfigurationen erstellt oder aktualisiert, um die Sicherheitsstufe in Ihrer Instanz zu steuern. Diese Konfigurationen entschärfen viele der häufigsten OWASP-Angriffe, indem sie eine strikte Zugriffskontrolle, Eingabevalidierung und Ausgabecodierung ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Konfigurationen umfassen:

- Zugriffssteuerung
- Business-Regeln
- Systemeigenschaften
- UI-Richtlinienaktion
- Skriptaktionen
- Skripteinbindungen

Beispiel

Sehen Sie sich die Beispiele für die folgenden Eigenschaften an:

Eigenschaft	Thema
glide.ui.escape_all_script	Escape Jelly
glide.security.strict.actions	Überprüfen Sie die UI-Aktion vor der Ausführung
glide.security.csrf_ previous.allow	Anti-CSRF-Token
glide.security.csrf.strict.validation.mode	Strenge CSRF-Validierung

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.high_security
Konfigurationstyp	Systemdefinition > Plugins – Entwicklung
Kategorie	Zugriffssteuerung
Zweck	Dieses Plugin muss aktiviert sein. Sie erhöht die Sicherheitsstufe einer Instanz, wodurch die Angriffsfläche reduziert wird, indem die 10 wichtigsten OWASP-Angriffe wie CSRF, XSS, Cookies für Sicherheitssitzungen und Datei-Uploads abgeschwächt werden.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	(Hoch) Dieses Plugin aktiviert mehrere Systemsicherheitskonfigurationen, die sich auch auf die Benutzeroberfläche und Funktionalität auswirken können.
Sicherheitsrisiko	(Hoch) Viele Sicherheitskonfigurationen werden unbeabsichtigt offen gelassen, was die Tür für einige der kritischen Schwachstellen öffnen kann.
Referenzen	Strenge Sicherheitseinstellungen werden aktiviert Strenge Sicherheitseinstellungen

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACLs mit Admin-Aufhebung berücksichtigen

Die Eigenschaft *glide.security.admin.override.accessterm* steuert, dass Administratoren die ACL-Auswertung nicht überschreiben können, auch wenn die Überschreibung wirksam sein sollte.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.admin.override.accessterm*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Steuert, dass Administratoren die ACL-Auswertung nicht überschreiben können.
Empfohlener Wert	True (Standard)
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) ACLs werden kumulativ ausgewertet. Wenn in einem bestimmten Feld eine Anzahl von ACLs vorhanden ist und die Option „Administratorüberschreibungen“ für eines von ihnen „falsch“ (nicht ausgewählt) ist, werden die effektiven Administratorüberschreibungen für alle ACLs als „falsch“ betrachtet.
Sicherheitsrisikobewertung	3.8
Referenzen	Zugriffskontrolllistenregeln

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Beschränken Sie JSONP-Anforderungen auf vertrauenswürdige URLs

Geben Sie vertrauenswürdige URLs für den Service AngularJS $http an, um JSONP-Anforderungen zuzulassen oder abzulehnen.

Die Eigenschaft *angular.jsonp.inclusion_list.enabled* gibt vertrauenswürdige URLs für den ServiceangularJS $http an, um JSONP-Anforderungen zuzulassen und/oder abzulehnen. Diese Eigenschaft ist erforderlich, da dies einen potenziell grundlegenden Change für Kunden darstellt, sodass sie eine Möglichkeit benötigen, ihre vertrauenswürdigen URLs hinzuzufügen. Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt ist, sind JSONP-Anforderungen an jede URL zulässig.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*angular.jsonp.inclusion_list.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: Mittel • CVSS-Punktzahl: 5,4 • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **false** “ festgelegt wird, werden JSONP-Anforderungen an eine beliebige URL gesendet.
Abhängigkeiten und Voraussetzungen	Keine

Deaktiviert die Ausführung der Rohdatenbankabfrage

Steuern Sie, ob ein Benutzer SQL-Rohabfragen in der Datenbank ausführen kann.

Mit der Eigenschaftund `glide.db.allow_unsafe_dbi_execute_sql` können Benutzer SQL-Rohabfragen in der Datenbank ausführen, die Zugriff auf Tabellen und Daten außerhalb der GlideRecord-Einschränkungen gewähren. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von `false`festgelegt ist, ermöglicht dies den Aufruf von `dbi.executeStatement()` aus einem skriptfähigen Glide-Element, was zur Ausführung schädlicher SQL-Anweisungen führen kann.

⚠ Warnung:
Diese Eigenschaft ist sowohl sicher als auch ohne DB-Überschreibung.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.db.allow_unsafe_dbi_execute_sql`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,2 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „ **falsch** “ festgelegt wird, wird `dbi.executeStatement()` aus einem skriptfähigen Glide-Element aufgerufen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Zugriffskontrolllistenregeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gastbenutzer für SOAP-Anforderungen festlegen [Aktualisiert in Security Center 1.3]

Konfigurieren Sie diese Eigenschaft, um die Zugriffsebene nicht authentifizierter SOAP-Anforderungen zu steuern.

Diese Eigenschaft steuert die Zugriffsebene nicht authentifizierter SOAP-Anforderungen. Wenn er nicht auf den empfohlenen Wert von *soap.guest*festgelegt ist oder auf einen Benutzer mit eingeschränkten Berechtigungen festgelegt ist, werden SOAP-Anforderungen im Namen des Benutzers ausgeführt. Wenn diese Eigenschaft leer ist, wird nicht authentifizierter Zugriff auf Vorgänge auf Administrator- oder Wartungsebene ermöglicht, wodurch alle Sicherheitskontrollen innerhalb der Instanz aufgehoben werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.soap.guest_user*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	seif.gast
Standardwert	seif.gast
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „leer“ setzen, wird nicht authentifizierter Zugriff auf Vorgänge auf Administrator- oder Wartungsebene ermöglicht.
Abhängigkeiten und Voraussetzungen	Keine

Standardauthentifizierung für vom Client aufrufbare Skripteinbindungen erfordern [Aktualisiert in Security Center 1.3]

Standardmäßig sind vom Client aufrufbare Skripteinbindungen, die die Sichtbarkeit nicht explizit festlegen, öffentlich. Fügen Sie bei Bedarf die Eigenschaft *glide.script.ccsi.ispublic* hinzu, um die Datenschutzsteuerung für alle vom Client aufrufbaren Skripteinbindungen zu aktivieren, auf die von öffentlichen Seiten zugegriffen wird.

Wenn Sie diese Eigenschaft hinzufügen, müssen Sie ihren Wert auf **false**festlegen, was angibt, dass alle vom Client aufrufbaren Skripteinbindungen privat sind, und ihre Sichtbarkeit auf öffentlichen Seiten ändert.

Hinweis:
Sie können die Eigenschaft nicht mit dem Wert **true**hinzufügen oder ihren Wert von **false** in **true**ändern. Wenn Sie dies versuchen, wird eine Fehlermeldung angezeigt.

Bei Bedarf können Sie die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion isPublic() hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Einstellung `isPublic()` hat Vorrang vor der Eigenschaft *`glide.script.ccsi.ispublic`*.
- Wenn Sie beispielsweise `isPublic()` in einem einzelnen Skript auf „ **true** “ festlegen, wird es öffentlich gemacht, wodurch die Eigenschaft *`glide.script.ccsi.ispublic`* überschrieben wird, die alle anderen vom Client aufrufbaren Skripteinbindungen privat macht.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*`glide.script.ccsi.ispublic`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Wenn Sie vom Client aufrufbare Skripteinbindungen privat machen, können Gäste, die auf öffentliche Seiten zugreifen, nicht auf die vom Client aufrufbaren Skripteinbindungen zugreifen. Ein nicht angemeldeter Benutzer kann kein privates Skript ausführen.
Empfohlener Wert	false
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Hoch) Wenn die vom Client aufrufbaren Skripteinbindungen als öffentlich gekennzeichnet sind (d. h. diese Eigenschaft fehlt), können nicht authentifizierte Benutzer Client-Skripts ausführen. Fügen Sie die Eigenschaft hinzu, die die Ausführung von Skripts durch einen nicht angemeldeten Benutzer einschränkt.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft nicht hinzufügen, umgehen clientseitige Skripteinbindungen ACLs, was zu unbeabsichtigten öffentlichen Funktionen führen kann. Wenn das Client-Skript vertrauliche Informationen bereitstellt, kann dies ein nachteiliges potenzielles Sicherheitsrisiko darstellen.
Workaround	Wenn Sie die Eigenschaft *`glide.script.ccsi.ispublic`* auf „ **false** “ setzen, werden alle vom Client aufrufbaren Skripteinbindungen privat. Sie können die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion `isPublic()` hinzufügen. Die Funktion `isPublic` hat Vorrang vor der Eigenschaft *`glide.script.ccsi.ispublic`*. Fügen Sie der Skripteinbindung die folgende Syntax hinzu: `isPublic:function(){return[true/false];},`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Verhalten von Produktionsinstanzen erzwingen [Aktualisiert in Security Center 1.3]

Konfigurieren Sie, ob Ihre Instanz wie eine Produktions- oder Nicht-Produktionsinstanz behandelt werden soll.

Wenn die Eigenschaft `glide.installation.production` nicht auf den empfohlenen Wert **true**festgelegt ist, wird die Instanz nicht als Produktionsinstanz behandelt, sodass zboot und andere potenziell gefährliche Skripts ausgeführt werden können. Wenn Sie die Auswertung einer Produktionsinstanz als Nicht-Produktionsinstanz aktivieren, kann dies zu Informationsverlusten oder DoS-Angriffen (Denial of Service) führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.installation.production`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diesen Eigenschaftswert auf „ **false** “ setzen, wird die Instanz als Nicht-Produktionsinstanz behandelt, wodurch zboot und andere potenziell gefährliche Skripts ausgeführt werden können.
Abhängigkeiten und Voraussetzungen	Keine

Lesezugriff für Flow-Kontext einschränken [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft `com.snc.process_flow.reporting.require_flow_access`, um zu erzwingen, ob eine zusätzliche Zugriffsprüfung erforderlich ist, damit ein Benutzer eine Flow-Prüfung lesen kann.

Wenn die Eigenschaft `com.snc.process_flow.reporting.require_flow_access` auf den empfohlenen Wert „true“ festgelegt ist, erfolgt eine zusätzliche Zugriffsprüfung für einen Benutzer, der versucht, einen Flow-Kontext zu lesen. Wenn diese Eigenschaft auf „falsch“ festgelegt ist, kann die Offenlegung geringfügiger Informationen erfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.snc.process_flow.reporting.require_flow_access`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „false“ festgelegt wird, wird das vorhandene Verhalten beibehalten. Wenn diese Eigenschaft auf „true“ festgelegt wird, wird die hinzugefügte Sicherheitsebene des Lesezugriffs erzwungen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft aktiviert ist, wird die Sicherheit für das Lesen von Flow-Kontextdatensätzen erhöht. Die Instanz erzwingt, dass ein Benutzer, der versucht, den Flow-Kontext zu lesen, auch Lesezugriff auf den übergeordneten Flow hat.

Beschränken Sie den Zugriff auf das Hintergrundskript

Konfigurieren Sie die Eigenschaft the `glide.script_processor.admin`, um die Rolle festzulegen, die für den Zugriff auf das Modul „Skripthintergrund“ erforderlich ist.

Die Eigenschaft `glide.script_processor.admin` enthält die erforderliche Rolle für den Zugriff auf das Modul „Skripthintergrund“. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **admin**festgelegt ist, kann jeder Benutzer, unabhängig von seiner Rolle, Hintergrundskripts für die Instanz ausführen. Dadurch können fehlerhafte Akteure das ACL-System umgehen und erhalten vollständigen Zugriff auf Tabellen.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.script_processor.admin`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	Administrator
Standardwert	Administrator
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,8 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert **admin** festgelegt wird, kann jeder Benutzer Hintergrundskripts für die Instanz ausführen.
Abhängigkeiten und Voraussetzungen	Keine

Beschränken Sie den Zugriff auf E-Mails mit leerer Zieltabelle

Aktivieren Sie die Eigenschaft `glide.email.email_with_no_target_visible_to_all`, um den Benutzerzugriff auf E-Mails einzuschränken, es sei denn, er war der Absender der E-Mail oder hat eine Administratorrolle.

Nicht autorisierte Benutzer können in der Tabelle „sys_email_list“ auf E-Mails zugreifen, denen ein Zieldatensatz fehlt. Anstatt ACLs für E-Mail-Einträge zu erzwingen, beschränkt diese Eigenschaft den Zugriff nur auf den E-Mail-Absender und Benutzer mit der Administratorrolle.

Hinweis:
E-Mails, die an die Instanz gesendet und von ihr empfangen werden, werden in der Tabelle „sys_email_list“ angezeigt. Allerdings sollten nur empfangene E-Mails, die mit einem Fehler und dem Status Ignoriert markiert wurden, eine leere Zieltabelle haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.email.email_with_no_target_visible_to_all`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren	Zugriffssteuerung
Zweck	Um zu verhindern, dass der E-Mail-Client E-Mails anzeigt, wenn der Benutzer den Zugriff nicht autorisiert.
Empfohlener Wert	false
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Niedrig) Benutzer können E-Mails mit leerer Zieltabelle nicht mehr sehen, es sei denn, sie sind Administratoren oder der Absender der E-Mail.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Benutzer auf E-Mails zugreifen, bei denen das Feld target_table leer ist.
Referenzen	Erweiterte E-Mail-Eigenschaften

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Beschränken Sie den Zugriff auf das Plugin für bestimmte IP-Bereiche

Verwenden Sie das *com.snc.ipauthenticator* -Plugin, um den Zugriff auf bestimmte IP-Bereiche einzuschränken. Sofern kein öffentlicher Zugriff für die Instanz vorgesehen ist, sollten Administratoren den Zugriff auf die ihnen zugewiesenen IP-Netzblöcke beschränken.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, müssen Sie das Plugin „IP Range Based Authentication “ (com.snc.ipauthenticator)*com.snc.ipauthenticator* aktivieren. Weitere Informationen finden Sie unter IP-Bereichsbasierte Authentifizierung und im Abschnitt „Schritte zum Konfigurieren“ (unten).

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	*com.snc.ipauthenticator*
Konfigurationstyp	Systemsicherheit > IP-Adresszugriffssteuerung
Kategorie	Zugriffssteuerung
Zweck	So fügen Sie den IP-Adressbereich, der auf die Instanz zugreifen kann, den Listen der vertrauenswürdigen und nicht vertrauenswürdigen Domänen hinzu.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Vom Kunden verweigerte IP-Bereiche werden für dieses Korrekturelement verwendet. Keine Auswirkung, da der Kunde die Zielliste definiert.
Sicherheitsrisiko	(Niedrig) Unnötige Gefährdung der Zielinstanz im Internet sollte mithilfe der IP-Zugriffssteuerungsfunktionalität eingeschränkt werden.
Referenzen	IP-Bereichsbasierte Authentifizierung

Schritte zum Konfigurieren von

1. Stellen Sie sicher, dass das Plugin „com.snc.ipauthenticator“ aktiv ist.
2. Navigieren zu **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung**.
3. Klicken Sie auf **Neu**, um eine Ausschlussliste (Deny) oder eine Aufnahmeliste (Allow) von IP-Adressen zu erstellen.
4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf Knowledge Bases beschränken [Neu in Security Center 1.3]

Die Eigenschaft *glide.knowman.block_access_with_no_user_criteria* wird verwendet, um den Lese-/Schreibzugriff von Benutzern auf wissensbasierte Artikel zu steuern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.knowman.block_access_with_no_user_criteria*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 9,1 • CVSS-Punktzahl: Kritisch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt ist, kann jeder Benutzer eine KB lesen und dazu beitragen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Verweigert den Zugriff auf eine Knowledge Base, wenn entweder „Kann lesen“ oder „Kann mitwirken“ nicht angegeben ist.

Beschränken Sie die Berechtigungen für das CMDB-Modell

Verwenden Sie die Systemeigenschaft *csm_cmdb_model.customer_visible_flag*, um den Kundenzugriff auf Daten in der Tabelle „Produktmodelle“ als zusätzliche Zugriffskontrolle für das CMDB-Modell einzuschränken.

Legen Sie die Eigenschaft *csm_cmdb_model.customer_visible_flag* auf „ **true** “ fest, um das Feld Sichtbar für Kunden für die unten aufgeführten Tabellen zu aktivieren:

- Tabelle „Produktmodelle“ [cmdb_model]
- Tabelle „Softwaremodelle “ [cmdb_software_product_model]
- Tabelle „Anwendungsmodelle “ [cmdb_application_product_model]
- Tabelle „Verbrauchsgütermodelle “ [cmdb_consumable_product_model]
- Facility Models-Tabelle [cmdb_facility_product_model]
- Tabelle „Hardwaremodelle “ [cmdb_hardware_product_model]

Wenn diese Eigenschaft auf „ **true** “ festgelegt wird, werden standardmäßig alle cmdb_model-Werte ausgeblendet.

Legen Sie die Eigenschaft auf „ **falsch** “ fest, um die Spalte/das Attribut „customer_visible“ in der Tabelle „cmdb_model “ nicht zu berücksichtigen und sich auf die Basis-ACLs „cmdb_model“ zu verlassen, auf die sn_esm_user zugreifen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`csm_cmdb_model.customer_visible_flag`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Bei Einstellung auf di**true**verwendet das System die Einstellung im Feld Sichtbar für Kunden, um den Zugriff auf Produktmodelldaten im Customer Service Portal zu bestimmen.
Empfohlener Wert	True (False ist Standard).
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Mittel) Jeder Benutzer mit der Rolle „sn_esm_user“ und vordefinierten ACLs kann über Berechtigungen für das CMDB-Modell verfügen. **Hinweis:** Diese Rolle wird in der Regel externen Benutzern gewährt. Externen Benutzern könnten widerwillig Berechtigungen für das CMDB-Modell erteilt werden.
Referenzen	Zugriff auf Produktmodelldaten im Customer Service Portal beschränken

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Beschränken Sie den nicht authentifizierten Zugriff auf Anhänge

Verwenden Sie die Eigenschaft `glide.image_provider.security_enabled`, um die Sicherheitseinstellungen für Images zu steuern. Bei Festlegung auf **true**sind Images nur für authentifizierte und autorisierte Benutzer sichtbar. Bei **false**sind Bilder für alle sichtbar, die eine URL zum Anhang haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.image_provider.security_enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um den nicht authentifizierten Zugriff auf den Anhang zu verhindern, wenn er im `iix` -Format gerendert wird.
Empfohlener Wert	True (Standard)
Funktionale Auswirkung	(Niedrig) Keine nennenswerten Auswirkungen auf die Funktionalität. Die Benutzer-Experience kann etwas beeinträchtigt werden, da der Benutzer, der zuvor direkt auf .iix zugegriffen hat, sich authentifizieren muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Für nicht authentifizierte Benutzer muss eine Einschränkung angewendet werden, da einige Anhänge vertrauliche Informationen enthalten können.
Referenzen	Anhänge verwalten Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Zugriff auf benutzerdefinierte Journaleinträge beschränken [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.live_feed.custom_journal.acl_check_enabled`, um ACLs in benutzerdefinierten Journalfeldern zu berücksichtigen.

Wenn `glide.live_feed.custom_journal.acl_check_enabled` nicht auf den empfohlenen Wert „true“ festgelegt ist, können alle Benutzer alle Journaleinträge in der Live-Feed-Funktion anzeigen. Wenn Sie die Eigenschaft auf „wahr“ setzen, werden ACLs in benutzerdefinierten Journalfeldern berücksichtigt. Dies ist eine vorteilhafte Funktion.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.live_feed.custom_journal.acl_check_enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um zu steuern, welche Benutzer welche Journaleinträge basierend auf ACLs sehen.
Empfohlener Wert	Wahr
Konfigurationstyp	Boolescher Wert.
Sicherheitsrisiko	(Mittel) Bei „wahr“ werden nur die benutzerdefinierten Journaleinträge, die die ACL bestehen, im Live-Feed angezeigt. Andernfalls können alle Benutzer alle Journaleinträge sehen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Zugriffskontrollbedingungen für externe explizite Rollen überprüfen [Neu in Security Center 1.5]

Es wird empfohlen, das Plugin „Explicit Roles“ zu verwenden, um vorzuschreiben, dass alle Benutzer entweder über die Rolle „snc_internal“ für den Zugriff auf interne Ressourcen oder die Rolle „snc_external“ für den Zugriff auf externe Ressourcen verfügen.

Nach der Installation dieses Plugins wird allen vorhandenen Benutzern die Rolle „snc_internal“ zugewiesen, und vorhandene Zugriffssteuerungslisten (ACLs) werden mit den Rollenbedingungen ausgefüllt. Aufgrund der Automatisierungslogik oder des Eingreifens eines Instanzadministrators können die Rollen snc_internal oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

snc_external fälschlicherweise einer ACL hinzugefügt werden, die bereits eine strengere Rollenanforderung enthält. Da die ACL-Rollenbewertung für jeden Benutzer übergeben wird, der eine einer ACL zugeordnete Rolle enthält, ist das Hinzufügen von snc_internal oder snc_external möglicherweise zu weit für den beabsichtigten Zweck einer ACL. Dies kann zu Datenverlust führen, wenn einem Benutzer mit geringen Berechtigungen Zugriff über die ACL gewährt wird.

Beispielsweise wäre es nicht erforderlich, dass die Rollen „snc_internal“ und „admin“ derselben ACL innerhalb einer Tabelle zugeordnet werden. Die ACL soll Administratoren Zugriff gewähren. In diesem Fall ist die Rolle snc_internal ein Fehler. Oder die ACL soll allen snc_internal-Benutzern Zugriff gewähren, wodurch die Administratorrolle unnötig wird. Wenn das Plugin „Explicit Roles“ installiert ist, überprüfen Sie die ACLs, die eine Rollenbedingung für snc_internal oder snc_external sowie eine Bedingung für eine andere Rolle enthalten. Wenn die Rollen für einen bestimmten Anwendungsfall funktionieren, sollte das Ergebnis regelmäßig überprüft werden.

Führen Sie das folgende Hintergrundskript aus, um eine Liste von ACLs zu erfassen, bei denen snc_internal oder snc_external einer ACL hinzugefügt wurde, die bereits einer anderen Rolle zugeordnet ist. Überprüfen Sie, ob ACLs Benutzern mit den Rollen snc_internal oder snc_external Zugriff gewähren sollen. Wenn Benutzer mit geringen Berechtigungen keinen Zugriff über die ACL haben sollen, entfernen Sie die Rollen snc_internal oder snc_external. Das Entfernen dieser Rollen kann dazu führen, dass Benutzer nicht über eine verbleibende Rolle verfügen und nicht auf die durch die ACL geschützte Ressource zugreifen können.

```
var ExplicitRolesEnabled = new GlidePluginManager().isActive('com.glide.explicit_roles');

// Only check if Explicit Roles is enabled
if (ExplicitRolesEnabled) {

   var counterBadInternalACLs = 0;
   var counterBadExternalACLs = 0;
   var sysIdSncInternal = '7fcaa702933002009c8579b4f47ffbde';
   var sysIdSncExternal = '940ba702933002009c8579b4f47ffbe2';
   var api = new SNC.RoleManagementAPI();

   var gr = new GlideRecord('sys_security_acl_role');
   gr.addQuery('sys_user_role', sysIdSncInternal);
   gr.query();
   while (gr.next()) {
      var aclSysId = gr.sys_security_acl;
      var gr2 = new GlideRecord('sys_security_acl_role');
      gr2.addQuery('sys_security_acl', aclSysId);
      gr2.addQuery('sys_user_role', '!=', sysIdSncInternal);
      gr2.addQuery('sys_user_role', '!=', sysIdSncExternal);
      gr2.query();

      while (gr2.next()) {
         // exclude the roles if that contain snc_external
         var role = gr2.sys_user_role;
         var containedRoles = api.findAllContainedRolesForRole(role);
         if (containedRoles.contains(sysIdSncExternal))
            continue;
         gs.print('Found an ACL with snc_internal and yet another role=' + role + '; ACL sys_id='
 + aclSysId);
         counterBadInternalACLs++;
         break;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    }
  }

  var gr = new GlideRecord('sys_security_acl_role');
  gr.addQuery('sys_user_role', sysIdSncExternal);
  gr.query();
  while (gr.next()) {
    var aclSysId = gr.sys_security_acl;
    var gr2 = new GlideRecord('sys_security_acl_role');
    gr2.addQuery('sys_security_acl', aclSysId);
    gr2.addQuery('sys_user_role', '!=', sysIdSncInternal);
    gr2.addQuery('sys_user_role', '!=', sysIdSncExternal);
    gr2.query();

    while (gr2.next()) {
      // exclude the roles if that contain snc_internal
      var role = gr2.sys_user_role;
      var containedRoles = api.findAllContainedRolesForRole(role);
      if (containedRoles.contains(sysIdSncInternal))
        continue;
      gs.print('Found an ACL with snc_external and yet another role=' + role + '; ACL sys_id='
+ aclSysId);
      counterBadExternalACLs++;
      break;
    }
  }

  gs.print('Total number of ACLs with snc_internal and other roles: ' +
counterBadInternalACLs);
  gs.print('Total number of ACLs with snc_external and other roles: ' +
counterBadExternalACLs);
}
```

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.explicit_roles*, *sys_security_acl* und *sys_security_acl_role*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Kein Datentyp
Empfohlener Wert	Kein empfohlener Wert
Standardwert	Kein Standardwert
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Aufgrund der Automatisierung oder des Eingreifens eines Instanzadministrators können die Rollen src_internal oder src_external einer ACL hinzugefügt werden, die bereits eine strengere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Rollenanforderung enthält. Da die ACL-Rollenbewertung für jeden Benutzer übergeben wird, der eine Rolle enthält, die einer ACL zugeordnet ist, ist das Hinzufügen einer der beiden Rollen für den Zweck einer ACL zu weit gefasst und kann zu Datenverlust führen, wenn einem Benutzer mit geringen Berechtigungen Zugriff über die ACL gewährt wird.
Referenzen	Explizite Rollen

Sicherheits-Jump-Start-Plugin aktivieren (ACL-Regeln) [Aktualisiert in Security Center 1.3]

Aktivieren Sie das Plugin „Security Jump Start (ACL Rules)“ (com.snc.system_security*com.snc.system_security*), um mehrere wichtige ACLs zu erstellen, die die Zugriffskontrollen für einige der wichtigsten Systemtabellen in [Now Platformvalidieren.

Diese Regeln bieten eine Starthilfe für die Sicherung vieler Systemtabellen und erleichtern es einer Organisation, eine Instanz in die Produktion zu bringen. Das Plugin „Security Jump Start (ACL Rules)“ wird automatisch auf allen neuen Instanzen installiert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	*com.snc.system_security*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Aktivieren Sie das Plugin Security Jump Start (ACL Rules), um eine ordnungsgemäße Sicherheits-Compliance zu erreichen. Sie bietet einige grundlegende ACLs, die Systemtabellen an erster Stelle sichern, anstatt für jede Systemtabelle, die mit der Standardbereitstellung einer Instanz einhergeht, manuell erstellt zu werden. Diese ACLs sind hilfreich, wenn die neu erstellte Instanz schnell in die Produktion gehen muss.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Mittel) Es gibt erhebliche funktionale Auswirkungen, wenn dieses Plugin ohne Audit der vorhandenen ACLs in der Instanz installiert wird. Kundenkontakt und Definitionen sind erforderlich, bevor die Fehlerkorrektur erfolgen kann.
Sicherheitsrisiko	(Hoch) Die Zugriffskontrolle sollte erzwungen werden, um den unbeabsichtigten Zugriff auf die Instanz zu sperren. ACL-Jumpstart-Regeln wurden erstellt, um einen Ausgangspunkt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	für die Sicherung vieler Systemtabellen zu bieten, damit eine Organisation schnell in die Produktion gehen kann.
Referenzen	Sicherheits-Jump-Start – ACL-Regeln

Schritte zum Konfigurieren von

Wenn dieses Plugin in Ihrer Instanz nicht aktiviert ist, wenden Sie sich an den ServiceNow. Wenn Sie das Plugin zu diesem Zeitpunkt aktivieren, kann dies den Sicherheitszugriff auf Tabellen ändern, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die das Plugin bereitstellt, können Sie bei Bedarf eine oder mehrere davon manuell in einer vorhandenen Instanz erstellen. Diese Liste von ACLs kann in diesem Fall als Leitlinie verwendet werden.

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin .

Abfrageregeln für Arbeitsauftragsverwaltung für Serviceorganisationen aktivieren [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft *sn_fsm.use_query_rules*, um Regeln und Filter auf die Außendienst-Management-Tabellen anzuwenden.

Wenn die Eigenschaft *sn_fsm.use_query_rules* auf „true“ festgelegt ist, werden die Regeln und Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf Außendienst-Management-Tabellen authentifizierter Benutzer zu bestimmen. Dies geschieht durch Abfragen von Business Rules und Lese-ACLs. Wenn diese Eigenschaft auf „false“ festgelegt ist, werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. Abfrage-Business Rules fügen zusätzliche Sicherheitsvalidierungen hinzu, wenn sie für diese Eigenschaft aktiviert werden, und sie filtern Datensätze nach Service Desk-Mitarbeitern, Qualifizierern und Einsatzplanern basierend auf dem zugewiesenen Gebiet oder der Gebietsmitgliedschaft. Dadurch wird das Prinzip der geringsten Berechtigung beim Lesen von Datensätzen implementiert.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_fsm.use_query_rules*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden Regeln und Filter aus sn_query_rule verwendet, um den Lesezugriff auf Tabellen im Außendienst-Management zu bestimmen, wobei das Prinzip der geringsten Berechtigung implementiert wird. Bei „false“ werden die Datensätze nicht basierend auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Business Rules für Abfragen gefiltert und bergen möglicherweise ein erhöhtes Risiko für Daten aus Außendienst-Management-Tabellen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Bei „wahr“ werden Regeln/Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf zugehörige Tabellen des Außendienst-Managements zu bestimmen. Zum Beispiel Arbeitsauftrag (WO) und Arbeitsauftragstabelle (WOT) für den angemeldeten Benutzer durch Abfragen von Geschäftsregeln und Lese-ACLs. Bei „false“ werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. Durch Aktivieren dieser Eigenschaft werden die Daten gesichert, und alle Daten (wm_task und wm_order) sind für die Benutzer nicht sichtbar.
Referenzen	

Verwendung des Vorgangs zum sicheren Einfügen mehrerer Elemente innerhalb der Import Set-API

Verwenden Sie die Eigenschaft `com.glide.import_set_api.insert_multiple_optimize`, um zu steuern, ob `GlideRecordSecure` oder `GlideRecord` für den Vorgang Mehrere einfügen in der Import Set-API verwendet wird.

Wenn `com.glide.import_set_api.insert_multiple_optimize` auf den empfohlenen Wert „false“ festgelegt ist, wird `GlideRecordSecure` zum Einfügen von Datensätzen verwendet, und Zugriffskontrolllisten (ACLs) auf Tabellenebene werden ausgewertet. Wenn diese Eigenschaft auf „true“ festgelegt ist, wird `GlideRecord` zum Einfügen von Datensätzen verwendet, und ACLs auf Tabellenebene werden nicht ausgewertet. Darüber hinaus müssen Sie sicherstellen, dass Import Set API Insert Multiple REST Endpoint ACL (sys_id: 3101b770ff2211105cf343d0653bf182) aktiv ist und Benutzer die Rolle import_transformer haben.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.import_set_api.insert_multiple_optimize`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Zugriffssteuerung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „falsch“ festgelegt ist, kann ein Benutzer mit geringen Berechtigungen Daten in Tabellen außerhalb des Bereichs seiner privilegierten Rollen einfügen.
Umkehrbares Verhalten	Sowohl sichere Überschreibung als auch keine DB-Überschreibung.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft optimiert die Leistung der Import Set-API, indem Daten mithilfe von GlideRecord gespeichert werden. Wenn der Parameter festgelegt ist, muss ein Integrationsbenutzer über die Rolle import_transformer verfügen, um auf die API zugreifen zu können.
Referenzen	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

Erzwingen Sie strikte Sicherheit für SOAP-Anforderungen

Verwenden Sie die Eigenschaft `glide.soap.strict_security`, um die Sicherheit von Webservices zu erzwingen.

Diese Eigenschaft verwendet eine Kombination aus:

- Abfrage/Rückmeldung der Standardauthentifizierung über das HTTP-Protokoll und
- Zugriffskontrollen auf Systemebene im Plugin „Contextual Security: Role Management“..

Wenn Sie diese Eigenschaft auf **true**festlegen, werden die folgenden Aktionen ausgeführt:

- Wenn der Benutzer über die entsprechende Rolle zum Ausführen des Vorgangs verfügt, wird die eingehende SOAP-Anforderung auf Rollenberechtigung zur Validierung überprüft. Es tritt bei Aufrufen/Anforderungen von SOAP-Webservices für Tabellen Now Platform auf, wenn CREATE-, READ-, UPDATE- oder DELETE-Vorgänge ausgeführt werden.
- Überprüft die ACLs auf Systemebene beim Abrufen von Daten in Form von SOAP-Daten aus der Tabelle.
- Überprüft die ACLs auf Feldebene auf CRUD-Vorgänge, die für ein Feld der Tabelle ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.soap.strict_security`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Stellt sicher, dass Sicherheits-ACLs auch dann überprüft und validiert werden, wenn auf die Datensätze über SOAP-Aufrufe zugegriffen wird
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Fehlerkorrektur erzwingt die Zugriffskontrolle auf Systemebene beim Abrufen von Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz. Wenn derzeit Benutzer auf diese Daten zugreifen, ist der Zugriff auf die Daten gemäß den ACL-Regeln eingeschränkt/erlaubt. Informationen zu den Standardrollen, die Zugriff auf die SOAP-Daten haben, finden Sie unter SOAP web service .
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende SOAP-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Enforce strict security for inbound SOAP SOAP web service

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Erforderliche JMS-Verbindungsfactorys [Aktualisiert in Security Center 1.5]

Die Eigenschaft `mid.property.jms.command.allowed_factory_names` steuert die JMS-Verbindungsfactorys (Java Messaging Service), die der MID Server verwenden kann.

Sie ist für einige ausgewählte Factorys gedacht, die von Plugins für JMS-Aktivitäten oder -Aktionen benötigt werden. Das Einbeziehen zusätzlicher Factorys könnte ein Schritt in einer Angriffskette für Schwachstellen wie JDNI-Einfügungen sein, die auf Fähigkeiten basieren, die ein Angreifer in zulässigen Factorys nutzen kann. Um die Möglichkeit einer genutzten Schwachstelle zu verhindern, beziehen Sie keine Factorys ein, die über die erforderlichen Standardwerte hinausgehen.

Um dieses Sicherheitsrisiko zu beheben, überprüfen Sie die Liste der Namen, die für die MID-Eigenschaft angegeben wurden, `mid.property.jms.command.allowed_factory_names`. Stellen Sie sicher, dass zusätzliche Java-Factory-Namen erforderlich sind, die über die Standardwerte von connectionFactory, queueConnectionFactory und topicConnectionFactory hinausgehen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`mid.property.jms.command.allowed_factory_names`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.1 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn das MID Server-Plugin (*com.glideapp.agent*) aktiv ist, überprüfen Sie die Liste der Namen, die für die MID-Eigenschaft *mid.property.jms.command.allowed_factory_names*angegeben wurden. Stellen Sie sicher, dass zusätzliche Factory-Namen erforderlich sind, die über die Standardwerte von connectionFactory, queueConnectionFactory und topicConnectionFactory hinausgehen.
Abhängigkeiten und Voraussetzungen	Keine

Legen Sie den Gastbenutzer für SOAP-Anforderungen fest

Konfigurieren Sie diese Eigenschaft, um die Zugriffsebene nicht authentifizierter SOAP-Anforderungen zu steuern.

Diese Eigenschaft steuert die Zugriffsebene nicht authentifizierter SOAP-Anforderungen. Wenn er nicht auf den empfohlenen Wert von *soap.guest*festgelegt ist oder auf einen Benutzer mit eingeschränkten Berechtigungen festgelegt ist, werden SOAP-Anforderungen im Namen des Benutzers ausgeführt. Wenn diese Eigenschaft leer ist, wird nicht authentifizierter Zugriff auf Vorgänge auf Administrator- oder Wartungsebene ermöglicht, wodurch alle Sicherheitskontrollen innerhalb der Instanz aufgehoben werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.soap.guest_user*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	seif.gast
Standardwert	seif.gast
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „leer“ setzen, wird nicht authentifizierter Zugriff auf Vorgänge auf Administrator- oder Wartungsebene ermöglicht.
Abhängigkeiten und Voraussetzungen	Keine

Richtlinienbasierten Sitzungszugriff für Mobilgeräte aktivieren [Neu in Security Center 1.5]

Verwenden Sie das Plugin „The Zero Trust – Policy Based Session Access“, um zu steuern, ob die Rollen von Benutzern, die sich über eine Mobile-App authentifizieren, reduziert werden.

Mit dem Plugin „Zero Trust – Policy Based Session Access“ können Sicherheitsadministratoren den Benutzerzugriff in einer Sitzung basierend auf Parametern wie IP-Adresse, Standort, Provider-Attributen und Benutzerattributen mit adaptiven Authentifizierungsrichtlinien reduzieren. Wenn dieses Plugin aktiviert oder auf „true“ festgelegt ist, werden die Rollen von Benutzern, die sich über ein Mobilgerät authentifizieren, gemäß den Richtlinien des Plugins eingeschränkt. Instanzadministratoren möchten möglicherweise den Zugriff mit hohen Berechtigungen einschränken, wenn sich Benutzer über ein Mobilgerät authentifizieren, da dies auf eine unsichere Umgebung für vertrauliche Vorgänge hinweisen könnte.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.session_access.mobile.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,7 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Härtungseinstellung auf „wahr“ festgelegt ist, wird der richtlinienbasierte Sitzungszugriff für die Instanz für mobile Anmeldungen erzwungen, und Benutzer, die nicht aus einer vertrauenswürdigen Umgebung stammen oder keine vertrauenswürdigen Geräte verwenden, erhalten reduzierte Rollen -Berechtigungen. „Wahr“ ist die sichere Einstellung. Wenn diese Einstellung auf „falsch“ konfiguriert ist, ist der richtlinienbasierte Sitzungszugriff deaktiviert, und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	die Benutzer haben weiterhin vollständige Rollen, einschließlich der Rollen mit hohen Berechtigungen wie „admin“.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn der Administrator die Sitzungszugriffsrichtlinie für die Instanz konfiguriert hat, werden die Rollen der Benutzer nach der mobilen Anmeldung reduziert, wenn sie nicht aus einer vertrauenswürdigen Umgebung stammen oder ein vertrauenswürdiges Gerät verwenden.
Referenzen	Adaptive Authentifizierung

Aktivieren Sie das SNC-Zugriffssteuerungs-Plugin

Aktivieren Sie das Plugin „SNC Access Control“ (com.snc.snc_access_control`com.snc.snc_access_control`), um den Zugriff auf Ihre Instanzen durch Mitarbeiter von Kundenservice und Support zu steuern.

Die Standardkonfiguration für Now Platform ermöglicht Kundenservice und Support den Zugriff auf Instanzen über einen internen Prozess, der Anmeldeinformationen für den kurzfristigen Support erstellt. Obwohl jeder Zugriff geprüft wird, ziehen es einige Kunden vor, diesen Zugriff zu steuern.

Mit diesem Plugin können Kundenservice und Support Kundenservice und Support Mitarbeitern den Zugriff auf die Instanz verweigern. Diese Entscheidung wirkt sich auf Support-SLAs aus, da Sie den Zugriff Now Platform aktivieren müssen, bevor Support-Aktivitäten beginnen können. Weitere Informationen finden Sie unter ServiceNow-Zugriffssteuerung.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	`com.snc.snc_access_control`
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Verbietet Kundenservice und Support Mitarbeitern den Zugriff auf die Instanz
Empfohlener Wert	Aktiv
Erforderliche Rolle	Der Kundenadministrator kann dieses Plugin nicht aktivieren. Es muss explizit angefordert werden, da es erhöhte Berechtigungen erfordert, um das Plugin zu aktivieren.
Sicherheitsrisikobewertung	8.2
Funktionale Auswirkung	(Niedrig) Wenn dieses Plugin inaktiv ist, können alle Kundenservice und Support Mitarbeiter auf die Instanz des Kunden zugreifen. Durch die Aktivierung des Plugins kann der Kunde den Zugriff auf autorisierte Kundenservice und Support Mitarbeiter beschränken.
Sicherheitsrisiko	(Hoch) Unnötige Offenlegung des Instanzzugriffs für eine breitere Gruppe von Personen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	ServiceNow-Zugriffssteuerung

Schritte zum Konfigurieren von

1. Führen Sie die Schritte in ServiceNow Zugriffssteuerung wird aktiviertaus, um das Plugin anzufordern. Kunden müssen das Plugin „SNC Access Control“ (com.snc.snc_access_control) von HI anfordern.
2. Führen Sie die Schritte in ServiceNow Zugriffssteuerung konfigurierenaus, um die SNC-Zugriffssteuerung zu aktivieren. Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere Kundenservice und Support Mitarbeiter anzugeben, die berechtigt sind, sich bei Ihrer Instanz anzumelden.

Sicherheitsbereich für Agent Workspace for HR Case Management erzwingen [Neu in Security Center 1.5]

Konfigurieren Sie das Plugin „Agent Workspace for HR Case Management“, sodass nur Benutzer mit den richtigen Berechtigungen auf Daten in den Master-Tabellen des Bereichs zugreifen können, wodurch das Prinzip der geringsten Berechtigung erzwungen wird.

Wenn das Plugin *`glide.enforce_security_scope.sn_hr_agent_ws`* auf den empfohlenen Wert „true“ konfiguriert ist, werden nur die Zugriffskontrolllisten (ACLs) im Plugin „Agent Workspace for HR Case Management“ verwendet, um den Zugriff auf eine Ressource zu bestimmen. Wenn diese Einstellung auf „false“ festgelegt ist, werden die Daten von Agent Workspace for HR Case Management in den Master-Tabellen des Bereichs verfügbar gemacht, da den ACLs aus allen Bereichen Zugriff gewährt wird.Beispielsweise kann ein IT-Administrator auf Agent Workspace for HR Case Management-Daten zugreifen, wenn diese Einstellung auf „false“ festgelegt ist. Um dies zu verhindern, setzen Sie *`glide.enforce_security_scope.sn_hr_agent_ws`* auf den empfohlenen Wert true, um sicherzustellen, dass das Prinzip der geringsten Berechtigung gilt, da Benutzer nur auf Ressourcen zugreifen können, für die sie berechtigt sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*`glide.enforce_security_scope.sn_hr_agent_ws`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Einstellung auf „falsch“ konfigurieren, werden die Daten von Agent Workspace for HR Case

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Management in den Master-Tabellen des Bereichs verfügbar gemacht, da den ACLs aus allen Bereichen Zugriff gewährt wird.
Abhängigkeiten und Voraussetzungen	Mitarbeiterbereich für HR-Fallmanagement
Funktionale Auswirkung	Wenn Sie diese Einstellung auf „true“ konfigurieren, wird die Ausführung globaler ACLs für eine Tabelle erzwungen, wenn für sie keine bereichsbezogenen ACLs vorhanden sind.
Referenzen	• https://owasp.org/www-project-proactive-controls/#div-numbering • Add a component to Agent Workspace

Playbook für Sicherheitsbereichslizenz und -erlaubnis erzwingen [Neu in Security Center 1.5]

Verwenden Sie diese Eigenschaft, um zu bestimmen, ob nur die Zugriffssteuerungslisten (ACLs) im Plugin „License and Permit“ für die Bestimmung des Zugriffs auf den Bereich verwendet werden oder ob ACLs aus allen Bereichen berücksichtigt werden.

Wenn die Eigenschaft *glide.enforce_security_scope.sn_gsm_lic_prmt* auf den empfohlenen Wert true festgelegt ist, werden nur ACLs im Plugin „License and Permit“ verwendet, um den Zugriff auf den Bereich zu bestimmen. Wenn diese Einstellung auf „false“ konfiguriert ist, werden die Daten von Lizenz- und Erlaubnis-Playbooks in den Master-Tabellen des Bereichs verfügbar gemacht, da ACLs aus allen Bereichen Zugriff erhalten. Um die Datenexposition zu reduzieren, setzen Sie *glide.enforce_security_scope.sn_gsm_lic_prmt* auf den empfohlenen Wert true.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.sn_gsm_lic_prmt*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Einstellung auf den empfohlenen Wert „true“ konfigurieren, werden die Daten der Lizenz- und Erlaubnis-Playbooks in den Master-Tabellen des Bereichs gesichert, indem nur ACLs aus dem Bereich *sn_gsm_lic_prmt* für die Gewährung des Zugriffs berücksichtigt werden. Wenn diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Option auf „falsch“ gesetzt wird, werden die Lizenz- und Erlaubnis-Playbook-Daten in den Bereichshaupttabellen verfügbar gemacht, indem die ACLs aus allen Bereichen für die Gewährung von Zugriff berücksichtigt werden. Beispielsweise kann der IT-Administrator auf Lizenz- und Erlaubnis-Playbook-Daten zugreifen, wenn diese Einstellung auf „falsch“ gesetzt ist.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• Using License and Permit Playbook • Application scope

Verhindern, dass sich inaktive Benutzer anmelden [Neu in Security Center 1.5]

Konfigurieren Sie diese Eigenschaft, um zu steuern, ob sich inaktive Benutzer bei Ihrer Instanz authentifizieren können.

Wenn die Einstellung `glide.authenticate.only.allow.active.user.login` nicht auf den empfohlenen Wert true festgelegt ist, können sich Benutzer in der Tabelle sys_user, die als inaktiv markiert sind, weiterhin bei der Instanz anmelden. Benutzer können als inaktiv markiert werden, wenn sie nicht mehr zur Anmeldung berechtigt sind, z. B. wenn ihnen ein Unternehmen gekündigt wird. Wenn die Einstellung auf „falsch“ konfiguriert ist, können Benutzer weiterhin auf die Instanz und die Daten zugreifen, auf die sie zuvor Zugriff hatten.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.only.allow.active.user.login`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, können inaktive Benutzer wie ein gekündigter Mitarbeiter weiterhin auf die Instanz und alle Daten zugreifen.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API und Webservice

Die Kategorie „API und Webservice“ stellt sicher, dass Anwendungen über eine angemessene Authentifizierung, Autorisierung und Sitzungsverwaltung verfügen, alle Eingaben validieren, die eine Vertrauensgrenze überschreiten, und Sicherheitskontrollen für alle API-Typen enthalten.

Spezifische Steuerungen in dieser Kategorie befassen sich mit der Validierung von Eingaben nach Servicetyp, z. B. XDS-Schemavalidierung für SOAP Web Services oder Denial of Service-Schutz für graphQL-APIs.

Validieren Sie den SOAP-Inhaltstyp

Verwenden Sie die Eigenschaft `glide.soap.require_content_type_xml`, um die Validierung eines Inhaltstyps als text/xml zu aktivieren und vor ungültigen SOAP-Anforderungen zu schützen.

- Bei Festlegung auf **true**validiert Now Platform den Inhaltstyp als text/xml und schützt vor ungültigen SOAP-Anforderungen.
- Bei **false**ist jeder Inhaltstypwert zulässig.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.soap.require_content_type_xml`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Schutz vor ungültigen SOAP-Anforderungen
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur ermöglicht die Validierung des SOAP-Inhaltstyps für alle eingehenden SOAP-Anforderungen. • Wenn Sie für eingehende Anforderungen einen anderen Inhaltstyp als Text/XML verwenden, kann dies zu einem potenziellen Fehler bei SOAP-Transaktionen führen. • Wenn Sie nicht den richtigen MIME-Typ verwenden, kann dies die Integration von Drittanbietern unterbrechen.
Sicherheitsrisiko	(Mittel) Bei der Annahme eingehender SOAP-Anforderungen wird die entsprechende Validierung durchgeführt, um sicherzustellen, dass der relevante Inhaltstyp als Teil der Anforderung definiert wird. Sie schränkt die ungültigen SOAP-Antworten ein, die als Sicherheitsrisiko angesehen werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenz	Inhaltstypen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für PDF-Anforderungen anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.pdf`, um anzugeben, ob für eingehende PDF-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.pdf`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für PDF-Anforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von PDF-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Webservice-Importsätze .
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende PDF-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierung für Event Management-HTTP-Prozessor erforderlich [Neu in Security Center 1.3]

Erfahren Sie, wie Sie eine sichere Basic Authentication für eingehende SNS-Anforderungen (Amazon Simple Notification Service) einrichten, wenn das Event Management-Plugin (`com.glideapp.itom.snac`) aktiviert ist.

Wenn die Eigenschaft `glide.basicauth.required.evtmgmthttpprocessor` nicht auf den empfohlenen Wert **true**festgelegt ist und das Event Management-Plugin (`com.glideapp.itom.snac`) aktiv ist, ist die Basic Authentication nicht für alle eingehenden SNS-Anforderungen (Amazon Simple Notification Service) erforderlich. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.

Um dieses Sicherheitsrisiko zu beheben, stellen Sie sicher, dass `glide.basicauth.required.evtmgmthttpprocessor` auf „**true** “ festgelegt und `com.glideapp.itom.snac` aktiv ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.basicauth.required.evtmgmthttpprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	API und Webservice
Sicherheitsrisiko	• Schweregradpunktzahl: 7 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn`glide.basicauth.required.evtmgmthttpprocessor` nicht auf den empfohlenen Wert „true“ festgelegt und das Plugin `com.glideapp.itom.snac` „[]“ nicht aktiviert wird, wird die Basic Authentication für eingehende SNS-Anforderungen nicht aktiviert. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Access control
Funktionale Auswirkung	Wenn `glide.basicauth.required.evtmgmthttpprocessor` nicht auf den empfohlenen Wert True festgelegt ist und das Event Management-Plugin (com.glideapp.itom.snac) aktiv ist, ist die Basic Authentication nicht für alle eingehenden SNS-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Anforderungen von Amazon Web Services erforderlich. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.

Autorisierung für SOAP-Anforderungen erfordern [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft *glide.basicauth.required.soap*, um anzugeben, ob für eingehende SOAP-Anforderungen eine Standardautorisierung erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.soap*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Autorisierung von SOAP-Anforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Benutzer, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Anmeldeinformationen für SOAP Web Service und MID Server-Authentifizierung und SOAP-Anforderungen.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung, die für die SOAP-Datenquellenanforderungen konfiguriert ist, kann ein nicht autorisierter Benutzer auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autorisierung für Entladeanforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.unl` (useUnloadFormat), um anzugeben, ob für eingehende Entladeanforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.unl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Basic Authentication bei Entladeanforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von Entladedaten für die Instanz abgerufen werden.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung, die für die Entladeanforderungen für Datenquellen konfiguriert ist, kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten. Stellen Sie sicher, dass `glide.basicauth.required.unl` in sys_properties_table vorhanden und auf „true“ festgelegt ist.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für CSV-Anforderungen anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.csv`, um anzugeben, ob für eingehende CSV-Anforderungen (Comma-Separated Values) die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.csv`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für CSV-Anforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von CSV-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende CSV-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte und Daten in der Zielinstanz erhalten. Stellen Sie sicher, dass `glide.basicauth.required.csv` in der Tabelle „sys_properties“ vorhanden und auf „true“ festgelegt ist.
Referenzen	Webservice-Sicherheit

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

Autorisierung für Excel-Anforderungen anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.excel`, um anzugeben, ob für eingehende Excel-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.excel`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	So erzwingen Sie die Basic Authentication für Excel-Anforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von Excel-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende Excel-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für Importanforderungen anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.importprocessor`, um anzugeben, ob für eingehende Importanforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.importprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für Importanforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	5.3

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird beim Importieren von Datenquellen in die Instanztabellen/-seiten durchgeführt. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung, die für die Datenquellen-Importanforderungen konfiguriert ist, kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	SOAP-Webservices Sicherheit SOAP-Webservice

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

Autorisierung für JSONv2-Anforderung anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.jsonv2`, um anzugeben, ob für eingehende JSONv2-Anforderungen eine Standardautorisierung erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.jsonv2`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Autorisierung von JSONv2-Anforderungen.
Sicherheitsrisikobewertung	7.5
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von JSON-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Benutzer, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter JSONv2-Webservice JSONv2-Webservice .
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung, die für die JSON-Anforderungen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Benutzer auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung Basic Authentication für eingehende JSONv2-Anforderungen anfordern

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für WSDL-Anforderung anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.wsdl`, um anzugeben, ob für eingehende WSDL-Anforderungen (Web Services Description Language) die Basic Authentication erforderlich sein soll.

Hinweis:
Wenn Sie keine Basic Authentication für eingehende WSDL-Anforderungen anfordern möchten, müssen Sie die Zugriffskontrollregeln (ACL) ändern, damit Gastbenutzer auf den WSDL-Inhalt zugreifen können.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.wsdl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Basic Authentication für WSDL-Anforderungen.
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von WSDL-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung, die für die WSDL-Webservices konfiguriert ist, kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche WSDL-Inhalte/-Daten in der Zielinstanz erhalten.
Referenzen	Webservice-Sicherheit

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Berechtigung für XML-Anforderungen anfordern

Verwenden Sie die Eigenschaft `glide.basicauth.required.xml`, um anzugeben, ob für eingehende XML-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.xml`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für XML-Anforderungen.
Sicherheitsrisikobewertung	7.5
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von XML-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter XML-Parser-Schritt.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende XML-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property.

Berechtigung für XML-Ausgabeanforderungen erfordern

Konfigurieren Sie diese Eigenschaft so, dass für alle eingehenden XMLOutputProcessor-Anforderungen eine Standardautorisierung erforderlich ist.

Wenn die Eigenschaft `glide.basicauth.required.xmloutputprocessor` nicht auf den empfohlenen Wert **true**festgelegt ist, ist für eingehende XMLOutputProcessor-Anforderungen keine Standardautorisierung erforderlich, was zu einer nicht authentifizierten Offenlegung von Informationen durch die Instanz führen kann.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.basicauth.required.xmloutputprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	API und Webservice
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn die Eigenschaft nicht auf den empfohlenen Wert „ **true** “ festgelegt wird, kann dies dazu führen, dass vertrauliche Informationen aus der Instanz verloren gehen.
Abhängigkeiten und Voraussetzungen	Keine

Autorisierung für XSD-Anforderungen erfordern

Verwenden Sie die Eigenschaft *glide.basicauth.required.xsd*, um anzugeben, ob für eingehende XSD-Anforderungen (XML-Schemadefinition) die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.xsd*glide.basicauth.required.xsd*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für XSD-Anforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von XSD-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Nicht interaktive Sitzungen .
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für eingehende XSD-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigung für Skriptanforderungen anfordern

Verwenden Sie die Eigenschaft `glide.basicauth.required.scriptedprocessor`, um anzugeben, ob für eingehende Skriptanforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.scriptedprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für Skriptanforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Authentifizierung in Form der Standardautorisierung. • Diese Authentifizierung wird während der Verarbeitung von Skriptanforderungen für die Instanz durchgeführt. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende Skriptanforderungen greift ein nicht autorisierter Benutzer auf vertrauliche Inhalte/Daten in der Zielinstanz zu.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für SCHEMA-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.schema`, um eine Standardautorisierung für alle Anforderungen des eingehenden Tabellenschemas zu erfordern.

Der Schemaprozessor für eingehende Tabellen verarbeitet eingehende Schemaanforderungen für die -Plattform.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie `glide.basicauth.required.schema` auf den empfohlenen Wert von „ **true** “ fest, um eine Standardautorisierung für alle Anforderungen des Schemaprozessors für eingehende Tabellen zu erfordern. Legen Sie den Wert auf **„false“ fest**, um keine Standardautorisierung für alle Anforderungen des Schemaprozessors für eingehende Tabellen zu erfordern.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.schema`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um Basic Authorization für alle Anforderungen des eingehenden Tabellenschemas zu erfordern.
Empfohlener Wert	True (Standardwert).
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Mittel) Wenn die Authentifizierung von diesem Prozessor ausgelassen wird, führt dies zu nicht authentifiziertem Zugriff auf Instanzdaten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für RSS-Anforderungen anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.rss`, um anzugeben, ob für eingehende RSS-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.rss`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für RSS-Anforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.5

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird während der Verarbeitung von RSS-Anforderungen für die Instanz durchgeführt. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter RSS-Feed-Generator .
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende RSS-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	RSS-Basic Authentication

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für API-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.api`, um die Sicherheit für die Standardautorisierung für eingehende REST-Anforderungen zu verbessern.

Legen Sie die Eigenschaft `glide.basicauth.required.api` auf „ **true** “ fest, um eine Autorisierung für alle REST-Anforderungen zu erfordern. Legen Sie die Eigenschaft auf **„false“ fest**, um die Autorisierung für alle REST-Anforderungen zu umgehen.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.api`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Standardberechtigung für eingehende REST-Anforderungen.
Empfohlener Wert	True (Standard)
Konfigurationstyp	Zeichenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Wenn „glide.basisauth.erforderlich.api“ nicht auf den empfohlenen Wert „wahr“ festgelegt ist, wird die Standardauthentifizierung für die API-Anforderung deaktiviert, was zu nicht authentifiziertem Zugriff auf Instanzdaten führt.
Sicherheitsrisikobewertung	8.6

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Berechtigung für Entladeanforderungen anfordern

Verwenden Sie die Eigenschaft `glide.basicauth.required.unl` (useUnloadFormat), um anzugeben, ob für eingehende Entladeanforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.unl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Basic Authentication bei Entladeanforderungen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von Entladedaten für die Instanz abgerufen werden.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung, die für die Entladeanforderungen für Datenquellen konfiguriert ist, kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Architektur, Design und Bedrohungsmodellierung

Diese umfassende Steuerung befasst sich mit allgemeinen Designüberlegungen und Schlüsselelementen zur Implementierung einer sicheren Anwendung. Dies umfasst die Mandanten der Verfügbarkeit, der Integrität der Vertraulichkeitsverarbeitung, der Unbestreitbarkeit und des Datenschutzes. Darüber hinaus sind Elemente eines sicheren Softwareentwicklungslebenszyklus enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbasierte Authentifizierung nicht erzwungen

Die Eigenschaft `glide.authenticate.mutual.enabled` aktiviert die zertifikatsbasierte Authentifizierung, eine Art der gegenseitigen Authentifizierung für eingehende REST-Verbindungen zu REST- und SOAP-APIs in der Now Platform.

Die gegenseitige Authentifizierung stellt eine Vertrauensstellung zwischen Server und Client her, indem SSL-Zertifikate (Secure Socket Layer) ausgetauscht werden, um das Zertifikat bei einer vertrauenswürdigen Zertifizierungsstelle zu validieren. Dies ermöglicht die Überprüfung, ob eine vertrauenswürdige Quelle eine Verbindung zu Now Platformherstellt. Wenn diese Instanz nicht auf den empfohlenen Wert „true“ festgelegt ist, ist sie möglicherweise angreifbar für Man-in-the-Middle-Angriffe (MitM).

Um diese Sicherheitsbedrohung zu beheben, aktivieren Sie die gegenseitige Authentifizierung für eingehende Webservices. Wenn Sie das Plugin für die zertifikatsbasierte Authentifizierung (`com.glide.auth.mutual`)) für Now Platform] zum ersten Mal installieren, folgen Sie den Anweisungen von Richten Sie die zertifikatsbasierte Authentifizierung ein. Stellen Sie außerdem sicher, dass die Eigenschaft `glide.authenticate.mutual.enabled` auf „true“ festgelegt ist, um das Plugin zu aktivieren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.mutual.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, validiert die zertifikatsbasierte Authentifizierung keine Zertifikate bei einer vertrauenswürdigen Zertifizierungsstelle. Dies erhöht die Wahrscheinlichkeit, dass ein schlechter Akteur eine Instanz mit MitM-Angriffen angreift.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • Zertifikatbasierte Authentifizierung • Konfigurieren der gegenseitigen Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identitätswechsel bei ACL-Auswertung in HR-App überprüfen [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft *sn_hr_core.impersonateCheck*, um zu verhindern, dass ein Benutzer die Identität eines anderen Benutzers annimmt und auf dessen HR-Informationen zugreift.

Eine sichere Einstellung verhindert, dass ein Administrator die HR-Informationen eines anderen Benutzers einsehen kann, während er Identitäten annimmt. Eine unsichere Einstellung für diese Eigenschaft ermöglicht es einem Administrator, die Identität eines Benutzers anzunehmen und mit dem Zugriff des Benutzers, dessen Identität Sie annehmen, auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zuzugreifen. Aufgrund der Art dieser Art von Daten, z. B. Informationen, die nur für den Benutzer selbst verfügbar sein sollten, wie E-Mails, wird dies nicht empfohlen. Das Festlegen von *sn_hr_core.impersonateCheck* auf „true“ ermöglicht den Zugriff auf HR-Informationen nur, wenn der Benutzer nicht die Identität anderer annimmt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_hr_core.impersonateCheck*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Eine unsichere Einstellung für diese Eigenschaft ermöglicht es einem Administrator, die Identität eines Benutzers anzunehmen und mit dem Zugriff des Benutzers, dessen Identität angenommen wird, auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zuzugreifen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „true“ festgelegt ist, wird verhindert, dass ein Administrator die HR-Informationen eines anderen Benutzers sieht, während er Identitäten annimmt. Bei „false“ kann ein Administrator die Identität eines Benutzers annehmen und mit dem Zugriff des Benutzers, dessen Identität Sie annehmen, auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zugreifen. Aufgrund der Art dieser Art von Daten, z. B. Informationen, die nur für den Benutzer selbst verfügbar sein sollten, wie eine E-Mail, wird dies nicht empfohlen. Das Festlegen von sn_hr_core.impersonateCheck auf „true“ ermöglicht nur den Zugriff auf HR-Informationen, wenn der Benutzer nicht die Identität anderer annimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Deaktivieren Sie nicht authentifizierte veröffentlichte Berichte

Deaktivieren Sie diese Eigenschaft, um zu verhindern, dass der Benutzer Berichte veröffentlicht oder darauf zugreift. Diese Eigenschaft deaktiviert die Funktion für veröffentlichte Berichte in der Berichterstellung.

Aktivieren Sie das Veröffentlichen von Berichten, indem Sie `glide.report.published_reports.enabled` auf **true**setzen.

Sicherheit für Berichte erzwingen ist konform, wenn `glide.report.published_reports.enabled` auf **false**festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.report.published_reports.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Deaktiviert die Funktion für veröffentlichte Berichte in der Berichterstellung.
Typ	wahr | falsch
Empfohlener Wert	**false**
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	(Mittel) Der Benutzer kann keine Berichte veröffentlichen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, können Benutzer möglicherweise auf Berichte zugreifen oder diese veröffentlichen, die vertrauliche Daten verfügbar machen. Durch das Veröffentlichen eines Berichts wird eine URL erstellt, über die jeder auf den Bericht zugreifen kann, einschließlich Personen, die keine Benutzer sind. Wenn jemand zur URL navigiert, wird der Bericht mit aktuellen Daten aus der Instanz generiert.
Referenzen	Berichte veröffentlichen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Erzwingen Sie Feld-ACLs für eingehende Abfrageanforderungen

Verwalten Sie, wie eingehende Abfragen in Ihrer Instanz validiert werden.

Verwenden Sie die Eigenschaft `glide.report.report_view.check_published`, um zu überprüfen, wie eingehende Abfragen in Ihrer Instanz validiert werden. Wenn die Eigenschaft auf den empfohlenen Wert **true**festgelegt ist, werden Feld-ACLs auf eingehende Abfragen überprüft und abgelehnt, wenn der Benutzer nicht autorisiert ist. Wenn die Eigenschaft auf **false**festgelegt ist, werden ACLs nicht auf eingehende Abfragen überprüft und weiterhin ausgeführt, was zur Offenlegung von Informationen an nicht autorisierte Parteien führen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.report.report_view.check_published`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,4 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **false**“ festgelegt ist, werden ACLs nicht auf eingehende Abfragen überprüft, die zur Offenlegung von Informationen führen können.
Abhängigkeiten und Voraussetzungen	Keine

Lese-ACLs in Berichtsansichten erzwingen

Verwalten Sie, wie Lese-ACLs in Ihrer Instanz erzwungen werden.

Verwenden Sie die Eigenschaft `glide.report.report_view.read_acl`, um die Lese-ACL (Tabellenebene) für Berichtsfunktionen zu erzwingen, wenn für die Tabelle oder das Feld keine Berichtsansichts-ACL vorhanden ist. Wenn diese Eigenschaft nicht auf „ **erzwingen**“ festgelegt ist, können ACLs umgangen werden, was zu einem Verlust vertraulicher Informationen führt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.report.report_view.read_acl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	erzwingen
Standardwert	erzwingen
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,1 • CVSS-Punktzahl: Hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „ **Erzwingen** “ festgelegt wird, kann dies dazu führen, dass ACLs umgangen werden.
Abhängigkeiten und Voraussetzungen	Keine

Definieren zulässiger ServiceNow interner IP-Adressen [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft *glide.ip.authenticate.strict*, um IP-Bereiche anzugeben, die eingehende Verbindungen in einer Instanz herstellen können.

Wenn *glide.ip.authenticate.strict* auf truefestgelegt ist, können nur in *glide.ip.authenticate.allow.secured* angegebene IP-Bereiche eingehende Verbindungen in einer Instanz herstellen. Diese Eigenschaft enthält eine Liste nur der wichtigen internen IP-Bereiche von ServiceNow (Sicheres VPN, DC).

Wenn *glide.ip.authenticate.allow.secured* nicht auf den empfohlenen Wert „10.0.0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0.0/17, 149.96.0.0/16, 199.91.136.0/21, 148.139. 0.0/16, 127.0.0.1, 0:0:0:0:0:0:0:1", kann nicht vertrauenswürdige Quellen außerhalb von ServiceNow DataCenter und sicheres VPN den Zugriff auf vertrauliche Überwachungsendpunkte in Instanzen zulassen.

⚠ Warnung:
Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ip.authenticate.strict*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Ermöglicht ServiceNow-Mitarbeitern den Zugriff auf die Instanz nur über gesicherte IP-Bereiche
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	(Niedrig) Wenn diese Eigenschaft nicht aktiviert ist, können ServiceNow-Mitarbeiter über alle IP-Bereiche auf die Instanz des Kunden zugreifen. Durch Aktivieren der Eigenschaft wird der Zugriff auf einen sicheren Satz von IP-Bereichen (Sicheres VPN, DC) eingeschränkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Hinweis: Wenn Sie diese Eigenschaft auf `true` festlegen, verwendet Now Platform eine restriktivere `glide.ip.authenticate.allow.secured` -Eigenschaft anstelle der Leistungsüberwachungs-IP-Einschränkungseigenschaft (`glide.ip.authenticate.allow.secured`) für eine Reihe von IP-Bereichen, die auf die Instanz zugreifen können.
Sicherheitsrisiko	(Niedrig) Unnötige Offenlegung des Instanzzugriffs für eine breitere Gruppe von Personen.
Referenz	IP-Bereichsbasierte Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Hinweis:
Eine Deny-All-Regel muss der IP-Zugriffssteuerung hinzugefügt werden, um den Zugriff von IP-Adressen einzuschränken, die nicht der IP-Zugriffssteuerung hinzugefügt wurden. Alle erforderlichen zulässigen IPs müssen dann der IP-Zugriffssteuerung hinzugefügt werden.

Legacy-JQuery-Verhalten deaktivieren [Aktualisiert in Security Center 1.3]

`glide.jquery.legacy` wird verwendet, um zu verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die nicht gepatchte Schwachstellen in die Bibliothek einführen.

Legen Sie `glide.jquery.legacy` auf den empfohlenen Wert **false** fest, um zu verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die nicht gepatchte Schwachstellen in die Bibliothek einführen. Legen Sie den Wert auf „ **true** “ fest, um vorinstallierte JQuery-Versionen zuzulassen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.jquery.legacy`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Um potenzielle Sicherheitsrisiken zu verhindern, die durch Angriffe auf Schwachstellen entstehen, die in veralteten Versionen der JQuery-Bibliothek erkannt wurden.
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Verhindert, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die nicht gepatchte Schwachstellen in die Bibliothek einführen. Die Systemeigenschaft ist ausfallsicher, falls Organisationen von den nicht gepatchten Versionen von AngularJS abhängig sind, um ihre benutzerdefinierten Implementierungen auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	7.1

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Legacy-Verhalten für GlideRecord-Umfangsbegrenzung aktivieren [Neu in Security Center 1.3]

Die Eigenschaft `glide.record.legacy_cross_scope_access_policy_in_script` deaktiviert die Bereichsbegrenzung, sodass bereichsbezogene Apps auf globale Skriptschnittstellen zugreifen können. Es wurde als Patch für den bereichsübergreifenden Zugriff von GlideRecord erstellt.

GlideRecord bietet bereichsübergreifenden Erstellungs- und Aktualisierungszugriff auf Tabellen, die nicht mit dieser Zugriffsebene konfiguriert wurden. Um zu verhindern, dass Anwendungen von Kunden beschädigt werden, wenn dieses bereichsbezogene Zugriffsverhalten gepatcht wurde, wurde die Eigenschaft `glide.record.legacy_cross_scope_access_policy_in_script` erstellt. Wenn diese Eigenschaft auf „true“ festgelegt ist, greift der bereichsübergreifende Zugriff auf das veraltete Verhalten zurück, das unsicher ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.record.legacy_cross_scope_access_policy_in_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	Wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Die Umfangsdefinition stellt sicher, dass Anwendungen nur auf Ressourcen mit explizitem Zugriff oder innerhalb ihres Bereichs zugreifen können, indem das Prinzip der geringsten Berechtigung angewendet wird. Das Deaktivieren dieser Funktion kann Auswirkungen auf Vertraulichkeit, Verfügbarkeit und Integrität haben.
Abhängigkeiten und Voraussetzungen	Keine

Legacy-AngularJS-Verhalten deaktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.angular.legacy`, um sich vor potenziellen Sicherheitsrisiken zu schützen, die durch Angriffe auf Schwachstellen entstehen, die in veralteten AngularJS-Bibliotheksversionen erkannt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie *glide.angular.legacy* auf den empfohlenen Wert **false** fest, um zu verhindern, dass ältere vorab gepatchte AngularJS-Versionen verwendet werden. Legen Sie die Eigenschaft auf „ **true** “ fest, um ältere vorab gepatchte AngularJS-Versionen zu verwenden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.angular.legacy*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Die Systemeigenschaft ist ausfallsicher, falls Organisationen von den nicht gepatchten Versionen von AngularJS abhängig sind, um ihre benutzerdefinierten Implementierungen auszuführen.
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Die Verwendung älterer Versionen von AngularJS kann möglicherweise zu Sicherheitsrisiken führen, die durch Angriffe auf Schwachstellen entstehen, die in veralteten AngularJS-Bibliotheksversionen erkannt wurden.
Sicherheitsrisikobewertung	7.1

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Öffentlicher Zugriff auf Favoriten

Verwenden Sie *glide.ui.magellan.favorites.allow_public*, um anzugeben, ob nicht authentifizierte Benutzer **Favoriten** im Navigator anzeigen dürfen.

Öffentlicher Zugriff auf Favoriten ist konform, wenn *glide.ui.magellan.favorites.allow_public* auf „ **falsch**“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.magellan.favorites.allow_public*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Steuern Sie, ob nicht authentifizierte Benutzer **Favoriten** im Navigator anzeigen dürfen.
Typ	wahr/falsch
Empfohlener Wert	*false*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsabhängigkeiten	Legen Sie *glide.ui.magellan.favorites.allow_public* auf **false fest**.
Funktionale Auswirkung	(Mittel) Die Aktivierung dieser Eigenschaft dient als Schutzschicht vor nicht autorisierten Benutzern.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Favoriten erstellen oder anzeigen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Autorisierung für Daten-Broker-REST-API anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.databrokerrestapiprocessor*, um eine Standardautorisierung für alle eingehenden Daten-Broker-REST-API-Anforderungen zu erfordern.

Wenn diese Eigenschaft auf **true**festgelegt ist, wird die Autorisierung angewendet. Wenn dies auf „ **false**“ festgelegt ist, wird keine Autorisierung verwendet, was dazu führen kann, dass vertrauliche Informationen aus Ihrer Instanz weitergegeben werden.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.basicauth.required.databrokerrestapiprocessor*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,6 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „ **falsch**“ festgelegt ist, wird keine API-Authentifizierung angewendet, sodass ein schlechter Akteur auf vertrauliche Daten zugreifen kann.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig mit leeren ACLs verweigern

Verwenden Sie die Eigenschaft *glide.sm.default_mode*, um das Standardverhalten des Sicherheitsmanagers zu steuern, wenn festgestellt wird, dass vorhandene ACL-Regeln Teil der ACL-Regeln der Platzhaltertabelle sind.

Wenn das Plugin „Strenge Sicherheitseinstellungen“ (com.glide.high_security) während der Erstinstallation der Instanz aktiviert wird, wird diese Eigenschaft erstellt, und Platzhalter-ACL-Regeln werden erstellt. Um rollenbasierten Zugriff auf Systemtabellen bereitzustellen, steuern diese Regeln eine erhebliche Anzahl von ACLs und die häufigsten datensatzbasierten Vorgänge:

- Lesen
- Schreiben
- Erstellen
- Löschen

Wenn Sie das High Security-Plugin nicht mit aktivierter Standardverweigerungsoption verwenden, sind viele Tabellen nicht geschützt. Now Platform verwendet ein standardmäßiges Deny-Sicherheitsmodell, das verhindert, dass Nicht-Administratoren auf -Objekte zugreifen, es sei denn, sie erfüllen eine übereinstimmende ACL-Regel. Mit diesem Modell werden viele Angriffsvektoren entfernt, z. B. unsichere Skripts.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sm.default_mode*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Die beste Sicherheitspraxis wäre es, den Zugriff auf die Tabellen durch nicht autorisierte Benutzer einzuschränken. • Wenn keine ACL-Regeln für Tabellen vorhanden sind, stellt diese Eigenschaft sicher, dass mindestens Platzhalter-ACLs für alle CRUD-Vorgänge validiert werden, die für die Tabelle/das Feld ausgeführt werden. • Diese Regeln schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Benutzer hat die Administratorrolle oder erfüllt die Anforderungen einer anderen Tabellen-ACL-Regel.
Empfohlener Wert	verweigern
Funktionale Auswirkung	(Hoch) Wenn Sie diese Eigenschaft auf Zulassen festlegen, **erlauben**die ACL-Regeln der Platzhaltertabelle CRUD-Vorgänge für alle Tabellen, es sei denn, es sind bestimmte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Tabellen-ACL-Regeln vorhanden, um solche Vorgänge einzuschränken. **Hinweis:** Dieses Plugin ist nicht für vorhandene Instanzen gedacht, da es den Sicherheitszugriff auf Tabellen ändern kann, die bereits in einer Produktionsumgebung verwendet werden.
Sicherheitsrisiko	8.8
Referenzen	Standardmäßige Deny-Eigenschaft

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Authentifizierung

Die Authentifizierungskategorie deckt die Hauptelemente der modernen Authentifizierung ab, um zu bestätigen, dass eine Entität und ihre Behauptungen Authentizität und Richtigkeit aufweisen, identitätswechselfest sind und das Abfangen von Passwörtern verhindern.

Der ASVS-Standard basiert auf der Spezifikation NIST 800-63b (https://pages.nist.gov/800-63-3/sp800-63b.html) .

Die Authentifizierung umfasst Passwortrichtlinien, Steuerungen und Speicherung, die ordnungsgemäße Implementierung von Authentifikatoren und die ordnungsgemäße Implementierung von Out-of-Band- oder einmaligen Verifizierern.

Aktivieren Sie die rollenbasierte Multifaktor-Authentifizierung

Verwenden Sie die Eigenschaft `glide.authenticate.multifactor`, um die rollenbasierte Multifaktor-Authentifizierung (MFA) für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den dem Benutzer zugewiesenen Rollen. Wenn einem Anwender in der Multifaktor-Rollenliste die Rollen „admin“, „security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

- Legen Sie diese Eigenschaft auf **„true** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf „ **false** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer zu deaktivieren, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.authenticate.multifactor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer, die bestimmten Rollen zugewiesen sind.
Typ	wahr/falsch
Empfohlener Wert	`true`
Sicherheitsabhängigkeiten	Aktivieren **Sie die rollenbasierte Multifaktor-Authentifizierung** in der **Tabelle „Multifaktor-Kriterien“**.
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft wird die Experience des Benutzers verbessert. Sie fungiert als zusätzliche Schutz- und Sicherheitsebene gegen gefährdete Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht die Gefahr eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Accountwiederherstellung aktivieren [Aktualisiert in Security Center 1.5]

Die Eigenschaft `glide.sso.acr.enabled` steuert die Funktion zur Kontowiederherstellung.

Legen Sie `glide.sso.acr.enabled` auf den empfohlenen Wert von „ **wahr** “ fest, um die Accountwiederherstellung nach Benutzer-ID zu ermöglichen. Legen Sie den Wert auf „ **false** “ fest, um die Accountwiederherstellung nach Benutzer-ID zu verhindern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sso.acr.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Steuert die Funktion „Accountwiederherstellung nach Benutzer-ID“.
Empfohlener Wert	True (Standard)
Konfigurationstyp	Boolean
Sicherheitsrisiko	Kritisch (Ohne Aktivierung dieser Eigenschaft können Anwender ihren Account nicht anhand der Benutzer-ID wiederherstellen.
Sicherheitsrisikobewertung	9.1
Referenzen	Weitere Informationen finden Sie unter Accountwiederherstellung (ACR).

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschleierung der klassischen Mobile-App-UI erforderlich machen

Verwenden Sie die Eigenschaft *glide.ui.m.blur_ui_when_backgrounded*, um alle Felder aus dem Snapshot zu verschleiern, da das Bild während des Hintergrundprozesses gespeichert wird.

Auf Android-Geräten erstellt das Android-Betriebssystem einen Screenshot zur Verwendung im Menü „Letzte Aufgabe“, wenn die Anwendung in den Hintergrund gesendet wird. Benutzer können auch manuelle Screenshots der Anwendung erstellen, die öffentlich auf dem Gerät gespeichert werden.

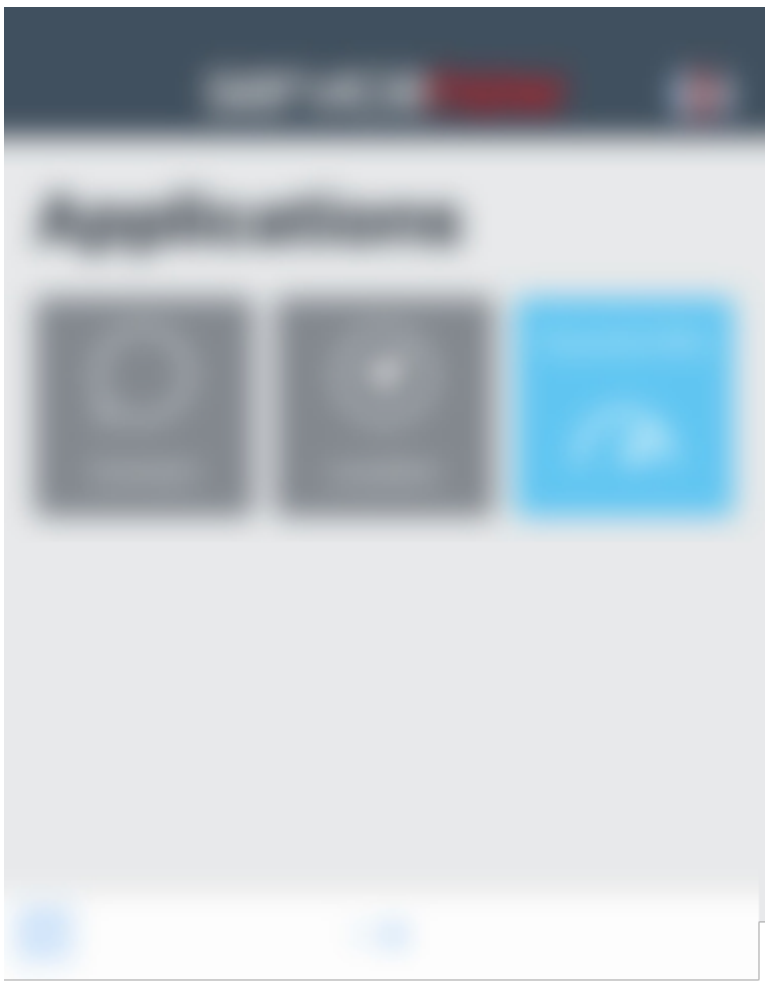
Auf iOS-Geräten ermöglicht das iOS-Betriebssystem Anwendungen auch das Speichern einer Bilddatei. Diese Datei stellt den letzten Bildschirm dar, den der Benutzer gesehen hat, wenn die Anwendung in den Hintergrund gesendet wurde. Dies soll zwar eine bessere Benutzer-Experience bieten, stellt jedoch auch ein Sicherheitsrisiko dar, da die Bilder als PNG-Bilddateien gespeichert werden.

Hinweis:
Diese Einstellung oder Konfiguration ist pro Instanz, daher muss der Benutzer eine Verbindung zur Instanz mit der konfigurierten Eigenschaft herstellen.

Informationen zum Verschleiern aller Felder aus dem Snapshot in der ServiceNow Classic-App finden Sie unter App-Unscharf-Option zur Verbesserung der Sicherheit konfigurieren .

Beispiel

Wenn Sie diese Eigenschaft auf wahr] festlegen, wird die Hintergrundanwendung „b“ für iOS-Geräte verschleiert und für Android-iOS-Geräte gesperrt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaft/Plugin-Name	`glide.ui.m.blur_ui_when_backgrounded`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Um alle Felder aus dem Snapshot zu verschleiern, wenn das Bild während des Hintergrundprozesses gespeichert wird.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	2.4
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft `glide.ui.m.blur_ui_when_backgrounded`] auf truefestgelegt ist, verwenden die nativen Apps den auf dem Server definierten Parameter, um den Bildschirm unscharf zu machen, wenn die App in den Hintergrund wechselt. • Die von iOS und Android aufgenommenen Screenshots werden unscharf, wenn die App in den Hintergrund wechselt. • Die Benutzer-Experience kann beeinträchtigt werden, da sie den Inhalt nicht sehen können, wenn die App in den Hintergrund gesendet wird.
Sicherheitsrisiko	(Mittel) Ein gefährdetes Gerät (mit Jailbreak) ermöglicht einem Angreifer vollständigen Zugriff auf das Dateisystem und den Zugriff auf Dateien/Snapshots mit eingebetteten vertraulichen Informationen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Deaktivieren Sie die Authentifizierung ohne Passwort

Verwenden Sie die Eigenschaft `glide.login.no_blank_password`, um zu verhindern, dass sich Benutzer mit leeren Passwörtern bei der NOW-Plattform anmelden oder das **Passwortfeld** leer lassen.

Selbst wenn der Administrator absichtlich einen leeren Wert oder ein leeres Passwort in Benutzerdatensätzen zuweist, kann sich ein Benutzer nicht anmelden, ohne einen Wert im Feld **Passwort** anzugeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.login.no_blank_password`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um eine starke Authentifizierung sicherzustellen, da der Benutzername innerhalb einer Organisation manchmal leicht zu erraten ist.
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Vorgänge sollten keine leeren Passwörter verwenden, da dies als kritisches Sicherheitsrisiko angesehen wird. Wenn jedoch ein gültiger Fall für eine solche Verwendung vorliegt, besteht die Möglichkeit eines Ausfalls. Benutzer mit leeren Passwörtern können sich nicht bei der Instanz anmelden.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann sich bei der Instanz mit den Standardbenutzernamen oder einer bestimmten Person/Gruppe (normalerweise vorname.nachname) ohne Passwort anmelden. Dies wird als kritisches Sicherheitsrisiko angesehen, da ein öffentlicher Benutzer die Vertraulichkeit und Integrität der Instanzdaten verletzen könnte.

Wenden Sie bei der Anmeldung keine Passwortrichtlinie an

Verwalten Sie, wie die Passwortkomplexität in Ihrer Instanz gehandhabt wird.

Verwenden Sie die Eigenschaft the `glide.apply.password_policy.on_login`, um die Passwortkomplexität zu verwalten. Wenn diese Eigenschaft auf **false**festgelegt ist, wird während der Anmeldung keine Passwortkomplexität erzwungen. Wenn die Option auf „ **true**“ festgelegt ist, wird die Passwortkomplexität erzwungen, was zu Problemen bei der Compliance mit Organisationsrichtlinien führen kann. Anstatt die Passwortkomplexität zu erzwingen, schlägt Application Security Verification Standard (ASVS) vor, eine Mindestlänge von12 Zeichen für die Passwortlänge zu erzwingen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.apply.password_policy.on_login`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,4 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Das Festlegen dieser Eigenschaft auf „ **true** “ kann die Passwortkomplexität erzwingen und zu Compliance-Problemen der Organisation führen.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie die Validierungsprüfung für Passwörter auf der schwarzen Liste

Verwalten Sie die Passwörter auf der schwarzen Liste in der Tabelle „Ausgeschlossenes Passwort“.

Verwenden Sie die Eigenschaft *glide.enable.blacklist_password*, um Passwörter auf der schwarzen Liste zu überwachen. Wenn die Eigenschaft auf **True**festgelegt ist, wird das Passwort des Benutzers mit einer Liste von Passwörtern auf der schwarzen Liste verglichen, wodurch verhindert wird, dass er ein Passwort aus einer Reihe von Passwörtern verwendet, bei denen ein Verstoß vorliegt. Der Administrator kann die Liste verwalten, indem er Passwörter in die Tabelle „Ausgeschlossene Passwörter“ einfügt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enable.blacklist_password*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Authentifizierung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Ausschließen von Passwörtern durch Passwortrichtlinien in Ihrer Instanz

Captcha für die Registrierung externer Benutzer aktivieren [Aktualisiert in Security Center 1.5]

sn_ext_usr_reg.captchaEnabled steuert, ob CAPTCHA für die Registrierung externer Benutzer validiert wird.

Legen Sie *sn_ext_usr_reg.captchaEnabled* auf den empfohlenen Wert **true** fest, um Angriffe bei der automatischen Kontoerstellung zu verhindern, bei denen CAPTCHA für die Registrierung externer Benutzer erforderlich ist. Legen Sie den Wert auf „ **false** “ fest, um CAPTCHA für die Registrierung externer Benutzer nicht zu erfordern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*sn_ext_usr_reg.captchaEnabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Eigenschaft wird verwendet, um die CAPTCHA-Validierung während der Registrierung externer Benutzer in Portalen wie CSP und Community zu aktivieren oder zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	deaktivieren. Dies wird auch in Store-Apps wie VAM und CSM Guest Walkup verwendet, um Captcha zu aktivieren/deaktivieren.
Empfohlener Wert	Wahr
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) Die Eigenschaft steuert die CAPTCHA-Aktivierung bei der Registrierung externer Benutzer. Ein unidealer Wert kann zu Sicherheitsschwachstellen führen.
Sicherheitsrisikobewertung	3.7

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktivieren Sie CAPTCHA in der Passwortzurücksetzung

Verwenden Sie die Eigenschaft *password_reset.captcha.ignore*, um die Notwendigkeit einer CAPTCHA-Abfrage zu aktivieren oder zu deaktivieren, wenn ein Benutzer sein Passwort zurücksetzt.

Legen Sie *password_reset.captcha.ignore* auf den empfohlenen Wert „ **false** “ fest, um eine CAPTCHA-Abfrage für einen Benutzer zum Zurücksetzen des Passworts zu erfordern. Legen Sie den Wert auf **true** fest, um die CAPTCHA-Option für eine Passwortzurücksetzung zu ignorieren.

CAPTCHAs helfen, Automatisierungsangriffe zu verhindern, indem sie den Benutzer zu einer Abfrage/Antwort auffordern, die von automatisierten Systemen nicht einfach beantwortet werden kann. Wenn CAPTCHA deaktiviert ist, kann ein Angreifer bei automatisierten Angriffen auf die Funktion zum Zurücksetzen des Passworts erfolgreicher sein.

Hinweis:
Diese Eigenschaft wird nur für die Automatisierung der Passwortzurücksetzung verwendet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.captcha.ignore*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Eigenschaft wird verwendet, um die CAPTCHA-Validierung während der Passwortzurücksetzung zu aktivieren oder zu deaktivieren.
Empfohlener Wert	false
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Moderat) Ein unidealer Wert kann zu Sicherheitsschwachstellen führen.
Sicherheitsrisikobewertung	5.5

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktivieren Sie E-Mail-OTP für die Multifaktor-Authentifizierung

Verwalten Sie, wie die Zwei-Faktor-Authentifizierung auf Ihre Instanz angewendet wird.

Verwenden Sie die Eigenschaft the *glide.authenticate.multifactor.email.otp.enabled*, um zu steuern, ob ein Token für die Zwei-Faktor-Authentifizierung per E-Mail gesendet wird. E-Mail gilt als schwacher MFA-Faktor, auf den ein Angreifer eher Zugriff erhält, um MFA zu umgehen. Durch Festlegen dieser Eigenschaft auf **false**wird das Risiko reduziert, dass ein Angreifer die MFA umgeht, wenn er das Passwort eines Benutzers gefährdet hat.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.multifactor.email.otp.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	Wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3.1 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf **„false** “ festgelegt wird, wird das Risiko verringert, dass ein schlechter Akteur die Zwei-Faktor-Authentifizierung umgeht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Multifaktor-Authentifizierung mit E-Mail

Aktivieren Sie Richtlinienprüfungen für die Passwortzurücksetzung

Verwenden Sie die Eigenschaft **glide.enable.password_policy**, um Passwortrichtlinienprüfungen zu aktivieren, wenn ein Benutzer sein Passwort über die Benutzeroberfläche ändert.

Informationen zum Definieren der Passwortrichtlinie, die nach Aktivierung dieser Eigenschaft verwendet werden soll, finden Sie unter Passwortrichtlinien für Ihre Instanz aktivieren.

Hinweis:
glide.enable.password_policy gilt nicht, wenn ein Administrator ein Passwort ändert oder einen Benutzer über ein Skript hinzufügt.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.enable.password_policy`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Zum Anwenden der Passwortrichtlinie zum Zeitpunkt der Passwortänderung.
Empfohlener Wert	true (für Passwörter mit höherer Sicherheit)
Sicherheitsrisikobewertung	7.4
Funktionale Auswirkung	(Mittel) Wenn die Eigenschaft auf „true“ festgelegt wird, werden Passwortrichtlinienprüfungen aktiviert, wenn ein Benutzer sein Passwort zurücksetzt.
Sicherheitsrisiko	(Mittel) Ohne eine Passwortrichtlinie kann ein Benutzer ein schwaches Passwort erstellen, was die Wahrscheinlichkeit erhöht, dass ein Angreifer Zugriff auf die Instanz erhält.

Schritte zum Konfigurieren von

Wenn Sie diese Einstellung auf der Seite „Härtungs-Compliance-Konfiguration“ im Instanz-Sicherheitszentrum konfigurieren:

1. Wählen Sie unter **Mittel**die Option **Sitzungsverwaltung**aus.
2. Wählen Sie in der Einstellung **Enable Password Reset Policy Check** (Richtlinienprüfung für Passwortzurücksetzung aktivieren) **Mittel** für Passwörter mit mittlerer Stärke oder **Stark** für robustere Passwörter mit höherer Stärke aus. Wenn Sie eine dieser Optionen auswählen, wird die Eigenschaft **glide.enable.password_policy** auf „true“ festgelegt und ein Workflow gestartet, der Ihre Passwortrichtlinie automatisch aktualisiert.

Darüber hinaus können Sie die Systemeigenschaft `glide.apply.password_policy.on_login` festlegen, um Passwortrichtlinienprüfungen zum Zeitpunkt der Anmeldung zu aktivieren.

Aktivieren Sie SSL in der LDAP-Authentifizierung

Verwalten Sie die Verschlüsselung von LDAP-Authentifizierungsanforderungen in Ihrer Instanz.

Verwenden Sie die Eigenschaft [bisund `glide.ldap.use.ssl`, um die TLS-Verschlüsselung für über das Netzwerk gesendete LDAP-Authentifizierungsanforderungen zu aktivieren oder zu deaktivieren. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, ist die LDAP-Authentifizierung anfällig für Man-in-the-Middle-Angriffe.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ldap.use.ssl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **false**“ festgelegt wird, wird die LDAP-Authentifizierung angreifbar für Man-in-the-Middle-Angriffe.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Aktivieren Sie SSL in der LDAP-Authentifizierung

Minimieren der Ablaufdauer des Links für die Registrierung externer Benutzer [Aktualisiert in Security Center 1.5]

Verwalten Sie die Anzahl der Tage, für die auf einen Registrierungslink zugegriffen werden kann.

Verwenden Sie die Eigenschaft *sn_ext_usr_reg.Reg_link_expiration_days*, um zu verwalten, wer auf einen Registrierungslink zugreifen kann. Wenn der Link auf den empfohlenen Wert **3**festgelegt ist, kann ein Registrierungslink von einer anderen Person als dem beabsichtigten Benutzer verwendet werden, wenn der Link zu einem späteren Zeitpunkt erkannt wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_ext_usr_reg.Reg_link_expiration_days*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	3
Standardwert	3
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: Mittel • CVSS-Punktzahl: 6,6 • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf die Ganzzahl 3 festgelegt wird, kann dies dazu führen, dass der Registrierungslink von einem unbeabsichtigten Benutzer verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Verwaltung fehlgeschlagener Anmeldeversuche

Es sind zwei Skriptaktionen verfügbar, mit denen ein Site-Administrator verwalten kann, wie oft ein Benutzer ein falsches Passwort eingeben kann, bevor er von Now Platformausgesperrt wird. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldeversuche zu verwalten.

Weitere Informationen

Attribut	Beschreibung
Eigenschaft/Plugin-Name	N/V
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Kategorie	Authentifizierung
Zweck	Zum Erzwingen einer strikten Richtlinie für fehlgeschlagene Anmeldeversuche, um ein Brute-Forcing von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur ermöglicht es dem Administrator der Instanz, jeden böswilligen Benutzerzugriff zu überwachen und zu melden. Keine Auswirkungen auf die Funktionalität, nur Änderung der Benutzer-Experience.
Sicherheitsrisiko	(Mittel) Wenden Sie eine definierte Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Schritte zum Konfigurieren von

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen *`*SNC User`*.
3. Um die Verwaltung fehlgeschlagener Anmeldeversuche zu aktivieren, ändern Sie den Status Aktiv der Skriptaktionen *`SNC User Lockout Check with Auto Unlock`* oder *`SNC User Lockout Check`* von **false** in **true**.
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie die Skriptaktion *`SNC User Clear`* aktivieren.

Maximieren Sie die Zeitüberschreitungsdauer beim Entsperren der fehlgeschlagenen Anmeldung

Es sind zwei Skriptaktionen verfügbar, mit denen ein Site-Administrator verwalten kann, wie oft ein Benutzer ein falsches Passwort eingeben kann, bevor er von Now Platformausgesperrt wird. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldeversuche zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.user.unlock_timeout_in_mins`
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Kategorie	Authentifizierung
Zweck	Zum Erzwingen einer strikten Richtlinie für fehlgeschlagene Anmeldeversuche, um ein Brute-Forcing von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur ermöglicht es dem Administrator der Instanz, jeden böswilligen Benutzerzugriff zu überwachen und zu melden. Keine Auswirkungen auf die Funktionalität, nur Änderung der Benutzer-Experience.
Sicherheitsrisiko	(Mittel) Wenden Sie eine definierte Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Schritte zum Konfigurieren von

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen *`*SNC User`*.
3. Um die Verwaltung fehlgeschlagener Anmeldeversuche zu aktivieren, ändern Sie den Status Aktiv der Skriptaktionen *`SNC User Lockout Check with Auto Unlock`* oder *`SNC User Lockout Check`* von **false** in **true**.
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie die Skriptaktion *`SNC User Clear`* aktivieren.

Verschleierung der Mobile-App-UI erforderlich machen

Konfigurieren Sie die Eigenschaft undund `glide.sg.blur_ui_when_backgrounded` so, dass die Benutzeroberfläche der App unscharf ist, wenn die App im Hintergrund ausgeführt wird.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, ist die Benutzeroberfläche der Mobile-App sichtbar, wenn sie über den App-Umschalter angezeigt wird. Die Benutzeroberfläche ist auch dann sichtbar, wenn die App im Hintergrund ausgeführt wird, was für Endbenutzer ein geringeres Maß an Sicherheit und Vertraulichkeit bietet.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sg.blur_ui_when_backgrounded`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	false
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 2,4 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Das Festlegen des Werts auf „ **true** “ bietet ein höheres Maß an Vertraulichkeit und Datenschutz auf dem lokalen Gerät, indem die Benutzeroberfläche unscharf wird, wenn die App im Hintergrund ausgeführt wird.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Mobile-UI-Verschleierung

Benutzer während des Prozesses zum Zurücksetzen/Ändern des Passworts benachrichtigen [In Security Center 1.5 entfernt]

Verwenden Sie diese Anwendung, damit Endbenutzer Passwörter mithilfe eines Selfservice-Prozesses zurücksetzen oder ändern können.

Mit dieser Anwendung kann ein Endbenutzer ein Passwort mithilfe eines Selfservice-Prozesses zurücksetzen oder ändern. Alternativ dazu kann Ihr Unternehmen einen Prozess implementieren, bei dem ein Service Desk-Mitarbeiter Passwörter für Endbenutzer zurücksetzen muss.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`pwd_process.change, pwd_process.reset`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Benutzer bei einer Passwortänderung und/oder -zurücksetzung nicht über die Passwortaktualisierung benachrichtigt werden, kann ein schlechter Akteur diesen Benutzer möglicherweise ohne sein Wissen aus seinem Konto aussperren. Dies würde dem böswilligen Akteur mehr Zeit geben, um böswillige Aktivitäten auszuführen. Stellt sicher, dass der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Prozess zum Zurücksetzen des Passworts Benutzer benachrichtigt, wenn das Passwort geändert oder zurückgesetzt wird.
Abhängigkeiten und Voraussetzungen	Keine

Entfernen Sie die Anmeldeinformationen von der Willkommensseite

Ändern Sie den Standardinhalt auf der Willkommensseite, um die Standardanmeldeinformationen zu entfernen.

Zwei **Anmeldedatensätze** werden als Teil der Demodaten für das CMS-Plugin installiert.

Hinweis:
Wenn Sie die Demodaten für eine Instanz nicht installieren, sind diese Datensätze nicht vorhanden. In diesem Fall wird die Konfiguration gemäß den empfohlenen Sicherheitspraktiken als sicherheitskonform betrachtet.

Weitere Informationen

Attribut	Beschreibung
Name	*How to login*
Konfigurationstyp	Tabelle: sys_home
Kategorie	Authentifizierung
Zweck	Zum Entfernen von Standardanmeldeinformationen von der Willkommensseite, die mit Demodaten hinzugefügt wurden.
Empfohlener Wert	„False“ oder „null“, wenn keine Demodaten verwendet wurden.
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Mittel) Für das CMS-Plugin werden Demodaten bereitgestellt, die zwei Standardpasswörter auf der Willkommensseite enthalten. Wenn dieser nicht entfernt wird, könnte ein nicht autorisierter Angreifer Zugriff auf die Instanz erhalten.
Referenzen	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 Welcome pages

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Minimieren Sie die maximale Anzahl von SMS pro Tag für die Passwortzurücksetzung

Verwalten Sie die maximale Anzahl von SMS-Codes, die pro Tag vom Benutzer zur Überprüfung gesendet werden.

Die Eigenschaftund *password_reset.sms.max_per_day* stellt die maximale Anzahl von SMS-Codes dar, die täglich von einem Benutzer zur Überprüfung gesendet werden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`password_reset.sms.max_per_day`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	10
Standardwert	10
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **10** oder weniger festgelegt ist, ist es einfacher, den SMS-Code zu erzwingen.
Abhängigkeiten und Voraussetzungen	Keine

Minimieren Sie die Ablaufdauer der Anforderung zum Zurücksetzen des Passworts

`password_reset.request.expiry` gibt den Zeitraum in Minuten an, in dem ein Benutzer den Prozess zum Zurücksetzen des Passworts durchführen muss.

Hinweis:
Die Einstellung für die Eigenschaft `password_reset.request.expiry` hat Vorrang vor der Einstellung für die Eigenschaft `glide.pwd_reset.onetime.token.validity`, die einen Standardwert von 12 Stunden hat.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.expiry`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt den Zeitraum in Minuten an, in dem ein Benutzer den Prozess zum Zurücksetzen des Passworts durchführen muss.
Empfohlener Wert	Legen Sie eine Ganzzahl von **10** oder weniger fest. Der Standardwert ist 10.
Konfigurationstyp	Ganzzahlwerte
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 10 oder weniger festgelegt ist, erhöht dies die Wahrscheinlichkeit, dass jemand anderes die Anforderung errät und versucht, das Passwort zurückzusetzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	4.2
Referenzen	Konfigurieren Sie die Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Minimieren Sie den maximalen zulässigen Versuch für die Anforderung zum Zurücksetzen des Passworts

`password_reset.request.max_attempt` wird verwendet, um die maximale Anzahl der Fehlversuche zu steuern, nach denen ein Benutzer sein Passwort zurücksetzen oder ändern kann, bevor er für einen bestimmten Zeitraum ausgesperrt wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.max_attempt`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die maximale Anzahl der nicht erfolgreichen Versuche zum Zurücksetzen des Passworts an, bevor der Benutzer vom Prozess zum Zurücksetzen des Passworts ausgesperrt wird. Die Sperrzeit wird durch den Wert in `password_reset.request.max_attempt_window`bestimmt.
Empfohlener Wert	Auf einen positiven ganzzahligen Wert kleiner als drei festlegen. Der Standardwert ist **3**. Wenn Sie den Grenzwert für den oberen Bereich der Eigenschaft bestimmen, berücksichtigen Sie die Aufgabe, die der Benutzer ausführt.
Konfigurationstyp	Positive ganzzahlige Werte
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert „**3**“ oder einen anderen angemessen kleinen Wert festgelegt ist, kann ein Brute-Force-Angriff auf den Prozess zum Zurücksetzen des Passworts durchgeführt werden.
Sicherheitsrisikobewertung	7.5
Referenzen	Konfigurieren Sie die Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Fensterdauer für maximale Versuche für Anforderung zum Zurücksetzen des Passworts minimieren

Die Eigenschaft `password_reset.request.max_attempt_window` steuert die Anzahl der Minuten, die ein Benutzer warten muss, um sein Passwort zurückzusetzen oder zu ändern, nachdem die maximale Anzahl von Fehlversuchen überschritten wurde, die mit der Eigenschaft `password_reset.request.max_attempt` festgelegt ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.max_attempt_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt den Sperrzeitraum in Minuten an, nachdem die maximale Anzahl nicht erfolgreicher Versuche zum Zurücksetzen des Passworts erreicht wurde.
Empfohlener Wert	Stellen Sie einen positiven ganzzahligen Wert von **1440** oder weniger ein. Der Standardwert beträgt **1440** Minuten.
Konfigurationstyp	Positive ganzzahlige Werte
Funktionale Auswirkung	
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder weniger festgelegt ist, kann Brute-Force für das Konto ausgeführt werden, da das Konto nach einer maximalen Anzahl falscher Authentifizierungsversuche nicht gesperrt wird.
Sicherheitsrisikobewertung	7.5
Referenzen	Konfigurieren Sie die Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Maximieren Sie die Dauer des Wiederholungsfensters für die Anforderung zum Zurücksetzen des Passworts

Die Eigenschaft `password_reset.request.retry_window` steuert die Anzahl der Minuten, bevor die Anzahl der Versuche zum Zurücksetzen des Passworts aktualisiert wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.retry_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die Dauer in Minuten an, bevor die Anzahl der Passwortversuche aus der letzten Anforderung aktualisiert wird, bevor die Anzahl der Wiederholungen auf Null zurückgesetzt wird.
Empfohlener Wert	Stellen Sie einen positiven ganzzahligen Wert von **1440** oder mehr ein. Der Standardwert beträgt **1440** Minuten.
Konfigurationstyp	Positive ganzzahlige Werte.
Sicherheitsrisiko	Hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	7.5
Referenzen	Konfigurieren Sie die Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Minimieren Sie die Dauer des Fensters für die erfolgreiche Anforderung einer Passwortzurücksetzung

Die Eigenschaft *password_reset.request.success_window* steuert die Anzahl der Minuten, die ein Benutzer warten muss, um sein Passwort zurückzusetzen oder erneut zu ändern, nachdem das Passwort erfolgreich zurückgesetzt wurde. Der Anwender kann das Passwort für die angegebene Dauer nicht erneut zurücksetzen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.success_window*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die Zeit in Minuten an, die ein Benutzer nach dem erfolgreichen Zurücksetzen des Passworts warten muss, um das Passwort erneut zurückzusetzen.
Empfohlener Wert	Stellen Sie einen positiven ganzzahligen Wert von **1440** oder weniger ein. Der Standardwert beträgt **1440** Minuten.
Konfigurationstyp	Positive ganzzahlige Werte
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder weniger festgelegt ist, erhöht dies die Wahrscheinlichkeit, dass jemand anderes die Passwortzurücksetzungsfunktion missbraucht, um sich nicht autorisierten Zugriff auf ein Benutzerkonto zu verschaffen.
Sicherheitsrisikobewertung	4.9
Referenzen	Konfigurieren Sie die Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Maximieren Sie die Dauer des Entsperrungsfensters für die Anforderung zum Zurücksetzen des Passworts

Die Eigenschaft *password_reset.request.unlock_window* steuert die Anzahl der Minuten, die ein Benutzer warten muss, um eine Rücksetzanforderung nach der letzten erfolgreichen Aktion zum Entsperren eines Accounts zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.unlock_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die Zeit in Minuten an, die ein Benutzer nach dem erfolgreichen Zurücksetzen des Passworts warten muss, um das Passwort erneut zurückzusetzen.
Empfohlener Wert	Stellen Sie einen positiven ganzzahligen Wert von **1440** oder höher ein. Der Standardwert beträgt **1440** Minuten.
Konfigurationstyp	Positive ganzzahlige Werte
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder höher festgelegt ist, erhöht dies die Wahrscheinlichkeit eines böswilligen Akteurs, den Passwortzugriff mit automatischen Tools zu erzwingen.
Sicherheitsrisikobewertung	5.9
Referenzen	Konfigurieren Sie die Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Maximieren Sie die SMS-Komplexität beim Zurücksetzen des Passworts

Die Eigenschaft `password_reset.sms.default_complexity` steuert die minimale erforderliche SMS-Codeüberprüfungsgröße, die während der Passwortzurücksetzung erforderlich ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.sms.default_complexity`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die Größe der SMS-Codeüberprüfung an, die beim Zurücksetzen des Passworts erforderlich ist.
Empfohlener Wert	Legen Sie eine Ganzzahl von **4** oder größer fest. Der Standardwert lautet 4.
Konfigurationstyp	Ganzzahlwert größer als null
Sicherheitsrisiko	(Niedrig) Wenn die Eigenschaft nicht auf den empfohlenen Wert festgelegt ist, wird ein schwaches SMS-Validierungstoken verwendet. Dies erhöht die Wahrscheinlichkeit des Erratens von Token, was zu einer Kontoübernahme führen kann.
Sicherheitsrisikobewertung	3.8

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Minimieren Sie die Ablaufdauer der SMS für die Passwortzurücksetzung

Steuern Sie die Anzahl der verbleibenden Minuten, bevor der SMS-Code abläuft.

Die Eigenschaftund `password_reset.sms.expiry` stellt die Anzahl der verbleibenden Minuten dar, bis der SMS-Code abläuft.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`password_reset.sms.expiry`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	5
Standardwert	5
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,6 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **5** oder weniger festgelegt ist, steigt die Wahrscheinlichkeit, dass ein schlechter Akteur den SMS-Code errät und zum Zurücksetzen des Passworts verwendet.
Abhängigkeiten und Voraussetzungen	Keine

Maximieren Sie die Dauer des SMS-Pause-Fensters für die Passwortzurücksetzung

Verwalten Sie die Zeit in Minuten, die ein Benutzer warten muss, bevor er einen neuen Code für die Passwortzurücksetzung anfordern kann.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **2** Minuten oder mehr festgelegt ist, kann ein böswilliger Benutzer in einem kurzen Zeitfenster viele Passwortzurücksetzungscodes initiieren. Dies erhöht die Wahrscheinlichkeit, dass ein schlechter Akteur den SMS-Zurücksetzungscode vorhersagt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`password_reset.sms.pause_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	2
Standardwert	2
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,8 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Stellen Sie sicher, dass *password_reset.sms.pause_window* auf einen Wert von 2 oder mehr festgelegt ist.
Abhängigkeiten und Voraussetzungen	Keine

Maximieren Sie die Verzögerungsdauer der Verifizierung der Passwortzurücksetzung

Konfigurieren Sie die Verzögerung in Millisekunden, die ein Benutzer warten muss, bevor eine neue Anforderung zur Passwortzurücksetzung gesendet wird.

Ein schlechter Akteur könnte versuchen, Anmeldeinformationen mithilfe von Automatisierungstools wie Bots zu erzwingen, gegen die die Eigenschaft **„Verzögerung der Passwortzurücksetzung“** hilft. Der Eigenschaftswert stellt die Verzögerung in Millisekunden dar, die ein Benutzer warten muss, bevor er eine Anforderung zum Zurücksetzen des Passworts stellen kann. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **1000** oder mehr festgelegt ist, ist die Anmeldung anfälliger für Brute-Force-Angriffe.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.verification.delay*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	1000
Standardwert	1000
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie den Eigenschaftswert auf weniger als 1000 festlegen, wird Ihre Anmeldung anfälliger für Brute-Force-Angriffe.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Passwort für einen Benutzer konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dauer der SAML-Einschränkung „notBefore“ oder „notOnOrAfter“ minimieren [Aktualisiert in Security Center 1.5]

Konfigurieren Sie diese Eigenschaft, um einen Toleranzzeitraum hinzuzufügen, in dem SAML-Anforderungen und -Antworten als gültig betrachtet werden.

Diese Eigenschaft fügt eine Toleranzfrist hinzu, während der SAML-Anforderungen und -Antworten als gültig betrachtet werden. Der Eigenschaftswert stellt die Anzahl der Sekunden dar, die den Einschränkungen `NotBefore` und `NotOnOrAfter` hinzugefügt werden sollen, um Zeitunterschiede zwischen der Uhr des Identitätsanbieters (IdP) und der Uhr des Service Providers (SP) zu berücksichtigen. Diese Einschränkungen schützen vor Wiederholungsangriffen, indem Anforderungen abgelehnt werden, die nicht innerhalb des angegebenen Zeitrahmens gestellt werden. Wenn sich die IdP- und SP-Uhren erheblich unterscheiden, kann die Netzwerklatenz dazu führen, dass die SAML-Anforderung nicht autorisiert ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.sso.saml2.clockskew`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	60
Standardwert	180
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn der Eigenschaftswert auf oder höher 60 festgelegt wird, können die Einschränkungen möglicherweise nicht gegen Wiedergabeangriffe schützen.
Abhängigkeiten und Voraussetzungen	Keine

Erstellung von Anwendern aus eingehenden E-Mails deaktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.user.trusted_domain`, um die durch Kommas getrennte Liste der vertrauenswürdigen Domänen anzugeben, die bei der Erstellung von Benutzern aus eingehenden E-Mails verwendet wird.

Ein Administrator kann eine E-Mail-Eigenschaft so festlegen, dass Benutzer automatisch aus eingehenden E-Mails erstellt werden. Wenn diese Eigenschaft auf den unsicheren Wert festgelegt ist, erstellt die Instanz automatisch Benutzer aus eingehenden E-Mails. Jeder erstellte Benutzer hat dasselbe hartcodierte Standardpasswort, was die Umgehung der Authentifizierung durch Brute-Force erleichtert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.user.trusted_domain`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Empfohlener Wert	Kommagetrennte Liste der vertrauenswürdigen Domänen [Bsp. servicenow.com (ein bestimmter Domänenname)].
Sicherheitsrisikobewertung	7.4
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, akzeptiert die Instanz nur E-Mails von vertrauenswürdigen Domänen. Wenn Sie die Domäne nicht in die vertrauenswürdige Liste aufnehmen, wirkt sich dies auf Gastbenutzer aus, da Konten automatisch erstellt werden.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer eine E-Mail-Spoofing-/Spam-Kampagne verwenden, um mehrere E-Mails zu senden, was dazu führt, dass weitere unnötige Gastbenutzer erstellt werden.
Referenzen	Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Rollenbasierte Multifaktor-Authentifizierung aktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.authenticate.multifactor`, um die rollenbasierte Multifaktor-Authentifizierung (MFA) für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den dem Benutzer zugewiesenen Rollen. Wenn einem Anwender in der Multifaktor-Rollenliste die Rollen „admin“, „security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

- Legen Sie diese Eigenschaft auf **„true** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf „ **false** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer zu deaktivieren, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.authenticate.multifactor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Benutzer, die bestimmten Rollen zugewiesen sind.
Typ	wahr/falsch
Empfohlener Wert	`true`
Sicherheitsabhängigkeiten	Aktivieren **Sie die rollenbasierte Multifaktor-Authentifizierung** in der **Tabelle „Multifaktor-Kriterien“**.
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft wird die Experience des Benutzers verbessert. Sie fungiert als zusätzliche Schutz- und Sicherheitsebene gegen gefährdete Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht die Gefahr eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Legen Sie die minimale Passwortlänge fest

Legen Sie die Mindestlänge für ein Benutzerpasswort in Ihrer Instanz fest.

Die Eigenschaftund `set.password.length` definiert die Mindestlänge, die für ein Passwort erforderlich ist, und wird verwendet, um die Compliance mit der aktuellen Passwortrichtlinie zu bewerten. Der Eigenschaftswert ist eine Ganzzahl mit einem empfohlenen Mindestwert von **12**. Die Verwendung einer kürzeren Länge kann zu Compliance-Fehlern im Vergleich zu empfohlenen Vorschriften führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`set.password.length`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	12
Standardwert	12
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Das Festlegen der Eigenschaft auf einen kleineren Wert als 12 kann zu Compliance-Problemen führen und erhöht das Risiko, dass ein Angreifer Passwörter erfolgreich erzwingt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Legen Sie die OTP-Lebensdauer für die Passwortzurücksetzung auf maximal 12 Stunden fest

Steuern Sie die Dauer des Links in der Passwortzurücksetzungs-E-Mail.

Diese Eigenschaft lässt den Link in der Passwortzurücksetzungs-E-Mail nach der in der übergebenen Eigenschaft angegebenen Anzahl von Stunden ablaufen. Die Gültigkeit eines Passwortzurücksetzungstokens sollte so kurz wie möglich gehalten werden, ohne die normale Benutzer-Experience zu beeinträchtigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.pwd_reset.onetime.token.validity`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	12
Standardwert	12
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,6 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Eine lange Gültigkeitsdauer des Passwortzurücksetzungstokens erhöht die Wahrscheinlichkeit, dass ein schlechter Akteur eine Kontoübernahme durchführt.
Abhängigkeiten und Voraussetzungen	Keine

Einmalige Lebensdauer der Verifizierung außerhalb des Bereichs minimieren [Aktualisiert in Security Center 1.3]

Verwalten Sie die Zeitdauer für Out-of-Band-Verifizierungen.

Eine Out-of-Band-Verifizierung ist eine alternative Bereitstellungsmethode für Situationen mit einmaligem Code. Zum Beispiel das Zurücksetzen eines Multifaktor-Tokens. Wenn diese Methode von Administratoren im Plugin Multifaktor-Authentifizierung (MFA) aktiviert wird, wird ein Einmalcode per E-Mail zugestellt. Legen Sie einmalige Out-of-Band-Verifizierungen so fest, dass sie nach 10 Minuten ablaufen, um das Gültigkeitsfenster zu begrenzen. Ein größeres Zeitfenster lässt mehr Zeit, damit der Code durch illegale Mittel wie Phishing, Social Engineering oder „Schulter-Surfing“-Angriffe gefährdet werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.multifactor.onetime.code.validity`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	10
Standardwert	10
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,9 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Legen Sie einmalige Out-of-Band-Verifizierungen so fest, dass sie nach 10 Minuten ablaufen. Alles, was länger ist, erhöht das Risiko, dass der Code durch einen schädlichen Akteur gefährdet wird.
Abhängigkeiten und Voraussetzungen	Multifaktor-Authentifizierung (MFA)
Referenzen	Aktivieren Sie das MFA-Plugin

Anforderungen für Geräteverschlüsselung und Passcode erzwingen [Neu in Security Center 1.3]

Die Eigenschaft `glide.sg.device_encryption_enabled` erzwingt die Verschlüsselung nach US-Federal Information Processing Standard (FIPS 140-2). Verschlüsselung und Passcode für Mobilgeräte stellen sicher, dass ein nicht autorisierter Benutzer nicht auf den Inhalt eines Geräts zugreifen kann, auch wenn das Gerät physisch erworben wurde.

Wenn `glide.sg.device_encryption_enabled` auf „true“ festgelegt ist, überprüft die mobile ServiceNow-App, ob die Geräteverschlüsselung und der Gerätepasscode aktiviert sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sg.device_encryption_enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn Verschlüsselung oder Passcode nicht aktiviert ist, kann sich der Benutzer nicht mobil bei der Instanz anmelden
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „true“ festgelegt ist, überprüft die Mobile-App, ob die Geräteverschlüsselung aktiviert ist. Wenn die Verschlüsselung nicht aktiviert ist, können sich Benutzer nicht mobil bei der aktuellen Instanz anmelden.

Autorisierung für XML-Ausgabeanforderungen anfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.basicauth.required.xml`, um anzugeben, ob für eingehende XML-Anforderungen die Basic Authentication erforderlich sein soll.

Weitere Informationen

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.xml`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	So erzwingen Sie die Basic Authentication für XML-Anforderungen.
Sicherheitsrisikobewertung	7.5
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Basic Authentication und Zugriffskontrolle auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von XML-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastbenutzer ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Benutzer erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter XML-Parser-Schritt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung für eingehende XML-Anforderungen kann ein nicht autorisierter Benutzer Zugriff auf vertrauliche Inhalte und Daten in der Zielinstanz erhalten. Stellen Sie sicher, dass `glide.basicauth.required.xml` in der Tabelle „sys_properties“ vorhanden und auf „true“ festgelegt ist.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Captcha für Gast-Walk-up-Experience in der Kundenserviceanwendung anfordern [Aktualisiert in Security Center 1.5]

Das Captcha für die Walk-up-Experience für Gäste verhindert, dass nicht authentifizierte Gastbenutzer Buchungen erstellen, indem Benutzer eine Captcha-Überprüfung durchführen müssen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`sn_guest_walkup_cs.captcha.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Captcha nicht aktiviert ist, kann dies zu einer automatisierten Erstellung von Spam-Terminen führen, um das System zu überfordern oder alle verfügbaren Buchungsplätze zu füllen, was zu einem Denial of Service-Angriff (DoS) führt.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft aktiviert oder deaktiviert das Captcha in den Walk-up-Check-in-Widgets für CSM-Gäste. Standardmäßig ist er auf „true“ festgelegt.

Aktivieren Sie die SMS-Codebenachrichtigung für die Registrierung und Verifizierung

Die Eigenschaftund `password_reset.sms.use_notify` steuert die Verwendung von SMS-Codebenachrichtigungen für die Passwortzurücksetzung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Eigenschaft *password_reset.sms.use_notify* auf den empfohlenen Wert **true**festgelegt ist, wird der Benutzer aufgefordert, das Passwort mithilfe der SMS-Überprüfung und der Registrierung eines neuen Geräts zurückzusetzen, was sicherer als E-Mail ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.sms.use_notify*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Booelan
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „**falsch** “ gesetzt wird, wird E-Mail zur Standardmethode für die Passwortwiederherstellung, die weniger sicher als SMS ist.
Abhängigkeiten und Voraussetzungen	Keine

Geschäftslogik

Diese Kategorie befasst sich mit der Logik und dem Flow, die für jede Anwendung mit allgemeinen Sicherheitsprinzipien eindeutig sind. Stellen Sie insbesondere sicher, dass die beabsichtigte Reihenfolge des Geschäftslogik-Flows nicht umgangen werden kann, dass Grenzen für die Erkennung und Verhinderung automatisierter Angriffe vorhanden sind und dass Schutzmaßnahmen gegen Spoofing, Manipulation, Offenlegung von Informationen und Angriffe zur Erhöhung von Berechtigungen vorhanden sind.

Im Folgenden finden Sie einige Sicherheitskontrollen, die ein Administrator konfigurieren kann, um den nicht autorisierten Zugriff auf vertrauliche Entitäten innerhalb der Now Platform einzuschränken.

Maximale Anzahl von Kommentaren pro Benutzer pro Tag begrenzen

Konfigurieren Sie die Eigenschaft *sn_kb_social_qa.max_comments_per_user_daily*, um die Anzahl der QA-Kommentare pro Tag zu beschränken.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **500** oder weniger festgelegt ist, gibt es keine Beschränkung der Anzahl der QA-Kommentare pro Tag, die zu einer Erschöpfung der Ressourcen führen könnte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_kb_social_qa.max_comments_per_user_daily*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	500
Standardwert	500
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn der empfohlene Wert dieser Eigenschaft nicht auf 500 oder weniger festgelegt wird, gibt es keine Begrenzung für QA-Kommentare pro Tag, was zu einer Erschöpfung der Ressourcen führen kann.
Abhängigkeiten und Voraussetzungen	Keine

Begrenzen Sie die maximale Anzahl von Abonnements pro Benutzer pro Tag

Konfigurieren Sie die Eigenschaft undund *sn_kb_social_qa.max_subscriptions_per_user_daily*, um die maximale Anzahl von Abonnements zu begrenzen, die ein Benutzer an einem Tag abonnieren kann.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **500** oder weniger festgelegt ist, gibt es keine Beschränkung der maximalen Anzahl von F&A-Fragen, die ein Benutzer an einem Tag abonnieren kann. Diese Einschränkung kann zu einer Erschöpfung der Ressourcen führen und die Verfügbarkeit Ihrer Instanz beeinträchtigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_kb_social_qa.max_subscriptions_per_user_daily*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	500
Standardwert	500
Kategorie	Geschäftslogik

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Legen Sie den Eigenschaftswert auf 500 oder weniger fest, um eine Erschöpfung der Ressourcen zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine

SMTP-Empfängeranzahl minimieren [Aktualisiert in Security Center 1.3]

`glide.email.smtp.max_recipients` gibt die maximale Anzahl von Empfängern an, die die Instanz in der Zeile „ **An:** “ für eine einzelne E-Mail-Benachrichtigung auflisten kann.

Legen Sie `glide.email.smtp.max_recipients` auf den empfohlenen Wert von **100 oder weniger fest**. Benachrichtigungen, die diese Grenze überschreiten, erstellen stattdessen doppelte E-Mail-Benachrichtigungen, die an eine Teilmenge der Empfängerliste adressiert sind. Jede E-Mail-Benachrichtigung hat dieselbe maximale Anzahl an Empfängern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.email.smtp.max_recipients`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Geschäftslogik
Zweck	Wenn diese Eigenschaft auf einen unsicheren Wert über dem Standardwert von 100 festgelegt ist, kann in der Instanz eine Denial of Service auftreten.
Empfohlener Wert	Legen Sie eine Ganzzahl kleiner oder gleich 100 fest. Der Standardwert ist 100.
Konfigurationstyp	Ganzzahl
Funktionale Auswirkung	
Sicherheitsrisiko	(Mittel) Benachrichtigungen, die dieses Limit überschreiten würden, erstellen stattdessen doppelte E-Mail-Benachrichtigungen, die an eine Teilmenge der Empfängerliste adressiert sind.
Sicherheitsrisikobewertung	4.9

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Validieren Sie den Remotehost

Legen Sie die Eigenschaft auf „true“ fest, um zu verhindern, dass böswillige Akteure in Ihrem Netzwerk interne Port-Scans verwenden.

Wenn die Eigenschaft Team Development `glide.update_set.remote.check_host` nicht auf den empfohlenen Wert **true**festgelegt ist, lässt die Testfunktion der Remote-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz das Scannen interner Ports zu. Dies ist eine Methode, mit der schlechte Akteure Schwachstellen in einem Netzwerk erkennen können. Es ist dann möglich, alle offenen Ports auf einem bestimmten Host aufzulisten und in einigen Fällen Antwortdaten abzurufen, was zu Informationsverlusten oder nicht autorisiertem Datenzugriff führen kann.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.update_set.remote.check_host`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn die Eigenschaft nicht auf den empfohlenen Wert „ **wahr** “ festgelegt wird, können böswillige Akteure interne Port-Scans verwenden, um sich Zugriff auf nicht autorisierte Daten zu verschaffen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 Define a remote instance

Kommunikation

Diese Steuerung stellt eine ordnungsgemäße Verschlüsselung mit sicheren Algorithmen und Verschlüsselungen sicher. Dies umfasst die Sicherstellung, dass die empfohlene Version von TLS für die Clientkonnektivität verwendet wird, die Verwendung von sicheren Verschlüsselungssuites, die Verwendung vertrauenswürdiger und signierter Zertifikate, die Sicherstellung der Verschlüsselung von Verbindungen zwischen Komponenten und die Protokollierung von Verbindungsfehlern.

Zertifikatvertrauen erzwingen [In Security Center 1.5 entfernt]

Standardmäßig ist die Eigenschaft `com.glide.communications.trustmanager_trust_all` auf **false**festgelegt. Now Platform vertraut nur Zertifikaten, die mit dem JVM-Zertifikatspeicher verifiziert werden können. Selbstsignierten und unternehmenssignierten Zertifikaten wird nicht vertraut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Werte für diese Eigenschaften sind Sichere Überschreibung und können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden). Ändern Sie diesen Eigenschaftswert aus Sicherheitsgründen nicht. Wenn Sie weitere Fragen haben, wenden Sie sich an Kundenservice und Support.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.communications.trustmanager_trust_all`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Kommunikation
Zweck	So erzwingen Sie die Zertifikatvalidierung für ausgehende Anforderungen.
Empfohlener Wert	false
Sicherheitsrisikobewertung	6.6
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt eine strikte Validierung im Feld der Zertifizierungsstelle (Certificate Authority, Zertifizierungsstelle). Wenn eine vertrauenswürdige Entität (CA) das Zertifikat ausgegeben hat, akzeptiert die Instanz es zur weiteren Verwendung.
Sicherheitsrisiko	(Mittel) Aus Gründen der Vertraulichkeit und Integrität sollte die Anwendung die Zertifizierungsstelle des Zertifikats validieren, bevor das Zertifikat für Transaktionsvorgänge verwendet wird.
Referenzen	Zertifikate Verifizierung des HTTP-Client-Hostnamens

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Ausgehende SSLv2-/SSLv3-Verbindungen deaktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.outbound.sslv3.disabled`, um den MID Server zur Verwendung von TLS bei ausgehenden Verbindungen wie REST- und SOAP-Anforderungen zu zwingen. Normalerweise wird für ausgehende Verbindungen einer Instanz die Verwendung von TLS anstelle von SSL erzwungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.outbound.sslv3.disabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Kommunikation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um die Verwendung von TLS für alle ausgehenden Verbindungen von der ServiceNow-Instanz zu erzwingen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Verwendung der TLS-Protokollversion bei der Kommunikation über HTTPS. Wenn Geräte vorhanden sind, die von Kunden/Benutzern der Instanz verwendet werden und die TLS-Kommunikation nicht unterstützen, kann dies zu einem potenziellen Ausfall führen.
Sicherheitsrisiko	(Mittel) Legacy-Versionen von SSL erwiesen sich bei Verwendung für die Implementierung der sicheren HTTP-Shell aufgrund von clientseitigen Angriffen, einschließlich BEAST und SSL-Heartbleed, als unsicher.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Demozertifikate nicht für aktive SAML-Konfigurationen verwenden [Aktualisiert in Security Center 1.5]

Steuern Sie, ob Demozertifikate in Produktions-SAML-Konfigurationen verwendet werden.

Die von ServiceNow bereitgestellten Demozertifikate sollten nicht in SAML-Konfigurationen in der Produktion verwendet werden, da sie für alle Instanzen mit bekannter Passphrase gleich sind. Wenn eine der SAML-Eigenschaften, die einen Zertifikatschlüsselspeicher verwenden, aktiv ist (`require_signed_authnrequest`, `require_signed_logoutrequest`oder `encrypt_assertion`), sollten die Demodaten nicht verwendet werden. Da Demodaten von allen Instanzen gemeinsam genutzt werden, gibt es keine Integritätsgarantie für Anforderungen, die mit gemeinsam genutzten Zertifikaten signiert sind. Daher kann jede vom IdP verschlüsselte Nachricht von einem schädlichen Akteur entschlüsselt werden, wenn er abgefangen wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.sso.saml2.keystore`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	sys_id eines benutzerdefinierten Schlüsselspeichers
Standardwert	leere Zeichenfolge
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: 3,9 • CVSS-Punktzahl: Niedrig
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OCSP-Prüfung bei Netzwerkfehlern erzwingen [Neu in Security Center 1.3]

Erfahren Sie, wie Sie die Eigenschaft *com.glide.communications.httpclient.ocsp_allow_network_error* konfigurieren, um zu verhindern, dass schädliche Akteure OCSP-Prüfungen (Online Certificate Status Protocol) umgehen.

Wenn *com.glide.communications.httpclient.ocsp_allow_network_error* nicht auf den empfohlenen Wert „falsch“ festgelegt ist und bei der OCSP-Prüfung (Online Certificate Status Protocol) ein Netzwerkfehler auftritt (z. B. eine Zeitüberschreitung oder ein Problem beim Abrufen der Sperrinformationen), wird die OCSP-Sicherheitsprüfung umgangen it erfolgreich. Dies könnte es einem Angreifer mit einem widerrufenen Zertifikat ermöglichen, die Public Key-Infrastruktur (PKI) und das Vertrauen in digitale Zertifikate zu durchbrechen, die für das Web von grundlegender Bedeutung sind. Die Verwendung widerrufener Zertifikate ist häufig ein Indikator für böswillige Aktivität, es sei denn, die Server sind nicht synchron.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.communications.httpclient.ocsp_allow_network_er*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	Wahr
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „falsch“ festgelegt wird, kann ein schlechter Akteur die OCSP-Sicherheitsprüfung umgehen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft bestimmt, ob eine Anforderung an die AIA-URI (Online Certificate Status Protocol) im Falle eines Verbindungs- oder Zeitüberschreitungsfehlers zu einem positiven oder negativen Ergebnis führt. Bei „false“ kann der Sperrstatus des vorgelegten Serverzertifikats nicht validiert werden und führt zu einem Kommunikationsfehler mit diesem Endpunkt. Wenn ein Netzwerkfehler auftritt, wenn die Eigenschaft auf den Standardwert true festgelegt ist, wird das Zertifikat aus Sicht der Sperrung als gültig behandelt.

Zertifikatkette und Hostname überprüfen [Neu in Security Center 1.3]

Konfigurieren Sie die Eigenschaft *com.glide.communications.httpclient.verify_hostname*, um Man-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in-the-Middle-Angriffe zu verhindern, indem Sie sicherstellen, dass der Zertifizierungsverifizierungsprozess ausgeführt wird.

Wenn *com.glide.communications.httpclient.verify_hostname* nicht auf **true**festgelegt ist, kann dies Man-in-the-Middle-Angriffe ermöglichen, bei denen die Kommunikation zwischen zwei Parteien abgefangen wird. Wenn diese Eigenschaft auf „false“ festgelegt wird, wird der Zertifikatverifizierungsprozess deaktiviert. Um diese Sicherheitsbedrohung zu beheben, legen Sie *com.glide.communications.httpclient.verify_hostname* auf „ **true** “ fest, um zu verhindern, dass der HTTP-Client eine Verbindung zu einem potenziell schädlichen Hostnamen herstellt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.communications.httpclient.verify_hostname*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: Hoch • CVSS-Punktzahl: 7,4 • Details zum Sicherheitsrisiko: Wenn *com.glide.communications.httpclient.verify_hostname* nicht auf den empfohlenen Wert „true“ festgelegt wird, kann Ihre Instanz für Man-in-the-Middle-Angriffe angreifbar werden.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Überprüft den Hostnamen und die Zertifikatkette, die von Remote-SSL-Hosts (Secure Socket Layer) angegeben werden. Legen Sie diese Eigenschaft auf „true“ fest, um sich vor MITM-Angriffen (Man-in-the-Middle) zu schützen. **Hinweis:** Diese Eigenschaft überschreibt die Eigenschaft *com.glide.communications.trustmanager_trust_all*.

Automatische Übersetzung

Zertifikatwiderruf überprüfen [Neu in Security Center 1.3]

Die Eigenschaft *com.glide.communications.httpclient.verify_revoked_certificate* überprüft die Zertifikatwiderrufung während des TLS-Handshake (Transport Layer Security), um sicherzustellen, dass Sicherheitsprüfungen nicht umgangen werden.

Wenn *com.glide.communications.httpclient.verify_revoked_certificate* nicht auf den empfohlenen Wert **true**festgelegt ist, wird die Zertifikatwiderrufung während

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

des TLS-Handshake nicht überprüft. TLS verschlüsselt Daten, die über das Internet gesendet werden, um sicherzustellen, dass Angreifer keine vertraulichen Informationen wie Passwörter oder Kreditkartennummern sehen können. Das Umgehen des TLS-Handshake stellt ein Sicherheitsrisiko dar, da ein Angreifer mit einem widerrufenen Zertifikat die Bereitstellung eines gültigen Zertifikats vernachlässigen und die Public Key Infrastructure (PKI) und das Vertrauen in digitale Zertifikate brechen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.communications.httpclient.verify_revoked_certif`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn `com.glide.communications.httpclient.verify_revoked_cert` nicht auf den empfohlenen Wert „true“ festgelegt wird, wird die Zertifikatwiderrufung während des TLS-Handshake nicht überprüft.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft sollte auf „true“ festgelegt werden, um sicherzustellen, dass eine TLS-Sitzung (Transport Layer Security) mit einem authentifizierten Endpunkt gestartet wird. Wenn diese Eigenschaft auf „false“ festgelegt ist, wird das Zertifikat nicht überprüft, was die Sicherheit der Instanz gefährden könnte.

Automatische Übersetzung

Konfiguration

Die Konfigurationskategorie stellt sicher, dass Anwendungen über eine sichere Build-Umgebung und gesicherte Bibliothekskomponenten von Drittparteien verfügen. Insbesondere wird sichergestellt, dass eine Build- und Bereitstellungspipeline wiederholbar ist, automatisierte Tests umfasst und die Bereitstellung bekannter Sicherheitsprobleme verhindert. Dazu gehört, dass Abhängigkeiten auf dem neuesten Stand und frei von bekannten Schwachstellen gehalten werden.

Cache-Control-HTTP-Header-Wert [Entfernt in Security Center 1.5]

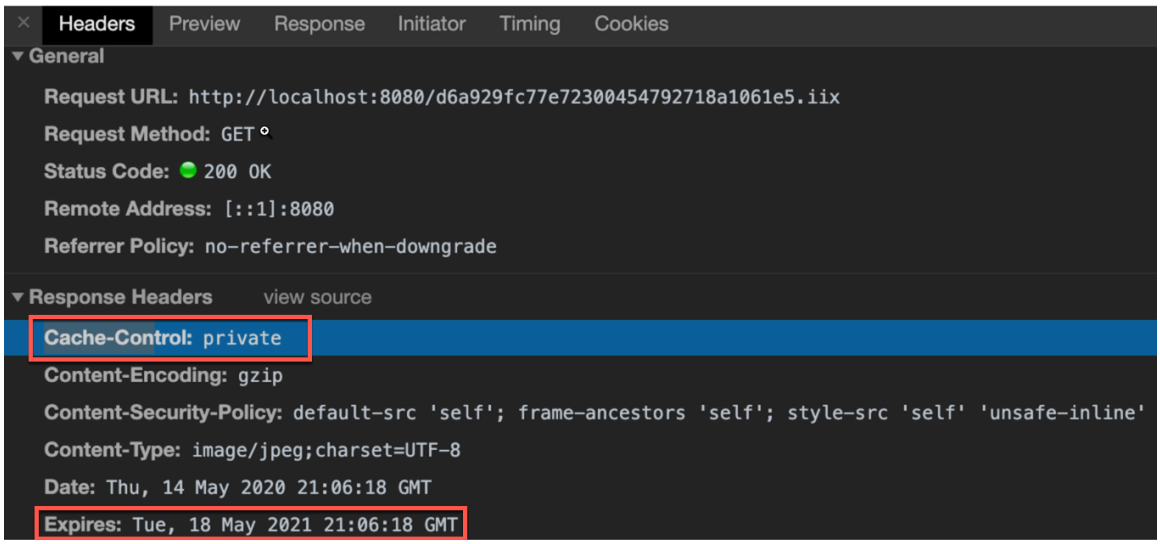
Verwenden Sie die Eigenschaft `glide.http.cache_control`, um den standardmäßigen Cache-Steuerungswert in den HTTP-Antwortkopfzeilen festzulegen, die von Now Platform gesendet werden, wenn statische Inhaltsdaten für eine Seite angefordert werden. Beispiele für statischen Inhalt sind Bilder, CSS und JavaScript, das in für eine Seite gerendert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Eigenschaft `glide.http.cache_control` legt den Standardwert für Cache-Control in HTTP-Antwortheadern auf **private** oder **public**fest. Der Standardwert ist **privat**.

Wert	Beschreibung
Privat	Statische Inhalte können auf Browserebene (Client) zwischengespeichert werden, jedoch nicht auf Proxyserverebene.
Öffentlich	Statische Inhalte können auf Browserebene (Client) und auch auf Proxyserverebene zwischengespeichert werden.

Der Wert für Ablauf in den HTTP-Antwortkopfzeilen steuert, wann der statische Inhalt abläuft. Er hat einen Standardwert von 369 Tagen. Um den Standardwert manuell zu überschreiben, verwenden Sie die Eigenschaft `glide.http.expire.days`.



Hinweis:
Sie können die Eigenschaft `glide.http.cache` verwenden, um festzulegen, ob die Einstellung der Werte für Cache-Steuerung und Ablauf in HTTP-Antwortheadern aktiviert oder deaktiviert werden soll. Der Standardwert ist **true**. Damit können Sie Folgendes festlegen:

- Cache-Control-Wert, Standard unter Verwendung der Eigenschaft `glide.http.cache_control`.
- Läuft standardmäßig mit der Eigenschaft `glide.http.expire.days` ab.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.http.cache_control`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	So konfigurieren Sie den Cache-Control-HTTP-Antwortheaderwert für statischen Inhalt.
Empfohlener Wert	Privat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	(Mittel) Legt den Standardwert für Cache-Control in einem HTTP-Antwortheader fest.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft auf „ **public**“ festlegen, können Instanzen mit CDN/Proxys statischen Inhalt zwischenspeichern und ohne Authentifizierung rendern. • **private** ist eine geeignetere Einstellung für Instanzen mit CDN/Proxy-Setup. • Wenn für die Instanz kein CDN/Proxy eingerichtet ist, sollte einer der Werte in Ordnung sein.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Deaktivieren Sie das Chatserver-Debugging

Aktivieren oder deaktivieren Sie die Systemprotokolle Ihrer Instanz, indem Sie diese Eigenschaft konfigurieren.

Verwenden Sie die Eigenschaft`glide.cs.debug`, um zu verwalten, wie Ihre Instanz Systemprotokolle verarbeitet. Wenn die Eigenschaft auf den empfohlenen Wert **false**festgelegt ist, werden Systemprotokolle nicht aktiviert. Wenn er auf **true**festgelegt ist, sind Systemprotokolle aktiviert. Legen Sie die Eigenschaft nur dann auf „ **true** “ fest, wenn Sie eine Problembehandlung durchführen möchten, und deaktivieren Sie sie, wenn Sie fertig sind. Das Aktivieren von Systemprotokollen kann dazu führen, dass viele Nachrichten generiert werden, wodurch die Systemprotokolle überlastet werden könnten. Protokollnachrichten könnten versehentlich vertrauliche Informationen offenlegen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.cs.debug`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 2,3 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Das Aktivieren von Systemprotokollen kann dazu führen, dass viele Nachrichten generiert werden, die das System mit Protokollnachrichten überlasten könnten, die versehentlich vertrauliche Informationen offenlegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Deaktivieren Sie das Debuggen von gesperrten Formularelementen

Hier ist die Beschreibung für `glide.security.explain.write.locks`.

Legen Sie `glide.security.explain.write.locks` auf den empfohlenen Wert **false fest**, um die Anzeige von Erklärungen zu gesperrten Formularelementen zu verhindern. Legen Sie den Wert auf **true fest**, um die Erklärung der gesperrten Formularelemente anzuzeigen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.explain.write.locks`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Begrenzt das Anzeigeverhalten von SecurityDebugger ohne Abhängigkeit von anderen Eigenschaften.
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) Verhindert die Anzeige der Erklärung für gesperrte Formularelemente. Dadurch wird die Anwendung etwas sicherer, da der Sicherheitsdebugger weniger Informationen bereitstellt.
Sicherheitsrisikobewertung	3.5

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Multisso-Debugging deaktivieren [Aktualisiert in Security Center 1.5]

Die Eigenschaft `glide.authenticate.multisso.debug` steuert die Debug-Protokollierung für Multi-SSO.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.authenticate.multisso.debug`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Deaktiviert Multi-SSO-Debugging.
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Legen Sie die Eigenschaft auf den empfohlenen Wert „Falsch“ fest. Andernfalls ist MultiSSO-Debugging aktiviert, was

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	zu einem unbeabsichtigten Verlust vertraulicher Informationen führen kann.
Sicherheitsrisikobewertung	4.0
Referenzen	SSO-Eigenschaften, -Tabellen und -Skripts für mehrere Anbieter

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Klonen von Zielen nicht zulassen [Neu in Security Center 1.3]

Konfigurieren Sie die Eigenschaft `glide.db.clone.allow_clone_target`, um zu verhindern, dass Ihre Instanz als Klonziel verwendet wird.

Wenn `glide.db.clone.allow_clone_target` nicht auf den empfohlenen Wert „false“ festgelegt ist, kann die Instanz als Klonziel verwendet werden oder ein Datensatz, der die Instanz-URL und die für das Klonen verwendeten Anmeldeinformationen angibt. Ein Systemklon liegt vor, wenn alles in einer Datenbank von einer Instanz in eine andere kopiert wird. Dies stellt ein Sicherheitsrisiko dar, da die Instanzdatenbank beim Klonvorgang überschrieben werden kann, was zu Datenverlust und fehlender Datenintegrität führt. Stellen Sie als Fehlerkorrektur sicher, dass `glide.db.clone.allow_clone_target` auf „false“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.db.clone.allow_clone_target`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	Wahr
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „false“ festgelegt wird, kann die Instanz als Klonziel verwendet werden. Dies stellt ein Sicherheitsrisiko dar, da die Instanzdatenbank beim Klonvorgang überschrieben werden kann.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• System clone • Clone Target Registration and Authentication

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Diese Eigenschaft bietet einen zusätzlichen Schutz, der verhindert, dass in eine Produktionsinstanz geklont wird. Der Standardwert ist „false“ für Produktionsinstanzen und „true“ für Test- und Entwicklungsumgebungsinstanzen wie dev oder qa. Damit eine Instanz als Klonziel verwendet werden kann, legen Sie diese Eigenschaft auf „true“ fest.

Stack-Trace-Anzeige für SOAP-Fehler deaktivieren

Verwalten Sie, wie Stack Traces in Ihrer Instanz angezeigt werden.

Verwenden Sie die Eigenschaft `glide.soapfault.display_stack_trace`, um Stack Traces in Ihrer Instanz zu verwalten. Wenn diese Eigenschaft auf „ **false**“ konfiguriert ist, können vertrauliche Informationen offengelegt werden. Wenn er auf **true**festgelegt ist, wird kein Stack Trace angezeigt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.soapfault.display_stack_trace`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf **„falsch** “ festgelegt wird, können vertrauliche Informationen aus dem Stack Trace verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine

Beschränken Sie den Zugriff auf die Leistungsüberwachung

Verwenden Sie die Eigenschaft `glide.security.diag_txns_acl`, um den Zugriff auf „stats.do“, „threads.do“, „thread_pool_stats“ und „replication.do“ über eine nicht authentifizierte Verbindung zu steuern.

Wenn Sie diese Eigenschaft auf **true**festlegen, ermöglicht die Eigenschaft `glide.security.diag_txns_acl` nur dem Administratorkonto den Zugriff auf Folgendes:

- https://<instancename> .servicenow.com/stats.do
- https://<instancename> .servicenow.com/threads.do
- https://<instancename> .servicenow.com/replication.do
- https://<instancename> .servicenow.com/thread_pool_stats.do

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ohne diese Einstellung zu aktivieren, ist es weiterhin möglich, über eine nicht authentifizierte Verbindung auf diese Ressourcen zuzugreifen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.diag_txns_acl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Beschränken Sie den Zugriff auf Konfigurationsseiten nur auf das Administratorkonto
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt, dass nur der Administratoraccount zu Protokollierungs- und Fehlerbehebungszwecken Zugriff auf vertrauliche Anwendungsdaten erhält.
Sicherheitsrisiko	(Mittel) Vertrauliche Daten wie Serverdetails, Threads und auf dem Server ausgeführte Prozesse sollten für Endbenutzer ohne entsprechende Berechtigungen niemals sichtbar oder zugänglich sein.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktualisierte Version des Multi-SSO-Plugins aktivieren [In Security Center 1.5 aktualisiert]

Stellen Sie sicher, dass Sie v2 des Multi-SSO-Plugins verwenden und dass es auf „true“ festgelegt ist, um Sicherheitsschwachstellen zu reduzieren.

Wenn das Multi-SSO-Plugin in Ihrer Instanz aktiviert ist, sollte die Version v2 sein, und der Wert sollte auf **true**festgelegt sein. Die Versionen vor MultiSSOv2, einschließlich SAML 1.1 und SAML 2.0, entsprechen nicht den Sicherheitsstandards, da sie OpenSAML-Bibliotheksversionen mit bekannten gemeinsamen Schwachstellen und Gefährdungen (CVEs) verwenden. Wenn die bekannten CVEs Sicherheitsbedrohungen in veralteten OpenSAML-Bibliotheken wären, könnte dies einem schlechten Akteur ermöglichen, Nachrichten zu fälschen und die Authentifizierung durch XML-Signatur-Wrapping-Angriffe, Identitätswechsel für Entitäten oder Man-in-the-Middle-Angreifer zu umgehen, um sich nicht autorisierten Zugriff auf eine Instanz zu verschaffen .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.multissov2_feature.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	Wahr
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie den Eigenschaftswert auf „ **false** “ setzen, verwenden Sie frühere Versionen von MultiSSOv2, das OpenSAML-Bibliotheken mit Sicherheitsschwachstellen verwendet. Dies könnte es böswilligen Akteuren ermöglichen, Nachrichten zu fälschen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

Sichere Referrerrichtlinie erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *com.glide.security.referrerpolicy*, um sicherzustellen, dass der HTTP-Header „Referrer-Policy“ die entsprechende Datenebene an jede Seite ServiceNow® sendet, um Datenverluste zu vermeiden.

Wenn die Eigenschaft *com.glide.security.referrerpolicy* auf den Standardwert festgelegt ist, wird sichergestellt, dass der HTTP-Header Referrer-Policy mit der entsprechenden Ebene der gesendeten Informationen verwaltet wird, die speziell auf die Anforderungsseite Now Platform® zugeschnitten ist. Dadurch werden nicht autorisierte Datenverluste verhindert, auf die von anderen Teilen der vollständigen URL aus zugegriffen werden könnte, z. B. vom Pfad und der Abfragezeichenfolge.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.security.referrerpolicy*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Standard
Standardwert	Standard
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Stellen Sie sicher, dass die Eigenschaft

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	`com.glide.security.referrerpolicy` auf den Standardwert festgelegt ist, um die Weitergabe nicht autorisierter Daten zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Referrer-Richtlinie
Funktionale Auswirkung	Diese Eigenschaft steuert, wie viele Informationen über den Referrer-Header gesendet werden, wenn eine Anforderung von einer Seite gesendet wird: • Standard: Instanz übernimmt die Referrer-Header • same-origin: Vollständige Referrer-URL innerhalb der Instanz/gleicher Domäne und ohne Referrer außerhalb des Ursprungs senden • Ursprung: Senden Sie nur den Ursprung als Referrer innerhalb und außerhalb des Ursprungs • Origin-when-Cross-Origin: Vollständige Referrer-URL innerhalb der Instanz/gleicher Domäne senden und nur den Ursprung außerhalb des Ursprungs

Implementieren Sie die Sicherheitskopfzeile x-frame-options: SAMEORIGIN

Verwenden Sie die Eigenschaft `glide.set_x_frame_options`, um den X-Frame-Options-Antwortheader für alle UI-Seiten auf SAMEORIGIN festzulegen.

Verwenden Sie den X-Frame-Options-HTTP-Antwortheader, um anzugeben, ob der Browser eine Seite in `<frame>` oder `<iframe>`rendern darf. Websites können diese Funktion verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihr Inhalt nicht in andere Websites eingebettet wird. Ein Angreifer könnte Ihre Seite in seine eigene Seite einbetten und Ihre Seitenelemente in böswilliger Absicht ausführen. Der Endbenutzer denkt möglicherweise, dass die Seite legitim ist, da sie Ihrer Seite ähnelt. Der Endbenutzer kann wie gewohnt auf Elemente klicken, um schädliche Skripts oder Elemente auszuführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.set_x_frame_options`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Zur Abwehr von ClickJaking-Angriffen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.1
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung für das Rendern einer Now Platform -Anwendung in einer Drittanbieteranwendung in Form eines iFrame. Wenn Sie über

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	eine solche Integration verfügen, wird die Anwendung in der benutzerdefinierten Drittanbieter-App nicht gerendert.
Sicherheitsrisiko	(Mittel) Mit der Richtlinie „Same Origin“ können Sie verhindern, dass eine Domäne ein Skript oder eine Ressource aus einer anderen Domäne abruft. Alle modernen Browser unterstützen diese Funktionalität. Die Richtlinie validiert die Verbindung basierend auf Protokoll, Port und Host. CORS (Cross Origin Request) ist eine Änderung der Richtlinie für denselben Ursprung, die den Zugriff auf Ressourcen/Skripts aus einer anderen Domäne ermöglicht, wenn dies explizit als Teil des Headerwerts angegeben wird. • In diesem Fall steuert die X-Frame-Options-Kopfzeile, ob die Anwendung Now Platform auf der Drittanbieter-Website gerendert werden kann. • Dadurch wird das sensible Risiko reduziert, da der Eigenschaftswert bei Einstellung auf **SAMEORIGIN** das Rendern nicht ermöglicht.
Referenzen	Verfügbare Systemeigenschaften iFrames konfigurieren

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Schreibzugriff erfordern, um auf die Seite „Element hinzufügen“ im Servicekatalog zuzugreifen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.sc.request.add_item_write_access`, um zu verhindern, dass nicht autorisierte Vorgänge für Katalogelemente ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sc.request.add_item_write_access`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn die Eigenschaft `glide.sc.request.add_item_write_access`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	auf „false“ festgelegt ist, kann jeder angemeldete Benutzer auf die UI-Seite „Katalogelement hinzufügen“ zugreifen. Dies kann dazu führen, dass nicht autorisierte Vorgänge für Katalogelemente ausgeführt werden. Um dieses Sicherheitsrisiko zu beheben, legen Sie diese Eigenschaft auf „true“ fest.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn die Eigenschaft „true“ ist, muss der Benutzer im Kontext der UI-Seite Schreibzugriff auf den Datensatz haben.

Xframe-Optionen festlegen, um das Einbetten von Websites von Drittanbietern zu verhindern [Aktualisiert in Security Center 1.3]

Konfigurieren Sie diese Eigenschaft, um zu verhindern, dass der Inhalt einer Webanwendung in eine Drittanbieter-Website eingebettet wird.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **DENY** oder **SAMEORIGIN festgelegt**ist, kann der Inhalt einer Webanwendung mithilfe eines **ALLOW-FROM-** URI in eine Drittanbieter-Website eingebettet werden. Zulassen, dass nicht vertrauenswürdige Websites von Drittparteien Angriffe wie Clickjacking ermöglichen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.cs.embed.xframe_options`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	gleicher Ursprung
Standardwert	gleicher Ursprung
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 3.1 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt wird, kann der Inhalt einer Webanwendung in eine Drittanbieter-Website eingebettet werden, was Angriffe wie Clickjacking ermöglicht.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz

Die Datenschutzkategorie befasst sich mit den Elementen Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Daten.

Die CIA-Komponenten sind:

- Vertraulichkeit: Daten sind während der Übertragung und im Ruhezustand vor nicht autorisiertem Zugriff geschützt.
- Integrität: Daten werden vor nicht autorisierter Erstellung, Löschung oder Änderung geschützt.
- Verfügbarkeit: Daten sind bei Bedarf zugänglich.

„Benutzernamen speichern“ entfernen

Verwenden Sie die Eigenschaft `glide.ui.forgetme`, um das Kontrollkästchen „Benutzernamen speichern“ von der **Anmeldeseite** zu entfernen, um zu verhindern, dass Anmeldeinformationen zwischengespeichert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.forgetme`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datenschutz
Zweck	Um sicherzustellen, dass keine Authentifizierungsinformationen zwischengespeichert werden.
Sicherheitsrisikobewertung	3.5
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Benutzer-Experience ändern, indem sie automatisch von der Instanz abgemeldet wird, wenn ihre Sitzung abläuft. Der Ablauf der Sitzung hängt ausschließlich von dem Wert ab, der in der Systemeigenschaft festgelegt ist, wie in Managing user sessions beschrieben.
Sicherheitsrisiko	(Niedrig) Wenn Sie bei der **Anmeldung** das Kontrollkästchen Benutzernamen speichern aktivieren, wird ein zusätzliches Cookie auf dem Computer des Benutzers gespeichert. • Ihr Zweck besteht darin, die Sitzung für die nachfolgenden Besuche des angemeldeten Benutzers automatisch wiederherzustellen. • Dies stellt ein Sicherheitsrisiko dar, da die Benutzersitzung so lange aktiv bleiben kann, bis sie sich absichtlich abmeldet. Die Wahrscheinlichkeit eines Angriffs für dieses Szenario steigt, wenn der Endbenutzer den Browser unbeaufsichtigt gelassen hat oder wenn er durch einen anderen Angriff gefährdet ist.
Referenzen	Entfernen Sie das Kontrollkästchen Benutzernamen speichern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property

Leeren der Zwischenablage anfordern, wenn mobile Anwendung im Hintergrund ausgeführt wird [Neu in Security Center 1.3]

Die Eigenschaft `glide.sg.clear_pasteboard_when_backgrounded` steuert, ob Text, der aus der mobilen ServiceNow-App kopiert wurde, im Clipper und in der Zwischenablage beibehalten wird, nachdem sich die App im Hintergrundmodus befindet.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sg.clear_pasteboard_when_backgrounded`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, werden vertrauliche Informationen möglicherweise an die Android- oder iOS-Zwischenablage weitergegeben, wo sie anderen Anwendungen auf dem Gerät zur Verfügung stehen können.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft löscht die Zwischenablage für Kopieren und Einfügen, wenn die ServiceNow-App in den Hintergrund wechselt.

HR-Fallaktualisierungen aus persönlichen E-Mails beschränken [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft`sn_hr_core.restrict_guest_email`, um zu steuern, ob ein Benutzer mit seiner persönlichen E-Mail-Adresse auf einen HR-Fall antworten kann.

Wenn die Eigenschaft `sn_hr_core.restrict_guest_email` nicht auf „true“ festgelegt ist, kann ein Benutzer eine E-Mail von einem persönlichen Account senden, der auf den HR-Fall verweist, der in die Arbeitsnotizen aufgenommen werden soll. Dies kann zu geringfügigen Vertraulichkeits- oder Integritätsproblemen führen, wenn die persönliche E-Mail-Adresse gefährdet ist oder die Kommunikation unsicher ist. Ein Administrator möchte möglicherweise die Möglichkeit von Benutzern einschränken, über ihre persönliche E-Mail-Adresse auf HR-Fälle zu antworten, da sie nicht sicher sein können, ob der Benutzer auf das persönliche E-Mail-Konto zugreift.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`sn_hr_core.restrict_guest_email`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „wahr“ festgelegt ist, kann dies zu geringfügigen Vertraulichkeits- oder Integritätsproblemen führen, wenn die persönliche E-Mail-Adresse gefährdet ist oder die Kommunikation unsicher ist.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft steuert, ob eine Antwort von einer persönlichen E-Mail-Adresse einen HR-Fall aktualisiert. Bei Festlegung auf „true“ wird jede Antwort aus einer persönlichen E-Mail den Fallnotizen hinzugefügt. Bei „falsch“ werden der Fall und die Notizen nicht aktualisiert.

oauth-Parameter auf Post-Text beschränken [Neu in Security Center 1.3]

Die Eigenschaft `glide.oauth.allow.parameters.in.post.body.only` steuert die Akzeptanz von Zugriffstoken durch die eingehende OAuth-Authentifizierung. Zugriffstoken sind vertraulich und sollten nur akzeptiert werden, wenn sie sich in einem POST-Anforderungstext befinden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.oauth.allow.parameters.in.post.body.only`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregradpunktzahl: 7,4 • CVSS-Punktzahl: Hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn `glide.oauth.allow.parameters.in.post.body.only` nicht auf den empfohlenen Wert „wahr“ festgelegt ist, befinden sich Zugriffstoken möglicherweise im GET-Anforderungsparameter, der in den Protokollen der Client-Infrastruktur verbleiben kann und möglicherweise zu einer Kontoübernahme führt, wenn diese Protokolle offengelegt werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• OAuth 2.0 • Verwalten Sie OAuth-Token
Funktionale Auswirkung	Stellt sicher, dass der Prozessor oauth_token.do nur POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert.

Fehlerbehandlung und -protokollierung

Die Fehlerbehandlungs- und Protokollierungskategorie befasst sich mit der Qualität und Ausführlichkeit der protokollierten Informationen, die Stakeholdern zur Verfügung stehen.

Dazu gehört es sicherzustellen, dass Protokolle und Fehlermeldungen keine vertraulichen Informationen erfassen, Daten gemäß der Klassifizierung korrekt schützen und eine angemessene Lebensdauer haben. Darüber hinaus bezieht sich diese Kategorie auf die angemessene Fehlerbehandlung und darauf, dass vertrauliche Fehler für Endbenutzer nicht offengelegt werden, z. B. ausführliche Stack Traces für nicht behandelte Ausnahmen mit Sicherheitsauswirkungen.

Deaktivieren Sie die Protokollierung für Benutzer mit geringen Berechtigungen in der Skript-Sandbox

Verwalten Sie die Fähigkeit des Glide-Systems, in der Sandbox-Umgebung ausgeführte Skripts zu protokollieren.

Verwenden Sie die Eigenschaft `glide.security.sandbox_no_logging`, um die Fähigkeit des Glide-Systems zu steuern, in der Sandbox-Umgebung ausgeführte Skripts zu protokollieren. Wenn `glide.security.sandbox_no_logging` auf **false**festgelegt ist, ist die Protokollierung für Benutzer mit geringeren Berechtigungen verfügbar, die Sandbox-Skripts verwenden. Dies stellt eine potenzielle Sicherheitsschwachstelle dar, da Benutzer mit geringen Berechtigungen Protokolle einfügen können, die es einem schädlichen Akteur ermöglichen, einen Angriff potenziell zu verschleiern. Konfigurieren Sie die Eigenschaft auf „ **true“**, um zu verhindern, dass Benutzer mit geringeren Berechtigungen, die ein Sandbox-Skript verwenden, über Protokollierungsfunktionen verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.sandbox_no_logging`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2.2 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **falsch** “ gesetzt wird, wird die Protokollierung für Benutzer mit geringeren Berechtigungen aktiviert, wodurch ein schlechter Akteur einen Angriff verschleiern kann.
Abhängigkeiten und Voraussetzungen	Keine

Deaktivieren Sie das sichere Cookie-Debugging

Verwalten Sie die Protokollnachrichten im Zusammenhang mit Cookies in Ihrer Instanz.

Verwenden Sie die Eigenschaft the *`glide.secure_cookie.debug`*, um Ihre Protokollnachrichten im Zusammenhang mit Cookies zu verwalten. Wenn diese Eigenschaft auf **false**festgelegt ist, werden keine Protokollnachrichten angezeigt. Wenn sie auf **true**festgelegt ist, werden Nachrichten in den Klassen `SecureUserCookie` und `Cookie` protokolliert. Dies kann dazu führen, dass vertrauliche Informationen in Ihrer Instanz verfügbar gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*`glide.secure_cookie.debug`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Die Konfiguration dieser Eigenschaft auf „ **true** “ kann dazu führen, dass vertrauliche Informationen verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL-Fehlermeldungen deaktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.db.loguser*, um die Darstellung von SQL-Fehlermeldungen in einem Browser zu deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.db.loguser*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Fehlerbehandlung und -protokollierung
Zweck	So deaktivieren Sie die Anzeige von SQL-Fehlermeldungen im Browser.
Typ	Wahr|Falsch
Empfohlener Wert	false
Sicherheitsrisikobewertung	3.1
Funktionale Auswirkung	(Niedrig) Diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Dies hat keine Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Mittel) Keine vertraulichen SQL-Informationen, die einem Angreifer helfen könnten, sollten als Teil der Fehlermeldung auf einer Webseite angezeigt werden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

MID-Auditprotokoll aktivieren [Aktualisiert in Security Center 1.5]

Das Audit-Protokoll für MID Server-Befehle zeichnet Details wie den Befehlsnamen, den Befehls-Hash, den Namen der verwendeten Anmeldeinformationen und den Ausführungsstatus auf.

Nach der Aktivierung können Audit-Protokolle von Benutzern mit der Rolle agent_security_admin in der Tabelle ecc_agent_command_audit_log oder durch Navigieren zu angezeigt werden **MID-Server** > **Befehlsauditprotokolle**.

Setzen Sie *mid.log.command_audit.enable* in der Tabelle ecc_agent_property auf „true“, um die Überwachung für vom MID-Server ausgeführte Befehle zu aktivieren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*mid.log.command_audit.enable*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2.2 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Im Falle einer Sicherheitsuntersuchung kann diese Tabelle von Incident-Reaktionsteams verwendet werden, um die auf dem MID-Server ausgeführten Befehle zu prüfen. Ohne dieses Protokoll sind möglicherweise nicht genügend Details vorhanden, um auf Situationen wie die nicht autorisierte Kontonutzung zu reagieren.
Abhängigkeiten und Voraussetzungen	Keine

Plugin „Protected Tables“ aktivieren [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft `com.glide.security.protected_table.enabled`, um zu verhindern, dass Benutzer mit höheren Berechtigungen Protokolltabellen manipulieren.

Wenn die Eigenschaft `com.glide.security.protected_table.enabled` auf **true**festgelegt ist, wird das Plugin „Protected Tables“ verwendet, um zu verhindern, dass Benutzer mit höheren Berechtigungen in einer Instanz Protokolltabellen manipulieren. Die folgenden Protokolltabellen haben besonderen Schutz, wenn diese Eigenschaft auf **true**festgelegt ist:

- syslog (keine DB-Überschreibung)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- geschützt_tabelle_konfiguration (Keine DB-Überschreibung)

Die Integrität von Protokollen ist wichtig für die Bestimmung schädlicher Aktivitäten in einer Instanz durch einen Kundenadministrator.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.security.protected_table.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn *com.glide.security.protected_table.enabled* nicht auf den empfohlenen Wert „true“ festgelegt wird, können Benutzer mit höheren Berechtigungen in einer Instanz Protokolltabellen manipulieren.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Systemprotokolle

Alle ausgehenden HTTP-Anforderungsfelder protokollieren [Entfernt in Security Center v1.3.2]

Konfigurieren Sie die Eigenschaft the *glide.outbound_http.security.log.allow.all.fields* auf „false“, um zu verhindern, dass vertrauliche ausgehende HTTP-Felder im Nur-Text-Format protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **false**festgelegt ist, werden vertrauliche ausgehende HTTP-Felder möglicherweise im Nur-Text-Format protokolliert. Dies kann die Sicherheitslage Ihres Unternehmensnetzwerks beeinträchtigen, da ausgehende Anforderungen mit vertraulichen Daten und Anmeldeinformationen im unverschlüsselten Nur-Text-Format protokolliert und von Benutzern mit geringeren Berechtigungen angezeigt werden können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.outbound_http.security.log.allow.all.fields*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	30
Standardwert	30
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,8 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „ **falsch** “ festgelegt wird, erhöht sich die Wahrscheinlichkeit, dass vertrauliche ausgehende Felder im Nur-Text-Format protokolliert werden, was ein Sicherheitsrisiko darstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung protokollieren

Konfigurieren Sie die Eigenschaft `glide.html_sanitize.discarded_log.enable` , um festzulegen, ob HTML-Bereinigungs-Events in Ihrer Instanz protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, werden HTML-Bereinigungs-Events nicht in der Tabelle `sys_log` protokolliert. Eine fehlende Protokollierung kann sich negativ auf die automatisierten Sicherheitserkennungs- und Untersuchungsfunktionen Ihrer Instanz auswirken.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.html_sanitize.discarded_log.enable`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,4 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, werden HTML-Bereinigungs-Events nicht in der Tabelle `sys_log` protokolliert, was sich auf die automatisierten Sicherheitserkennungs- und Untersuchungsfunktionen auswirken könnte.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Aktivieren der HTML-Bereinigung

Sitzungsaudit-Ereignisse protokollieren [Neu in Security Center 1.3]

Legen Sie die Eigenschaft `glide.authenticate.session_access.log_audit_event` auf **true**fest, damit Sitzungsaudit-Ereignisse in der Tabelle `sys_session_access_audit` erstellt werden.

Das Protokollieren von Informationen über den Sitzungszugriff hilft Ihnen bei der Analyse von Cybersicherheitsangriffen. Zu den protokollierten Informationen gehören Benutzer, Sitzungs-ID (nicht vertraulich), IP-Adresse, Rollen und Richtlinien.

Hinweis:
Die Systemeigenschaft `glide.authenticate.session_access.log_audit_event` ist spezifisch für Zero Trust-Zugriff. Weitere Informationen finden Sie unter Zero Trust-Zugriff.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.session_access.log_audit_event`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt wird, können Events nicht protokolliert werden. Dies könnte verhindern, dass Sie im Falle eines Cyberangriffs schädliche Akteure finden.
Abhängigkeiten und Voraussetzungen	Keine

Benutzeridentitätswechsel protokollieren

Konfigurieren Sie `glide.sys.log_impersonation`, um zu steuern, ob Ereignisse mit Identitätswechsel zu Benutzern in Ihrer Instanz protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, werden Identitätswechsel-Events von Benutzern nicht mehr protokolliert. Das Fehlen der Protokollierung kann sich auf die automatisierten Sicherheitserkennungs- und Untersuchungsfunktionen in Ihrer Instanz auswirken.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sys.log_impersonation`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,4 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „ **true**“ festgelegt ist, werden Identitätswechsel-Events von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Benutzern nicht mehr protokolliert, was sich auf die Sicherheitserkennungs- und Untersuchungsfunktionen Ihrer Instanz auswirken könnte.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Impersonating users

Deaktivieren Sie ausführliche SQL-Fehlermeldungen für den Importprozessor

Konfigurieren Sie diese Eigenschaft, um zu steuern, ob ausführliche SQL-Fehlermeldungen angezeigt werden.

Wenn die Eigenschaft auf **false**festgelegt ist, wird eine ausführliche SQL-Fehlermeldung angezeigt, durch die vertrauliche Informationen verloren gehen können. Um dies zu vermeiden, legen Sie die Eigenschaft auf **„true“** fest, um eine generische Meldung anzuzeigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.import.error_message.generic`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3.1 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „ **false** “ festgelegt wird, werden ausführliche SQL-Nachrichten aktiviert, die zu Informationsverlusten führen können.
Abhängigkeiten und Voraussetzungen	Keine

Datei und Ressourcen

Die Datei- und Ressourcenkategorie stellt sicher, dass Anwendungen nicht vertrauenswürdige Dateidaten sicher verarbeiten und nicht vertrauenswürdige Daten aus nicht vertrauenswürdigen Quellen mit eingeschränkten Berechtigungen an einem geeigneten Speicherort speichern.

Dies umfasst Steuerungen wie das Vermeiden von Denial of Service durch große oder unerwartete Dateitypen, das Validieren des Dateityps und das Verhindern des Pfaddurchlaufs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Download infizierter Dateien nicht zulassen [Aktualisiert in Security Center 1.5]

Verwalten Sie diese Eigenschaft, um zu steuern, ob Stack Traces in Ihrer Instanz angezeigt werden.

Wenn `com.glide.snap.infected_download_allowed` nicht auf den empfohlenen Wert „falsch“ festgelegt ist, kann eine schädliche Datei heruntergeladen werden, die nicht gescannt wurde, was zu einer Infizierung des Desktops des Benutzers führt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.snap.infected_download_allowed`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 6,7 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „false“ festlegen, kann Ihre Instanz dem Herunterladen schädlicher Dateien ausgesetzt sein.
Abhängigkeiten und Voraussetzungen	Keine

Bewertung und Filterung von E-Mail-Spam aktivieren [Aktualisiert in Security Center 1.3]

Installieren Sie das Plugin „E-Mail-Filter“ (`com.glide.email_filter`), um die E-Mail-Filterung innerhalb der Instanz zu installieren. Diese Filterung identifiziert vorhandene Header, sodass Sie basierend auf dem zugeordneten Header entscheiden können, was mit der E-Mail geschehen soll.

Jede Nachricht, die über Now Platform E-Mail-Server gesendet wird, wird auf die Wahrscheinlichkeit geprüft, Spam zu sein.

Hinweis:
Wenn eine Instanz einen privaten E-Mail-Server verwendet, ist dieses Thema nicht anwendbar. Weitere Informationen finden Sie unter Bewertung und Filterung von E-Mail-Spam.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

Legen Sie die Eigenschaft `glide.email.read.active` auf „Wahr“ fest. Weitere Informationen finden Sie unter Eigenen POP3-Server verwenden .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	`com.glide.email_filter`
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Datei und Ressourcen
Zweck	Um die Filterung zu erzwingen, um Spam von E-Mails zu vermeiden.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Niedrig) E-Mails werden im Rahmen der Spam-Bewertung niemals in der Instanz gefiltert, blockiert oder unter Quarantäne gestellt. Sie wird nur bewertet und dann an die Instanz gesendet. Alle Filter werden innerhalb der Instanz mit dem Plugin „E-Mail Filter“ durchgeführt.
Sicherheitsrisiko	(Mittel) E-Mail-Filter ermöglichen es Administratoren, einen Bedingungsgenerator oder ein bedingtes Skript zu verwenden, um anzugeben, wann böswillige eingehende E-Mails von bekannten/unbekannten Absendern ignoriert werden sollen.
Referenzen	E-Mail-Filter https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Activate a plugin .

Aktivieren Sie die Antivirenprüfung

Die Eigenschaft `com.glide.snap.enable_scan` aktiviert die Antiviren-Scan-Funktionalität.

Legen Sie `com.glide.snap.enable_scan` auf den empfohlenen Wert **true** fest, um Antivirus-Scans zu aktivieren.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.snap.enable_scan`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datei und Ressourcen
Zweck	So aktivieren oder deaktivieren Sie Antivirus-Scans für die spezifische Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	True (Standard)
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Antivirus-Scans schützen Ihre Instanz vor Virusinfektionen, die durch Dateianhänge an Ihre Systemdatensätze wie Incidents, Probleme und Storys eingeführt werden können.
Sicherheitsrisikobewertung	7.7

Beschränken Sie herunterladbare Dateitypen in statischen Inhalten

Verwenden Sie die Eigenschaft *glide.ui.strict_customer_uploaded_static_content*, um Einschränkungen für die Dateitypen zu aktivieren, die heruntergeladen werden können, wenn sie mit der Funktion „Datei hochladen“ hochgeladen wurden.

Sie verwenden diese Eigenschaft mit der Eigenschaft *glide.ui.strict_customer_uploaded_content_types*, die eine durch Kommas getrennte Liste mit eingeschränkten herunterladbaren Dateitypen erstellt. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.

⚠ Warnung:
Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.strict_customer_uploaded_static_content*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datei und Ressourcen
Zweck	Um sicherzustellen, dass sichere Dateitypen aus der Anwendung heruntergeladen werden dürfen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	3.1
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung von Dateidownloads basierend auf den in der Eigenschaft *glide.ui.strict_customer_uploaded_content_types* angegebenen Werten. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.
Sicherheitsrisiko	(Niedrig) Dateidownload-Einschränkungen sollten auf alle nicht vertrauenswürdigen Benutzereingabequellen angewendet werden.

Begrenzen Sie die Anhangsgröße in Trainings- und Vorhersage-Flows für GraphQL-Endpunkte

Die Eigenschaft *glide.platform_ml_di.max_attachment_size_graphql* steuert die maximal zulässige Größe für die Rückgabe von Anhängen in GraphQL-Endpunkten von Trainings- oder Vorhersage-Flows.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.platform_ml_di.max_attachment_size_graphql`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	5.242.880
Standardwert	5.242.880
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert von 5.242.880 oder weniger festgelegt ist, kann die Rückgabe großer Dateien zu einem Denial of Service (DoS) führen.
Abhängigkeiten und Voraussetzungen	Keine

Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen [Aktualisiert in Security Center 1.5]

Die Eigenschaft `glide.platform_ml_di.max_attachment_size` steuert die maximal zulässige Größe für die Rückgabe von Anhängen in Trainings- und Vorhersage-Flows.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.platform_ml_di.max_attachment_size`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	4.000.000
Standardwert	4.000.000
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn `glide.platform_ml_di.max_attachment_size` nicht auf den empfohlenen Wert von 4.000.000

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	oder weniger festgelegt ist, kann die Rückgabe großer Dateien einen Denial-of-Service-Angriff (DoS) verursachen.
Abhängigkeiten und Voraussetzungen	Keine

Größe des HTTP-Antworttexts begrenzen [Aktualisiert in Security Center 1.5]

Konfigurieren Sie die Eigenschaften *glide.http.response.get_body.limit.enabled* und *glide.http.response.get_body.limit*, um Ihre Instanz vor *OutOfMemoryExceptions*zu schützen.

Die Eigenschaften *glide.http.response.get_body.limit.enabled* und *glide.http.response.get_body.limit* wurden eingeführt, um neue Funktionen zu aktivieren, die verhindern, dass *OutOfMemoryExceptions* aufgrund einer zu großen Anforderungsantwort ausgelöst werden. *OutOfMemoryExceptions* können Denial-of-Service-Angriffe (DoS) sowie andere Probleme verursachen, die Angreifern dabei helfen können, eine Instanz zu gefährden.

Um Ihre Instanz vor diesen Sicherheitsschwachstellen zu schützen, stellen Sie sicher, dass *glide.http.response.get_body.limit.enabled* auf „true“ festgelegt ist und *glide.http.response.get_body.limit* nicht mehr als 524.288.000 Megabyte (500 MB) beträgt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.http.response.get_body.limit.enabled* und *glide.http.response.get_body.limit*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 6,4 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaften nicht auf die empfohlenen Werte festlegen, wird Ihre Instanz möglicherweise angreifbar für *OutOfMemoryExceptions* und Denial-of-Service-Angriffe.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft reduziert die Wahrscheinlichkeit einer *OutOfMemoryException*, wenn ein Kunde versehentlich eine große Datei in den Speicher lädt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Begrenzen Sie die maximale Anzahl von Anhängen in E-Mails

Konfigurieren Sie die Anzahl der eingehenden E-Mail-Anhänge in Ihrer Instanz.

Die Eigenschaftund `glide.email.inbound.max_attachment_count` steuert die maximale Anzahl eingehender E-Mail-Anhänge in Ihrer Instanz. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **30** oder weniger festgelegt ist, können eingehende E-Mails zu einer Verschlechterung der Instanzleistung führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.email.inbound.max_attachment_count`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	30
Standardwert	30
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Das Festlegen des Eigenschaftswerts auf mehr als 30 kann zu Verschlechterungsproblemen führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Email properties

Minimieren Sie die zulässige Anhangsgröße

Konfigurieren Sie die Eigenschaft `com.glide.attachment.max_size`, um die maximale Größe zu steuern, die für einen hochgeladenen Anhang zulässig ist.

Diese Eigenschaft steuert die maximale Größe eines hochgeladenen Anhangs. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **1024** oder weniger festgelegt ist, kann die Plattform große Dateien akzeptieren, die den Speicher füllen und zu einem DoS-Angriff (Denial of Service) führen könnten.

Hinweis:
Eine tatsächliche Anhangsgröße wird berechnet, indem 1024 x 1024 mit dem Wert der Eigenschaft multipliziert wird. Wenn der Wert der Eigenschaft **1024**lautet, beträgt die maximal zulässige Größe für einen Anhang 1 GB.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.attachment.max_size`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	integer
Empfohlener Wert	1024
Standardwert	4096
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf **maximal 1024** festgelegt ist, akzeptiert die Plattform möglicherweise große Dateien, die zu einem DoS-Angriff führen können.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Attachment limit properties

MIME-Typ der Datei im SOAP Web Service „AttachmentCreator“ validieren [Neu in Security Center 1.3]

Die Eigenschaft `glide.attachment.enforce_security_validation` bestimmt, ob MIME-Dateien (Multifunktions-Internet-Mail-Erweiterungen) einer Validierung unterzogen werden.

Wenn `glide.attachment.enforce_security_validation` nicht auf den empfohlenen Wert **true**festgelegt ist, erfolgt keine Validierung für MIME-Dateien, sodass schädliche Dateien mit falschen Dateierweiterungen hochgeladen werden können. Wenn diese Eigenschaft auf **true**festgelegt ist, werden Dateien mit der richtigen Dateierweiterung hochgeladen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.attachment.enforce_security_validation`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „false“ festgelegt ist, werden MIME-Dateien während des Uploads nicht validiert. Dadurch könnten schädliche Dateien getarnt werden, indem ihre Dateierweiterung geändert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
Funktionale Auswirkung	Legen Sie diese Härtungseinstellung auf „true“ fest, um MIME-Typ- und Dateierweiterungsvalidierungen für hochgeladene Dateianhänge auszuführen. Wenn diese Eigenschaft auf „false“ festgelegt ist, werden keine Validierungen ausgeführt. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt.

Böswilliger Code

Die Kategorie „Böswilliger Code“ stellt sicher, dass alle Anstrengungen unternommen werden, um sicherzustellen, dass Ihr Code frei von Schwachstellen und unerwünschten Funktionen ist.

Dies umfasst die Sicherstellung einer sicheren und ordnungsgemäßen Behandlung böswilliger Aktivitäten, keine zeitbasierten Angriffe, keine ausgehende Kommunikation an nicht vertrauenswürdige Ziele und dass kein nicht autorisierter oder von Angreifern kontrollierter Code enthalten ist. Diese Kategorie enthält Audit- oder Bibliotheken von Drittanbietern aus der Anwendungscodebasis.

Gerootete Mobilgeräte oder Mobilgeräte mit Jailbreak blockieren

Sichern Sie Ihre Instanz, indem Sie nicht autorisierten Zugriff von Geräten mit Jailbreak verhindern.

Verwenden Sie die Eigenschaft `glide.sg.allow_rooted_jailbroken_device` , um Ihre Instanz vor dem nicht autorisierten Zugriff durch Geräte mit Jailbreak zu schützen. Wenn ein Benutzer versucht, sich mit einer Mobile-App bei einer Instanz zu authentifizieren, während diese Eigenschaft auf „ **false**“ festgelegt ist, erhält er die folgende Warnung: Auf diesem Gerät wurde anscheinend ein Jailbreak durchgeführt, und es kann nicht für den Zugriff auf diese Instanz verwendet werden. Wenden Sie sich an Ihren ServiceNow-Administrator. Die App ist eingefroren, während die Warnmeldung angezeigt wird. Die einzige Möglichkeit, diese Meldung zu schließen, besteht darin, **Abmelden**zu wählen. Wenn diese Eigenschaft auf „ **true** “ festgelegt ist, authentifizieren sich Benutzer bei einer Instanz mit einem Gerät mit Jailbreak.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sg.allow_rooted_jailbroken_device`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Böswilliger Code
Sicherheitsrisiko	• Schweregradpunktzahl: 4,5 • CVSS-Punktzahl: Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Der Mangel an Sicherheit auf Geräten mit Jailbreak macht sie zu einem Hauptziel für böswillige Akteure. Wenn nicht autorisierte Entitäten auf Unternehmensdaten zugreifen, kann dies die Sicherheitslage eines Unternehmensnetzwerks schwächen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Zugriffssteuerung

Root of Trust für ServiceNow deaktivieren [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft *com.snc.csf.servicenow_root_of_trust.disabled*, um zu steuern, welchen Build-Schlüsselzertifikaten in einer Instanz vertraut wird.

Wenn die Eigenschaft *com.snc.csf.servicenow_root_of_trust.disabled* nicht auf den empfohlenen Wert „true“ festgelegt ist, wird Signaturen in der Tabelle *sn_kmf_record_signature* mit ServiceNow-Build-Zertifikaten in der Instanz vertraut. Wenn die Eigenschaft auf „true“ festgelegt ist, werden nur Signaturen mit Kundenzertifikaten als vertrauenswürdig eingestuft. Instanzadministratoren sollten nur ihren eigenen Zertifikaten vertrauen, da dies die Sicherheitsauswirkung verringert, wenn der Build-Schlüssel und die Zertifikate von ServiceNow gefährdet sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.snc.csf.servicenow_root_of_trust.disabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Böswilliger Code
Sicherheitsrisiko	• Schweregradpunktzahl: 4 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt ist, wird Signaturen in der Tabelle *sn_kmf_record_signature* mit ServiceNow-Build-Zertifikaten in der Instanz vertraut. Dies erhöht die Sicherheitsauswirkung für den Fall, dass ein ServiceNow-Build durch einen fehlerhaften Akteur gefährdet wird.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft aktiviert oder deaktiviert ServiceNow Root of Trust.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur für Anwendungskonfigurationsdaten und Skripts aktivieren [In Security Center 1.3.2 entfernt]

Verwalten Sie die Codesignatur für Anwendungskonfigurationsdaten und Skripts in Ihrer Instanz.

Codesignatur kann zur Verbesserung der Sicherheit beitragen, indem vertrauliche Anwendungskonfigurationsdaten und Skripts validiert werden, bevor sie verwendet werden. Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Diese Überprüfung verhindert, dass schädliche Daten oder Skripts in der Instanz verwendet werden, was zu einer vollständigen Gefährdung der Instanz führen kann.

Verwenden Sie die Eigenschaft the `com.snc.kmf.signature.validation.flag`, um die Codesignatur für Anwendungskonfigurationsdaten und -skripts zu verwalten. Wenn diese Eigenschaft auf „ **true**“ festgelegt ist, wird die Codesignatur für Anwendungskonfigurationsdaten und Skripts aktiviert.

> **Warnung:**
> Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.snc.kmf.signature.validation.flag`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Böswilliger Code
Sicherheitsrisiko	• Schweregradpunktzahl: 6 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **true** “ festgelegt wird, wird die Codesignatur aktiviert, was zur Verbesserung der Sicherheit beiträgt, indem vertrauliche Anwendungskonfigurationsdaten und Skripts validiert werden.
Abhängigkeiten und Voraussetzungen	Keine

Sitzungsverwaltung

Diese Kategorie befasst sich mit der Sicherheit des Anwendungsstatus für einen Benutzer. Sitzungen sollten für jede Person eindeutig sein, nicht erraten oder geteilt werden können und nach Zeiträumen der Inaktivität oder wenn sie nicht erforderlich sind, für ungültig erklärt werden. Dies umfasst Faktoren wie Cookie-Attribute für Cookie-basierte Sitzungen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Generierung und Speicherung von Sitzungstoken und Anforderungen für die erneute Verbundauthentifizierung.

Minimieren Sie die absolute Zeitüberschreitungsdauer der Sitzung

Verwenden Sie die Eigenschaft *glide.ui.user_cookie.max_life_span_in_days*, um eine maximale Lebensdauer für Benutzercookies festzulegen, die erstellt werden, wenn sich Benutzer mit dem Kontrollkästchen „Benutzernamen **speichern** “ anmelden. Wenn das **Cookie** abläuft, müssen sich Benutzer, die das Kontrollkästchen „Benutzernamen speichern“ aktiviert haben, erneut bei der Instanz authentifizieren.

Dadurch bleibt das Benutzer-Cookie für die Dauer der angegebenen Tage gültig, beginnend mit der ersten Ausgabe des Cookies. Der Standardwert beträgt 30 Tage, die maximale Obergrenze liegt bei 365 Tagen.

Hinweis:
Informationen zum Erzwingen einer maximalen Sitzungszeit für aktive Benutzersitzungen finden Sie unter Managing user sessions .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.user_cookie.max_life_span_in_days*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Sitzungsverwaltung
Zweck	Um Benutzer, die das Kontrollkästchen „Benutzernamen speichern“ aktiviert haben, nach bestimmten Tagen zur **erneuten** Authentifizierung zu zwingen.
Empfohlener Wert	Kleiner oder gleich 30
Standardwert	30 Tage
Funktionale Auswirkung	(Mittel) Diese Eigenschaft erzwingt eine obligatorische erneute Anmeldung, indem jegliche Art von Cookie-Rotation nach einem bestimmten Zeitraum vermieden wird.
Sicherheitsrisikobewertung	4.2
Sicherheitsrisiko	(Mittel) Die Benutzercookies, die für eine unbegrenzte Zeit aktiv sind, stellen ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Ändern Sie die Einstellungen für das Kontrollkästchen Benutzernamen speichern und Cookies

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Rollen für Zeitüberschreitungsausnahmen für aktive Sitzungen definieren [Neu in Security Center 1.3]

Die Eigenschaft *glide.active.session.timeout.exception.roles* steuert die Rollen, die von einer Zeitüberschreitung für aktive Sitzungen ausgenommen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zeitüberschreitung für aktive Sitzungen stellt sicher, dass eine angehaltene Sitzung nicht unbegrenzt verwendet werden kann, ohne die Authentifizierungsinformationen erneut anzugeben. Um dieses Sicherheitsrisiko zu beheben, stellen Sie sicher, dass die Eigenschaft `glide.active.session.timeout.exception.roles` auf **„edge_encryption, mid_server“ festgelegt ist**.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.active.session.timeout.exception.roles`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Edge_encryption, mid_server
Standardwert	Edge_encryption, mid_server
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Berücksichtigt nur eine Ausnahme für die Zeitüberschreitung für aktive Sitzungen für interne Integrationskontorollen. Wenn eine Rolle eine Ausnahme von der Sitzungszeitüberschreitung erhält und diese Rolle einem Benutzer zugewiesen wird, der Opfer eines Hijacking-Angriffs auf die Sitzung wird, kann sich ein Angreifer unbegrenzt bei dieser Sitzung authentifizieren. Dies kann die Auswirkungen eines Security Incident erhöhen, da ein Angreifer mehr Zeit hat, um ein gekapertes Konto auszunutzen.
Abhängigkeiten und Voraussetzungen	Keine

Aktivieren Sie UserCookie Version 3.1

Verwalten Sie die Version von UserCookie, die in Ihrer Instanz aktiviert ist, um die Speicherung des geheimen Schlüssels im Quellcode zu sichern.

UserCookie v3 wird nur generiert, wenn die Eigenschaft `glide.ui.secure.cookies.use_kmf`deaktiviertist. UserCookie v3 ist nicht sicher, da der geheime Schlüssel für Hash-basierte Nachrichtenauthentifizierungscodes (HMAC) im Quellcode gespeichert wird, der für alle Kunden identisch ist. Ein schlechter Akteur kann einen geheimen Schlüssel verwenden, um zu versuchen, Benutzersitzungen zu kapern. Um diese Sicherheitsbedrohung zu beheben, stellen Sie sicher, dass die Eigenschaft `glide.ui.secure.cookies.use_kmf` auf „ **true** “ festgelegt ist, wodurch UserCookie v3.1 verwendet wird. Der geheime Schlüssel wird in einem sicheren Speicher wie KMF gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ui.secure.cookies.use_kmf`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Option auf „ **falsch** “ gesetzt wird, stellt dies eine Sicherheitslücke dar, da der geheime Schlüssel für Hash-basierte Nachrichtenauthentifizierungscodes (HMAC) im Quellcode gespeichert ist.
Abhängigkeiten und Voraussetzungen	Keine

Passwortzurücksetzung für API-Anforderungen erzwingen

Verwalten Sie, wie die Passwortzurücksetzungs-Funktion in Ihrer Instanz funktioniert.

Wenn ein Benutzer für **„Passwort muss zurückgesetzt“**markiert ist, muss er beim nächsten Authentifizierungsversuch ein neues Passwort angeben. Diese Eigenschaft steuert, ob die Passwortzurücksetzung vor API-Aufrufen obligatorisch ist. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können Benutzerkonten, die als **Passwort muss zurückgesetzt** markiert sind, weiterhin Vorgänge ausführen, indem sie die Tabellen-API über die Basic Authentication abfragen. Diese Sicherheitslücke kann zu Informationsverlusten führen, wenn ein inaktives Konto gefährdet ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.api.user.reset_password.mandatory`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Das Festlegen dieser Eigenschaft auf „ **falsch** “ kann zu Informationsverlusten führen, wenn ein inaktives Konto gefährdet ist.
Abhängigkeiten und Voraussetzungen	Keine

Kennzeichnung für „Nur-HTTP-Cookie“ aktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.cookies.http_only`, um das HTTPOnly-Attribut für vertrauliche Cookies zu aktivieren.

Verwenden Sie das Attribut HTTPOnly, um Angriffe wie websiteübergreifendes Skripting zu verhindern, da es keinen Zugriff auf das Cookie mit einem clientseitigen Skript wie JavaScript zulässt. Dadurch werden nicht die Risiken von websiteübergreifendem Skripting eliminiert, aber einige Ausnutzungsvektoren eliminiert.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.cookies.http_only`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Sitzungsverwaltung
Zweck	Um das Risiko eines clientseitigen Skripts zu verringern, das auf das geschützte Cookie zugreift.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt ein zusätzliches HTTPOnly-Flag in Sitzungscookies hinzu und schützt sie so vor Diebstahl. • Wenn Sie über benutzerdefinierte Funktionen verfügen, die JavaScript für den Zugriff auf das Cookie des Benutzers erfordern, wird diese Funktionalität beeinträchtigt. Unter normalen Umständen sollte dies nicht der Fall sein. • Now Platform behandelt die Sitzungsverwaltung, und es sollte keinen Grund geben, warum ein benutzerdefiniertes Skript auf die Cookies des Benutzers zugreift.
Sicherheitsrisiko	(Mittel) Sitzungscookies in der Anwendung authentifizieren einen Endbenutzer und stellen implizite Zugriffsberechtigungen für die Anwendung bereit. Das bedeutet, dass sie vor Diebstahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	oder Export geschützt werden müssen. Kennzeichnungen vom Typ „Nur HTTP“ schützen die Sitzungscookies vor JavaScript-Injektionen oder websiteübergreifenden Skripting-Schwachstellen, die sie stehlen.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Anzahl gleichzeitiger interaktiver Sitzungen minimieren [Aktualisiert in Security Center 1.3]

Verwenden Sie diese Eigenschaft mit dem Plugin „Gleichzeitige Sitzungen begrenzen“, um die Anzahl der aktiven Sitzungen zu steuern, die von einem Benutzer geöffnet werden können.

Verwenden Sie die Eigenschaft **Glide Authenticate Max Concurrent Interaktive Sitzungen** mit dem Plugin „ **Gleichzeitige Sitzung begrenzen** “ (`com.glide.limit.concurrent.sessions`), um die Anzahl der aktiven Sitzungen zu steuern, die für einen Benutzer geöffnet sind. Der empfohlene Wert ist **1**, wodurch die Anzahl der geöffneten Sitzungen reduziert wird (eine höhere Zahl erhöht die Wahrscheinlichkeit, dass eine Sitzung angegriffen werden könnte).

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.max.concurrent.interactive.sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1
Standardwert	1
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn der Standardwert der Eigenschaft größer als 1 ist, erhöht sich die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen.
Abhängigkeiten und Voraussetzungen	Das Plugin „ **Concurrent Interactive Sessions** “ (`com.glide.limit.concurrent.sessions`) sollte aktiv sein.
Referenzen	Begrenzen Sie gleichzeitige Sitzungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gleichzeitige Sitzungen auf allen Knoten beschränken [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.authenticate.limit.concurrent.sessions.across.all.nodes* mit dem Plugin „Gleichzeitige Sitzungen begrenzen“, um die Anzahl der Sitzungen zu verwalten, die auf allen Knoten nachverfolgt werden.

Wenn das Plugin Begrenzen Sie gleichzeitige Sitzungen aktiv ist, kann die Anzahl der offenen Sitzungen pro Benutzer begrenzt werden. Stellen Sie sicher, dass, wenn dieses Plugin aktiv ist, die Eigenschaft (**Glide-Authentifizieren, gleichzeitige Sitzungen auf allen Knoten begrenzen**) auf „ **true** “ festgelegt ist, damit die Anzahl der offenen Sitzungen für alle Knoten und nicht für einen einzelnen Anwendungsknoten nachverfolgt wird. Wenn diese Eigenschaft auf **false**festgelegt ist, können mehrere Sitzungen auf mehreren Knoten geöffnet sein, was die Wahrscheinlichkeit eines Sitzungs-Hijacking erhöht.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.limit.concurrent.sessions.across.all.n*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie bei Verwendung des Plugins „ **Gleichzeitige Sitzungen** begrenzen“ diese Eigenschaft auf „ **falsch** “ setzen, können mehrere Sitzungen auf mehreren Knoten geöffnet werden, was die Wahrscheinlichkeit einer Sicherheitsschwachstelle wie eines Sitzungs-Hijacking erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Begrenzen Sie gleichzeitige Sitzungen

Plugin „Gleichzeitige Sitzungen begrenzen“.

Konfigurieren Sie das Plugin „com.glide.limit.concurrent.sessions“, um die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen in Ihrer Instanz zu reduzieren.

Mit diesem Plugin kann ein Administrator die Anzahl der aktiven Sitzungen pro Benutzer und/oder Rolle begrenzen. Es wird empfohlen, dieses Plugin zu aktivieren und zu konfigurieren, um die Möglichkeit eines Sitzungs-Hijacking zu reduzieren. Wenn dieses Plugin aktiviert und konfiguriert ist, gibt es ein Limit für die Anzahl der offenen Sitzungen, die angegriffen werden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.limit.concurrent.sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Plugin
Empfohlener Wert	com.glide.limit.concurrent.sessions aktiviert und konfiguriert
Standardwert	com.glide.limit.concurrent.sessions aktiviert und konfiguriert
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn dieses Plugin nicht aktiv ist, besteht eine erhöhte Wahrscheinlichkeit eines Sitzungs-Hijacking.
Abhängigkeiten und Voraussetzungen	Keine

Lebensdauer aktiver Sitzungen des Gasts begrenzen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.guest.active.session.life_span`, um die Dauer der HTTP-Sitzungen eines aktiven Gasts zu steuern.

Die Eigenschaft `glide.guest.active.session.life_span` erzwingt eine maximale Lebensdauer für aktive Gast-HTTP-Sitzungen, unabhängig von deren Sitzungsinaktivität oder der Zeit, in der ein Benutzer inaktiv ist, bevor seine Sitzung abläuft und geschlossen wird. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von 0 wird die Zeitüberschreitung für aktive Sitzungen deaktiviert. Ein höherer Wert könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu bleiben, was die Wahrscheinlichkeit eines Security Incident erhöht. Diese Eigenschaft ist auf Gastbenutzer beschränkt, die geringe Zugriffsrechte für eine Instanz haben.

Um diese Sicherheitsschwachstelle zu beheben, legen Sie `glide.guest.active.session.life_span` auf einen Wert größer als 0 und kleiner oder gleich 720 fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.guest.active.session.life_span`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1-720 (Minuten)
Standardwert	0
Kategorie	Sitzungsverwaltung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn die maximale Lebensdauer auf einen hohen Wert festgelegt wird, erhält ein böswilliger Akteur mehr Zeit in einer Instanz, falls er eine Sitzung storniert.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Konfiguration erzwingt die maximale Lebensdauer aktiver Gast-HTTP-Sitzungen unabhängig von der Zeitüberschreitung inaktiver Sitzungen. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von 0 wird die Zeitüberschreitung für aktive Sitzungen deaktiviert. Die maximale Lebensdauer muss größer sein als die inaktive Zeitüberschreitung `glide.guest.session_timeout` (Standard: 30 Minuten).

Begrenzen Sie gleichzeitige interaktive Sitzungen

Verwalten Sie die Anzahl der interaktiven Sitzungen in Ihrer Instanz.

Verwenden Sie die Eigenschaft the `glide.authenticate.limit.concurrent.interactive.sessions`, um die Anzahl der interaktiven Sitzungen in einer Instanz zu verwalten. Diese Eigenschaft soll mit dem Plugin Begrenzen Sie gleichzeitige Sitzungen(com.glide.limit.concurrent.sessions) verwendet werden. Wenn das Plugin aktiv ist und die Eigenschaft auf „ **false**“ festgelegt ist, kann ein Benutzer eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen in einer Instanz haben. Eine größere Anzahl offener Sitzungen bedeutet eine höhere Wahrscheinlichkeit eines Sitzungs-Hijacking.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.limit.concurrent.interactive.sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn das Plugin aktiv ist und die Eigenschaft auf **„false**“ festgelegt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	ist, kann ein Benutzer eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen haben, was die Wahrscheinlichkeit eines Sitzungs-Hijacking erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Begrenzen Sie gleichzeitige interaktive Sitzungen

Lebensdauer aktiver Sitzungen von Integrationen begrenzen [Neu in Security Center 1.3]

Die Eigenschaft `glide.integrations.active.session.life_span` erzwingt die maximale Lebensdauer aktiver Gast-HTTP-Sitzungen unabhängig von der Zeitüberschreitung inaktiver Sitzungen. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von 0 wird die Zeitüberschreitung für aktive Sitzungen deaktiviert.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.integrations.active.session.life_span`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	0 bis 720
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Eine höhere maximale Lebensdauer könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu verharren, was die Reichweite eines Security Incident erhöht. Diese Eigenschaft ist auf Integrationen beschränkt, die geringe Berechtigungen für eine Instanz haben. Legen Sie die Glide-Eigenschaft `glide.integrations.active.session.life_span` auf einen Wert von 0 und kleiner oder gleich 720 fest.
Abhängigkeiten und Voraussetzungen	Keine

Lebensdauer aktiver UI-Sitzungen begrenzen [Neu in Security Center 1.3]

Die Eigenschaft `glide.ui.active.session.life_span` erzwingt die maximale Lebensdauer aktiver authentifizierter HTTP-Sitzungen unabhängig von der Zeitüberschreitung inaktiver Sitzungen.

Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von 0 wird die Zeitüberschreitung für aktive Sitzungen deaktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ui.active.session.life_span`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1-720
Standardwert	0
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Eine höhere maximale Lebensdauer könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu bleiben, was die Wahrscheinlichkeit eines Security Incidents erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Erzwingt die maximale Lebensdauer aktiver authentifizierter HTTP-Sitzungen unabhängig von der Zeitüberschreitung inaktiver Sitzungen. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von 0 wird die Zeitüberschreitung für aktive Sitzungen deaktiviert. Die maximale Lebensdauer muss größer sein als die inaktive Zeitüberschreitung glide.ui.session_timeout (Standard: 30 Minuten).

Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1.3]

Die Eigenschaft `glide.active.session.timeout.invalidate.session` steuert, ob eine Zeitüberschreitungssitzung vor dem Tomcat-Server proaktiv für ungültig erklärt wird.

Wenn `glide.active.session.timeout.invalidate.session` nicht auf **true**festgelegt ist, kann es ein kurzes Zeitintervall geben, in dem eine Sitzung mit Zeitüberschreitung nicht für ungültig erklärt wird (60 oder mehr Sekunden, abhängig von der Warteschlangengröße). Wenn eine Sitzung angegriffen wird, kann ein Angreifer während dieses kurzen Zeitraums möglicherweise eine Sitzung verwenden. Um dieses Sicherheitsrisiko zu beheben, legen Sie `glide.active.session.timeout.invalidate.session` auf **true**fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.active.session.timeout.invalidate.session`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	false
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,6 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, kann dies dazu führen, dass eine Sitzung mit Zeitüberschreitung nicht validiert wird. Dies erhöht die Wahrscheinlichkeit, dass ein böswilliger Akteur eine Sitzung übernimmt.
Abhängigkeiten und Voraussetzungen	Keine

HTTP-Sitzungsbezeichner rotieren

Verwenden Sie die Eigenschaft `glide.ui.rotate_sessions`, um die Rotation der HTTP-Sitzungsbezeichner zu aktivieren, um Sicherheitsschwachstellen zu reduzieren.

Wenn sich die Sitzungs-ID eines nicht authentifizierten Benutzers nach der Authentifizierung nicht ändert, ist eine Webanwendung angreifbar für einen Sitzungsfixierungsangriff. Ein böswilliger Benutzer könnte eine nicht authentifizierte Sitzung starten und die zugehörige Sitzungs-ID an das Opfer weitergeben. Sobald sich das Opfer authentifiziert hat, gibt der böswillige Benutzer diese authentifizierte Sitzung frei.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.rotate_sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Sitzungsverwaltung
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Durch diese Korrektur wurde die SessionID geändert, wenn der Benutzer von einer nicht authentifizierten Seite zu authentifizierten Seiten navigiert. • Wenn Sie einen Proxy verwenden oder die SessionID hartcodieren, wenn sich ein Benutzer zum ersten Mal anmeldet, oder aus irgendeinem Grund, kann dies potenzielle Auswirkungen auf die Funktionalität haben. • Wenn Sie das SAML 2.0-Plugin für die Single Sign-on-Authentifizierung verwenden, kann dies die gemeinsame Nutzung von Sitzungsinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	zwischen der Instanz und dem Identitätsanbieter beeinträchtigen. In einem solchen Fall können Sie diese Eigenschaft auf „false“ festlegen.
Sicherheitsrisiko	(Moderate) SessionID wird verwendet, um den Instanzbenutzer zu verarbeiten und zu authentifizieren, indem der Sitzungsstatus im Browser beibehalten wird. Daher gilt SessionID als vertrauliche Daten und sollte standardmäßig sicher sein. Die Sitzungsrotation ist eine Sicherheitskontrolle, die die Änderung der Sitzungs-ID erzwingt, wenn der Benutzer von nicht authentifizierten Seiten zu authentifizierten Seiten navigiert.
Referenzen	Authentifizierung mit SAML

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Minimieren Sie die Anzahl der gleichzeitigen interaktiven Sitzungen

Verwenden Sie diese Eigenschaft mit dem Plugin „Gleichzeitige Sitzungen begrenzen“, um die Anzahl der aktiven Sitzungen zu steuern, die von einem Benutzer geöffnet werden können.

Verwenden Sie die Eigenschaft **Glide Authenticate Max Concurrent Interaktive Sitzungen** mit dem Plugin „ **Gleichzeitige Sitzung begrenzen** “ (`com.glide.limit.concurrent.sessions`), um die Anzahl der aktiven Sitzungen zu steuern, die für einen Benutzer geöffnet sind. Der empfohlene Wert ist **1**, wodurch die Anzahl der geöffneten Sitzungen reduziert wird (eine höhere Zahl erhöht die Wahrscheinlichkeit, dass eine Sitzung angegriffen werden könnte).

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.max.concurrent.interactive.sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1
Standardwert	1
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn der Standardwert der Eigenschaft größer als 1 ist, erhöht sich die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Das Plugin „ **Concurrent Interactive Sessions** “ (`com.glide.limit.concurrent.sessions`) sollte aktiv sein.
Referenzen	Begrenzen Sie gleichzeitige Sitzungen

Minimieren Sie die Zeitüberschreitungsdauer der Sitzungsaktivität

Verwenden Sie die Eigenschaft `glide.ui.session_timeout`, um den Zeitüberschreitungswert der Aktivität in Minuten anzugeben.

Das Festlegen dieser Eigenschaft hat mehrere funktionale Auswirkungen:

- Je länger die angegebene Sitzungszeitüberschreitung ist, desto mehr Arbeitsspeicher wird während einer Verarbeitungssitzung verwendet. Das Basissystem verwendet eine Apache Tomcat-Standardzeitüberschreitungsdauer von 30 Minuten.
- Mit Now Platform werden Benutzer weiterhin mit „Benutzernamen speichern“ abgemeldet. Nach 30 Minuten Inaktivität in der Anwendung meldet die Plattform den Benutzer automatisch ab, es sei denn, das Kontrollkästchen Benutzernamen speichern auf der **Anmeldeseite** ist aktiviert. Der Unterschied zu besteht darin, dass sie sich nicht erneut anmelden, um fortzufahren.
- Wenn es auf den Homepages der Benutzer Anzeigen oder Inhalte gibt, die automatisch aktualisiert werden, wird diese Zeitüberschreitung möglicherweise nie erreicht.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.session_timeout`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Sitzungsverwaltung
Zweck	Zum Erzwingen einer Sitzungszeitüberschreitung.
Empfohlener Wert	Benutzerdefinierte Zeitüberschreitung in Minuten. Der empfohlene Wert beträgt 60 Minuten. Dieser Wert kann jedoch je nach Funktionalität und Sicherheitsanforderung variieren. Legen Sie diesen Wert nicht auf mehr als einen Tag fest.
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt den rechtzeitigen Ablauf des Benutzerkontos. Keine Auswirkungen auf die Funktionalität, die Benutzer-Experience wird jedoch geändert.
Sicherheitsrisiko	(Hoch) Benutzersitzungen, die auf unbestimmte Zeit aktiv sind, stellen ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Benutzersitzungen verwalten

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinienbasiertes Sitzungszugriffsintervall für Mobile-Aktualisierungstoken begrenzen [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft `glide.authenticate.session_access.mobile.refresh_token_interval`, um die Zeitspanne zu steuern, die verstreichen muss, bevor ein Mobilgerätbenutzer zur erneuten Authentifizierung gezwungen wird.

Ein Benutzer wird nur dann zur erneuten Authentifizierung aufgefordert, wenn der Administrator die Identitätsanbieterattribute in der Sitzungsrichtlinie konfiguriert hat (Attribute können bei jeder Anmeldung variieren) und sich der Benutzer mit Single Sign-on (SSO) authentifiziert. Der Standardwert stellt die Zeit in Sekunden dar, die einem Benutzer zur erneuten Authentifizierung zur Verfügung steht. Ein höherer Standardwert bietet einem schädlichen Akteur mehr Zeit für den Sitzungszugriff im Falle eines Sitzungs-Hijacking.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.session_access.mobile.refresh_token_in`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1800 (Sekunden)
Standardwert	1800 (Sekunden)
Kategorie	Sitzungsverwaltung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn die ZTA-Richtlinie für die Instanz aktiviert ist, müssen Benutzer, die SSO während der mobilen Anmeldung verwenden, sich abmelden und erneut anmelden, nachdem der Standardwert von 1800 Sekunden (30 Minuten) überschritten wurde. Wenn ein höherer Wert verwendet wird, müssen Benutzer die verstrichene Zeit abwarten.
Abhängigkeiten und Voraussetzungen	Zero Trust: Richtlinienbasierter Sitzungszugriff
Funktionale Auswirkung	Diese Einstellung regelt die Zeit in Sekunden nach der Anmeldung, während der Benutzer sich von Mobilgeräten abmelden müssen, wenn sie Single Sign-on zur Authentifizierung verwenden und der Administrator die Provider-Attribute identifizieren in der Sitzungszugriffsrichtlinie konfiguriert hat.

Minimieren Sie die Zeitüberschreitungsdauer des Sitzungsfensters

Verwenden Sie die Eigenschaft `glide.ui.user_cookie.life_span_in_days`, um den Ablaufzeitraum für das Erinnerungscookie festzulegen. Der Standardwert beträgt 15 Tage, die maximale Obergrenze liegt bei 30 Tagen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.user_cookie.life_span_in_days`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Sitzungsverwaltung
Zweck	So aktivieren Sie den standardmäßigen Ablauf des **Erinnerungscookies**.
Empfohlener Wert	Benutzerdefinierter ganzzahliger Wert (Anzahl der Tage) [Beispiel: 15]
Sicherheitsrisikobewertung	4.9
Funktionale Auswirkung	(Mittel) Diese Eigenschaft wird vom Endbenutzer aktiviert, wenn der Endbenutzer das Kontrollkästchen Benutzernamen speichern auf der **Anmeldeseite** aktiviert und sich bei Now Platformanmeldet.
Sicherheitsrisiko	(Mittel) Die Benutzercookies, die für eine unbegrenzte Zeit aktiv sind, stellen ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Ändern Sie die Einstellungen für das Kontrollkästchen Benutzernamen speichern und Cookies

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Gespeicherte Kryptografie

Diese Kategorie konzentriert sich auf die Verschlüsselung gespeicherter Daten. Sie umfasst mehrere wichtige Aspekte, z. B. die Verwendung etablierter Algorithmen und kryptografischer Module, die Sicherstellung der ordnungsgemäßen Generierung von Pseudozufallswerten, die Implementierung der Verschlüsselung basierend auf der Datenklassifizierung sowie die sichere Speicherung und Isolierung von Schlüsselmaterial.

Glide-KMF-Verschlüsselung aktivieren [Entfernt in Security Center 1.3.2]

Verwalten Sie die für Password2-Felder in Ihrer Instanz verwendeten Verschlüsselungsprogramme.

Verwenden Sie die Eigenschaft the `glide.kmf.encrypter.enabled`, um die KMF-Verschlüsselung als Standardverschlüsselung für Password2-Felder festzulegen. Diese Eigenschaft stellt sicher, dass starke und konforme Verschlüsselungsstandards anstelle eines veralteten Verschlüsselungsprogramms verwendet werden. Um sicherzustellen, dass die KMF-Verschlüsselung anstelle der veralteten Verschlüsselung verwendet wird, legen Sie diese Eigenschaft auf **true**fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.kmf.encrypter.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Gespeicherte Kryptografie
Sicherheitsrisiko	• Schweregradpunktzahl: 4,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **true** “ festgelegt wird, wird sichergestellt, dass die KMF-Verschlüsselung anstelle der veralteten Verschlüsselung verwendet wird.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Password2-Verschlüsselung mit dem Key Management Framework (KMF)

Validierung, Bereinigung und Codierung

Validierung, Bereinigung und Codierung befassen sich mit der Eingabevalidierung, um Schwachstellen wie websiteübergreifendes Skripting (XSS), SQL-Injektion und andere Angriffe zu verhindern.

Diese Steuerung stellt sicher, dass Eingabevalidierung und Ausgabecodierung vorhanden und korrekt konfiguriert sind, z. B. Codierung oder Escaping von Ausgabedaten. Diese Kategorie umfasst auch Prüfungen für Elemente wie Deserialisierung von Objekten, Sandboxing bei Bedarf und positive Validierung durch Allow-Listen.

Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [Aktualisiert in Security Center 1.3]

Die vom Client aufrufbare skriptfähige GlideSystemUserSessionSandbox-API stellt die Methoden addErrorMessageNoSanitization und addInfoMessageNoSanitization von GlideSystemUserSession der Javascript-Sandbox bereit. Dadurch können alle Benutzer diese Methode per Skript aufrufen.

Bei Festlegung auf **true**darf eine Sandbox-Benutzersitzung Informationen oder Fehlermeldungen ohne Bereinigung aufrufen. Beim Aufruf der Nachricht wird eine Warnung protokolliert. Bei „ **false“**ist der Anruf nicht zulässig.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sandbox.usersession.allow_unsanitized_messages`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Diese Eigenschaft verhindert, dass nicht bereinigte Informations- oder Fehlermeldungen in einer Sandbox-Benutzersitzung aufgerufen werden.
Typ	wahr | false boolean
Empfohlener Wert	false
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Hoch) Wenn Sie die Eigenschaft auf den Wert „false“ festlegen, werden keine Nachrichten erstellt oder protokolliert, wenn diese Funktionen aufgerufen werden.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Bereinigung kann auf potenziell gefährliche Inhalte zugegriffen werden, und die nicht bereinigte Fehlerfunktion ist für Skripts verfügbar.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Deaktivieren Sie JavaScript-Tags in eingebettetem HTML

Verwenden Sie die Eigenschaft `glide.ui.security.codetag.allow_script`, um die Unterstützung für die Einbettung von HTML-JavaScript-Code zu deaktivieren, der mit dem Tag [code] erstellt wurde.

Now Platform mindert viele Einschleusungs- und Cross-Site-Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Benutzer keine HTML-formatierten Eingaben für Journalfelder schreiben und übermitteln. Journalfelder können jedoch in Code-Tags eingeschlossenen Text als HTML darstellen. Stellen Sie sicher, dass die Eigenschaft `glide.ui.security.codetag.allow_script` in der Tabelle „sys_properties“ vorhanden und auf „false“ festgelegt ist.

- Es besteht jedoch ein Sicherheitsrisiko. Bei Festlegung auf **true**können böswillige Benutzer schädlichen HTML-JavaScript-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Setzen Sie diese Eigenschaft auf „ **false** “, damit Administratoren verhindern können, dass Journalfelder HTML-JavaScript-Code rendern, indem sie die Unterstützung für das Tag [code] deaktivieren.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.security.codetag.allow_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Schützt vor websiteübergreifendem Skripting und der Ausführung böswilliger Skripts
Empfohlener Wert	false
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt JavaScript-Escaping in der Benutzeroberfläche und rendert die codierten Ergebnisse für den Benutzer. Sie kann sich basierend auf der Interaktion des Instanzbenutzers mit den resultierenden Daten auf die Funktionalität auswirken.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Beschränken Sie das CODE-Tag in Journalfeldern Journalfeldeinträge als HTML darstellen Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Geschützten Java-Sicherheitsmanager aktivieren [Neu in Security Center 1.3]

Die Eigenschaft `glide.security.manager` enthält den Java-Klassennamen des aktuellen Java-Sicherheitsmanagers.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.manager`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	`com.glide.sys.security.ContextualSecurityManager`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	`com.glide.sys.security.ContextualSecurityManager`
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,2 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn `glide.security.manager` nicht auf den empfohlenen Wert von `com.glide.sys.security.ContextualSecurityManager`festgeleg ist, verwendet die Instanz möglicherweise einen veralteten Java-Sicherheitsmanager, in dem die erwarteten Härtungsrichtlinien fehlen. Ohne diese Härtung könnte ein böswilliger Akteur mit Skriptausführungszugriff eine Remotecodeausführung in der Instanz erhalten.
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung erzwingen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `com.glide.security.check_unsanitized_html`, um das Bereinigungsverhalten von „translated_html“-Feldern auf globaler Ebene für Feldzuweisungen zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Die Zuweisung von HTML-Feldern zu einem beliebigen Feldtyp bietet die Funktionalität zum Formatieren von Inhalten mithilfe von HTML-Tags (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Um böswillige Aktivitäten zu verhindern, können bestimmte HTML-Tags mithilfe einer Sperrliste gesperrt werden. Diese Eigenschaft verhindert, dass unzulässige Tags in „translated_html“-Feldern in Ihrer Instanz verwendet werden.

- Legen Sie diese Eigenschaft fest, um das Bereinigungsverhalten von „translated_html“-Feldern zu **erzwingen**.
- Legen Sie die Eigenschaft auf „disable“ fest, um die HTML-Bereinigung zu **deaktivieren** und blockierte HTML-Tags in „translated_html“-Feldern zuzulassen.

> ⚠ **Warnung:**
> Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.security.check_unsanitized_html`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert die Verwendung unsicherer HTML-Tags zum Schutz vor Angriffen wie websiteübergreifendem Skripting.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Typ	Zeichenfolge
Empfohlener Wert	`erzwingen`
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die HTML-Bereinigung in der Benutzeroberfläche und rendert übersetzte HTML-Felder für den Benutzer. Dies kann Auswirkungen auf die Lesbarkeit und Formatierung haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Benutzersitzungen im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	HTML-Bereinigung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Sandbox für vom Client generierte Skripts erzwingen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.script.use.sandbox`, um das Skript-Sandboxing zu aktivieren.

Es gibt zwei Fälle in Now Platform, die es dem Client ermöglichen, Skripts zur Auswertung an den Server zu senden:

Filter oder Abfragen

Es ist zulässig, einen Filter an den Server zu senden, z. B. assigned_to=JavaScript:getMyGroups().

System-API

Der API-Aufruf ermöglicht es dem Client, beliebige Skripts auf dem Server auszuführen und eine Antwort zu erhalten.

Wenn Sie das Skript-Sandboxing aktivieren, wird das an einem dieser beiden Einstiegspunkte ausgewertete Skript in einer Sandbox mit eingeschränkten Rechten mit den folgenden Eigenschaften ausgeführt:

- Nur die Business Rules, die als vom Client aufrufbar markiert sind, sind in der Sandbox verfügbar.
- In der Sandbox sind nur Skripteinbindungen verfügbar, die als vom Client aufrufbar markiert sind.
- Bestimmte API-Aufrufe (weitgehend, aber nicht vollständig, beschränkt auf Aufrufe, die sich mit direktem DB-Zugriff befassen) sind nicht zulässig.
- Sie können Daten in der Sandbox nicht einfügen, aktualisieren oder löschen. Beispielsweise werden alle Aufrufe von current.update()ignoriert. Wenn Sie Now Platform ausführen, ohne das Skript-Sandboxing zu aktivieren, gilt keine dieser Einschränkungen.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.script.use.sandbox`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für die Plattform gestartet werden
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	(Kritisch) Diese Fehlerkorrektur erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für Now Platformgestartet werden. Dies hat potenzielle Auswirkungen, wenn der Kunde über Anpassungen verfügt, die hartcodierte JavaScript-Abfragen zum Ausführen von CRUD-Vorgängen enthalten.
Sicherheitsrisiko	(Kritisch) Now Platform bietet eine Vielzahl von Features und Funktionen über JavaScript-Abfragen. Ohne entsprechende Autorisierung und Validierung besteht jedoch für einen Angreifer die Möglichkeit, nicht autorisierte Vorgänge auf der Plattform durchzuführen.
Referenzen	Konfigurieren der Skript-Sandbox-Eigenschaft `glide.script.use.sandbox` gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • `glide.script.allow.ajaxevaluate`: Siehe AJAXEvaluate aktivieren. • `glide.script.secure.ajaxgliderecord`: Siehe Aktivieren der AJAXGlideRecord-ACL-Überprüfung.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Eingehende E-Mail-Bilder in Anhänge konvertieren [In Security Center 1.5 entfernt]

Verwenden Sie die Eigenschaft `glide.email.inbound.convert_html_inline_attachment_references`, um anzugeben, ob eingehende E-Mail-HTML so konvertiert werden soll, dass E-Mail-Bilder in der HTML-Textvorschau der E-Mail angezeigt werden.

Folgendes geschieht, wenn die Systemeigenschaft `glide.email.inbound.convert_html_inline_attachment_reference` auf „false“ festgelegt ist:

- In Now Platformwerden anstelle der empfangenen Bilder defekte CID-Links (Inhalts-ID) angezeigt. Das Format, in dem das E-Mail-Bild angezeigt wird, hängt von der Eigenschaftseinstellung zum Zeitpunkt des Empfangs der E-Mail ab, nicht von der aktuellen Eigenschaftseinstellung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der im Anhang empfangene „böswillige“ Inhalt wird im HTML-Code der E-Mail nicht referenziert. Der Anhang selbst wird in der Tabelle „sys_attachment“ gespeichert.
- Bei der Verarbeitung eingehender E-Mails werden die HTML-Daten der E-Mail nicht aktualisiert, um den Speicherort des Anhangs in der Tabelle „sys_attachment“ wiederzugeben. Dies führt zu Folgendem:
  - Inline-Bilder werden im Aktivitätsformatierer nicht in der E-Mail-Anzeige angezeigt.

    Hinweis:
    Um dieses Problem mit dem Aktivitätsformatierer zu beheben, überprüfen Sie zuerst, ob keine Sicherheitsbedenken bestehen. Legen Sie dann die Systemeigenschaft `glide.email.inbound.convert_html_inline_attachment_reference` auf „ **true** “ fest, damit zukünftige empfangene E-Mails die erforderliche HTML-URL enthalten können, um auf das Bild zu verweisen. Durch das Ändern der Eigenschaft werden bereits empfangene E-Mails nicht aktualisiert. Der neue Wert wirkt sich nur auf eingehende E-Mails aus, die nach dem Ändern der Eigenschaft empfangen wurden.

  - Inline-Bilder werden nicht angezeigt, wenn die E-Mail in der HTML-Vorschau der E-Mail angezeigt wird.
  - Beim Anfügen von email.body_htm in eingehenden Aktionen zwischen Code-Tags fehlen die Bilder.

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft `glide.email.read.active` auf „true“ fest. Weitere Informationen finden Sie unter Enable using your own POP3 server .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.email.inbound.convert_html_inline_attachment_refere`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	So beschränken Sie das Rendern von Bildern in der HTML-Textvorschau.
Empfohlener Wert	false
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, kann der Benutzer die Bildvorschau im E-Mail-Text nicht sehen.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer ein schädliches Image senden, das Malware enthält.
Referenzen	Email properties Inbound mail configuration

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AJAXEvaluate deaktivieren

Verwenden Sie `glide.script.allow.ajaxevaluate`, um die System-API vor Schwachstellen der Client-Skriptausführung über AJAX-Aufrufe zu schützen.

Zum Bearbeiten der Eigenschaft ist eine Erhöhung auf die Rolle „security_admin“ erforderlich.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.script.allow.ajaxevaluate`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um zu verhindern, dass ein Benutzer Skripts mit Administratorrechten ausführt.
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt das Deaktivieren des AJAXEvaluate-Prozessors. Dies kann Auswirkungen auf die Funktionalität haben, wenn Sie den AJAX-Auswertungsprozessor explizit als Teil benutzerdefinierter Skripts verwenden.
Sicherheitsrisiko	(Hoch) Der AjaxEvaluator-Prozessor führt Client-Skripts in der Sandbox aus. Es gibt jedoch mehrere zusätzliche Eigenschaften, die es ermöglichen, den Umfang der Aktivitäten in der Sandbox zu erweitern oder vollständig zu deaktivieren.
Sicherheitsrisikobewertung	7.3
Referenzen	Diese Eigenschaft gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • `glide.script.use.sandbox`: Siehe vom Client generierte Skripts in der Sandbox. • `glide.script.allow.ajaxevaluate`: Siehe AJAXEvaluate aktivieren.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Entitätserweiterung deaktivieren [Aktualisiert in Security Center 1.5]

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie die Eigenschaft `glide.stax.allow_entity_resolution`, um die Erweiterung externer Entitäten vollständig zu deaktivieren. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie diese Eigenschaft auf **true**festlegen, versuchen alle externen Entitäten, abhängig von der Einstellung der Eigenschaft `glide.stax.whitelist_enabled`, Betreffentitäten aufzulösen oder zu erweitern.
- Wenn Sie diese Eigenschaft auf „ **false**“ festlegen, werden alle Entitätsauflösungen und -erweiterungen blockiert. Weitere Informationen finden Sie unter XMLdoc2-Entitätsvalidierung mit Whitelist.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaften `glide.xml.entity.whitelist.enabled` und `glide.stax.whitelist_enabled` auf „true“ fest. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit weißer Liste und XMLdoc2-Entitätsvalidierung mit weißer Liste.
- Definieren Sie eine Liste von durch Kommas getrennten FQDNs in der Eigenschaft `glide.xml.entity.whitelist`. Dies sind die einzigen URLs, die über die XML-Entitätsverarbeitung erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Whitelist.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.stax.allow_entity_resolution`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen XML-Entitätserweiterungs-/Billion-Lach-Angriff zu schützen.
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Kritisch) Ein Angreifer kann diese Schwachstelle verwenden, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.
Workaround	Wenn die Anpassung eine Entitätserweiterung erfordert, legen Sie diese Eigenschaft auf „true“ fest, und befolgen Sie die in XMLdoc2-Entitätsvalidierung mit weißer Listedokumentierten Schritte.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property

Weitere Informationen zu OWASp-Ressourcen finden Sie unter OWASp .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Externe Inhalts-URL deaktivieren

Verwalten Sie mit Connect-Chat, wie Metadaten externer Links in Ihrer Instanz verwendet werden.

Verwenden Sie die Eigenschaft `glide.ui.url.external.content`, um Metadaten externer Links in Ihrer Instanz zu verwalten. Wenn die Eigenschaft auf den empfohlenen Wert **false**festgelegt ist, werden keine externen Link-Metadaten gerendert. Bei „ **true** “ ruft Connect Chat externe Link-Metadaten aus Quellen wie YouTube oder Nachrichtenartikel ab, um umfangreichere Nachrichten zu rendern. Dies kann zu SSRF-Angriffen (Server Side Request Forgery) führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ui.url.external.content`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	Wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **true** “ setzen, ist Ihre Instanz möglicherweise SSRF-Angriffen (Server Side Request Forgery) ausgesetzt.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Connect Chat

Beschränken Sie herunterladbare MIME-Typen

Die Eigenschaft `glide.ui.attachment.download_mime_types` erzwingt, dass die angegebene Liste der gefährlichen Dateitypen auf den Client heruntergeladen und nicht inline im Browser angezeigt wird.

Wenn der MIME-Typ einer Datei in `glide.ui.attachment.download_mime_types` vorhanden ist, wird ein Download erzwungen. Zum Beispiel erzwingt das Herunterladen von text/html, dass eine HTML-Datei als Datei auf den Client heruntergeladen und nicht inline im Browser angezeigt wird, wodurch ein XSS-Angriff verhindert wird.

Um eine Liste vorhandener MIME-Typen anzuzeigen, `geben Sie / sys_attachment_icon_rule_list.do ein`. Sie können einen dieser MIME-Typen aktivieren, um die Sicherheits-Compliance-Anforderungen in Now Platformzu erfüllen.

Hinweis:
Zum Bearbeiten der Eigenschaft ist die Rolle security_admin erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.attachment.download_mime_types`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Durch die ordnungsgemäße Verwaltung der Liste der gefährlichen Dateitypen, die im Browser nicht angezeigt werden können, werden Cross Site Scripting-Angriffe (XSS) verhindert.
Empfohlener Wert	Liste der anwendbaren MIME-Typen oder Standard: `text/html,image/svg,image/svg+xml,application/xml`
Konfigurationstyp	Zeichenfolge: alle durch Kommas getrennten Werte von Anwendungs-MIME-Typen.
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt die Durchführung von Validierungsprüfungen, bevor eine Aktion ausgeführt wird, wenn Sie in einer Now Platform -Anwendung auf einen Anhang klicken. Es gibt keine potenziellen Auswirkungen, aber die Benutzer-Experience wird geändert.
Sicherheitsrisiko	(Mittel) Angreifer können MIME-Typen missbrauchen und unbeabsichtigte Skriptinhalte im Anhang auf der Seite des Opfers platzieren, um vertrauliche Informationen zu erfassen. Die Möglichkeit, über XSS zu verfügen, kann zu einer leicht zu erreichenden Berechtigungseskalation auf höhere Rollen wie „Administrator“ führen, in der mehr Seitwärtsbewegung möglich ist. Füllen Sie im aktuellen Kontext die Eigenschaft mit einer Liste von durch Kommas getrennten MIME-Anhangtypen aus, die im Browser nicht inline dargestellt werden sollen.
Sicherheitsrisikobewertung	6.3
Zugehörige Eigenschaften	• `glide.ui.attachment.force_download_all_mime_types` • `glide.ui.attachment.tables_ignore_force_download`
Referenzen	Download von MIME-Typen erzwingen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Eingeschränkte herunterladbare MIME-Typen definieren [In Security Center 1.5 entfernt]

Verwenden Sie die Eigenschaft `glide.ui.attachment.force_download_all_mime_types`, um MIME-Typen herunterzuladen und im Browser nicht inline darzustellen.

Zum Beispiel erzwingt das Herunterladen von text/html, dass eine HTML-Datei als Datei auf den Client heruntergeladen und nicht inline im Browser angezeigt wird, wodurch ein XSS-Angriff verhindert wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine Liste vorhandener MIME-Typen anzuzeigen, geben Sie /sys_attachment_icon_rule_list.do ein. Sie können einen dieser MIME-Typen aktivieren, um die Sicherheits-Compliance-Anforderungen in Now Platformzu erfüllen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.attachment.force_download_all_mime_types*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um die Darstellung der Dateitypen im Browser einzuschränken, um die Ausführung versteckter schädlicher Skripts zu vermeiden.
CVSS-Bewertung	8
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt die Durchführung von Validierungsprüfungen, bevor eine Aktion ausgeführt wird, wenn Sie in einer Now Platform -Anwendung auf einen Anhang klicken. Es gibt keine potenziellen Auswirkungen, aber die Benutzer-Experience wird geändert.
Sicherheitsrisiko	(Hoch) Clientseitige Skripting-Angriffsvektoren gibt es in verschiedenen Varianten, und der Missbrauch von MIME-Typ-Anhängen ist keine Ausnahme. Angreifer können MIME-Typen missbrauchen und unbeabsichtigte Skriptinhalte im Anhang auf der Seite des Opfers platzieren, um vertrauliche Informationen zu erfassen. Die Möglichkeit, über XSS zu verfügen, kann zu einer leicht zu erreichenden Berechtigungseskalation auf höhere Rollen wie „Administrator“ führen, in der mehr Seitwärtsbewegung möglich ist. Füllen Sie im aktuellen Kontext die Eigenschaft mit einer Liste von kommagetrennten MIME-Typen für Anhänge aus, die im Browser nicht inline dargestellt werden sollen. Beispiele: text/html, text/csv
Zugehörige Links	Download von MIME-Typen erzwingen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Deaktivieren Sie eingebetteten HTML-Code

Verwenden Sie die Eigenschaft *glide.ui.security.allow_codetag*, um die Unterstützung für die Einbettung von HTML-Code zu deaktivieren, der mit dem Tag [code] erstellt wurde.

Now Platform mindert viele Einschleusungs- und Cross-Site-Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Benutzer keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTML-formatierten Eingaben für Journalfelder schreiben/übermitteln. Journalfelder können jedoch in Code-Tags eingeschlossenen Text als HTML darstellen.

- Es besteht jedoch ein Sicherheitsrisiko. Bei Festlegung auf `true`können böswillige Benutzer schädlichen HTML-JS-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Setzen Sie diese Eigenschaft auf „ `false` “, damit Administratoren verhindern können, dass Journalfelder HTML-Code rendern, indem sie die Unterstützung für das Tag `[code]` deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.security.allow_codetag
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schützen Sie sich vor websiteübergreifendem Skripting und der Ausführung böswilliger Skripts
Empfohlener Wert	false
Sicherheitsrisikobewertung	4.2
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die HTML-Codierung in der Benutzeroberfläche und rendert die codierten Ergebnisse für den Benutzer. Diese Eigenschaft ist standardmäßig auf „ `true` “ festgelegt. In diesem Status zeigt Ihre Instanz gerenderten HTML-Code in Journalfeldern und Formularen an. Wenn diese Eigenschaft auf „ `false`“ festgelegt ist, wird HTML nicht ordnungsgemäß dargestellt, und HTML-Tags werden möglicherweise in Journalfeldern in Formularen angezeigt. Dies kann sich negativ auf die Funktionalität und die Benutzerinteraktionen mit den resultierenden Daten auswirken.
Sicherheitsrisiko	(Mittel) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

HTML-Bereinigung in Virtual Agent aktivieren

Verwenden Sie die Eigenschaft *`com.glide.cs.html.sanitizer.enabled`*, um HTMLSanitizerService zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`com.glide.cs.html.sanitizer.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert, dass die Anwendung Cross Site Scripting und HTML-Injektionsangriffe durchführt.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Benutzerdaten an den Benutzer zurückgegeben werden. Wenn der Kunde eine Anpassung hat, die das Rendern der HTML-Attribut- oder Inhaltsdaten umfasst, hat dies Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Hoch) Benutzereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden. Dadurch werden clientseitige Cross-Site-Scripting-Angriffe durch Ausgabecodierung der Daten reduziert.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Jelly JS-Interpolationsschutz aktivieren

Verwenden Sie die Eigenschaft `glide.ui.jelly.js_interpolation.protect`, um sicherzustellen, dass JavaScript-Code, der auf einer Jelly-Seite ausgeführt werden soll, mithilfe der Jelly-Interpolation vor der Eingabe geschützt wird.

Wenn Sie die Eigenschaft auf **true**festlegen, durchläuft eine Anwendung eine Jelly-Skriptstruktur (verschachtelt). Potenziell gefährliche Jelly-Ausdrücke werden mit einem Filter umschlossen, der:

- Versieht ihre Ergebnisse aus Sicherheitsgründen mit Escape-Zeichen, oder
- Wenn ihre Sicherheit nicht garantiert werden kann, generiert eine SecurityException, da der Ausdruck, der ausgewertet werden sollte, ein mögliches Sicherheitsproblem darstellt.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.jelly.js_interpolation.protect`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Zur Verringerung von Angriffen mit Ausführung von böswilligem Code, die durch Jelly-Injektion auftreten können.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	9
Funktionale Auswirkung	(Hoch) Diese Eigenschaft ermittelt am besten, ob ein Ausdruck in Anführungszeichen steht. Möglicherweise wird ein gültiger Ausdruck falsch in Anführungszeichen gesetzt. In diesem Fall kann es erforderlich sein, einen Ausdruck manuell als sicher zu kennzeichnen.
Sicherheitsrisiko	(Moderat) Die JEXL-Injektion ist eine Form der Eingabeinjektion, die für Now Platform eindeutig ist und sowohl zur standortübergreifenden Anforderungsfälschung als auch zur Codeausführung führen kann. Wenn Sie den Schutz vollständig deaktivieren, können möglicherweise viele P1-Sicherheitsschwachstellen geöffnet werden.
Workaround	Um einen Ausdruck manuell als sicher zu kennzeichnen, fügen Sie dem Jelly-Ausdruck das SAFE-Präfix hinzu: `${SAFE:sysparm_input};` Das blinde Hinzufügen von SAFE zu jedem Ausdruck ist die falsche Herangehensweise an das Problem, da dadurch eine Sicherheitslücke geöffnet werden kann. • Fügen Sie SAFE nur dann zu einem Ausdruck hinzu, wenn Sie garantieren können, dass der Ausdruck keine Eingaben vom Client enthält. • Wenn dies der Fall ist, kann ein böswilliger Client die Auswertung von privilegiertem JavaScript verursachen.
Referenzen	Jelly Tags Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Aktivieren Sie den Jelly JS-Interpolationsschutz für verschachtelte Ausdrücke

Verwalten Sie den Interpolationsschutz in Ihrer Instanz.

Verwenden Sie die Eigenschaft the *`glide.ui.jelly.js_interpolation.protect_nested_expressions`*, um den Interpolationsschutz zu verwalten. Der Interpolationsschutz stellt sicher, dass Jelly-Ausdrücke bei Verwendung in JavaScript als sicher eingestuft werden müssen, indem sie entweder in bestimmte Kategorien fallen oder im Ausdruck selbst als SAFE markiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden. Wenn diese Risikominderung nicht aktiviert ist, kann ein schlechter Akteur einen GET-Parameter an eine Jelly-Seite senden und veranlassen, dass der Inhalt dieses Parameters als serverseitiges JavaScript mit Administratorrechten ausgewertet wird. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, sind in JavaScript interpolierte schädliche Jelly-Ausdrücke zulässig, und ein Benutzer kann Code mithilfe einer Jelly-Vorlage ausführen.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.jelly.js_interpolation.protect_nested_expressions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	false
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 9 • CVSS-Punktzahl: Kritisch • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf **„false“** festgelegt ist, sind schädliche Jelly-Ausdrücke zulässig.
Abhängigkeiten und Voraussetzungen	Keine

Erzwingen Sie relative Links

Verwenden Sie die Eigenschaft *glide.cms.catalog_uri_relative*, um relative Links aus dem URI-Parameter für /ess/catalog.dozu erzwingen.

- Bei Festlegung auf **true**werden nur relative URLs über die Seite /ess/catalog.do mit dem Parameter *uri* zugelassen.
- Bei **false**sind alle URLs zulässig, was die Verknüpfung mit externen, nicht autorisierten Inhalten ermöglichen kann.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.cms.catalog_uri_relative*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um Versuche einzuschränken, externe nicht autorisierte Inhalte zu verknüpfen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	2.6
Funktionale Auswirkung	(Niedrig) Diese Fehlerkorrektur erzwingt die Validierung auf der Katalogseite, sodass nur relative URLs zulässig sind. Vorhandene Links zu externen Webanwendungen werden unterbrochen.
Sicherheitsrisiko	(Hoch) Absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil eines Parameters oder Feldwerts verwendet werden, wodurch die Quellseite auf eine von Angreifern kontrollierte Website umgeleitet wird.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Erzwingen Sie die Prüfung der URL-Allow-Liste

Verwenden Sie die Eigenschaft `glide.security.url.whitelist`, um eine zusätzliche Validierungsebene hinzuzufügen, um sicherzustellen, dass eine eingeführte externe URL Teil der URLs auf der Aufnahmeliste sein soll.

Eine offene Umleitung tritt auf, wenn eine angreifbare Webseite auf eine nicht vertrauenswürdige und schädliche Seite umgeleitet wird, die den Benutzer gefährden kann. Offene Umleitungsangriffe gehen mit einem Phishing-Angriff einher, da der geänderte angreifbare Link mit der ursprünglichen Website identisch ist, was die Erfolgswahrscheinlichkeit des Phishing-Angriffs erhöht.

Diese Eigenschaft ist in den folgenden Fällen anwendbar:

- `/logout.do?sysparm_goto_url={Externe URL}`
- `/cms_login_redirect.do?sysparm_goto_url={Externe URL}`

Benutzer werden zu einer externen vertrauenswürdigen Site weitergeleitet, nachdem sie sich von der Instanz abgemeldet haben:

- `/logout_redirect.do?sysparm_url={Externe URL}`
- `/saml_redirector.do?sysparm_uri={Externe URL}`

Wenn SAML aktiviert ist, wird eine Abmelde-URL eines Identitätsanbieters (IDP) aufgerufen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.url.whitelist`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Zum Implementieren einer sicheren URL-Umleitung während der Anmeldung, Abmeldung oder anderen Umleitungen. Diese Eigenschaft mindert einen der 10 häufigsten OWASP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Angriffe mit der Bezeichnung „Ungültige Umleitungen und Weiterleitungen“.
Typ	Zeichenfolge
Wert	Die genehmigten URLs Ihrer Organisation [Einige definierte FQDNs (vollständig qualifizierter Domänenname)] Bsp. http://www.servicenow.com]
Sicherheitsrisikobewertung	8.3
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die Validierung auf der Abmeldeseite. Sie kann funktionale Auswirkungen auf einen Benutzer einer Instanz mit einer SSO/SAML-Konfiguration haben.
Sicherheitsrisiko	(Hoch) Clientseitige offene Umleitung ermöglicht es Angreifern, Opfer/Anwender auf die vom Angreifer kontrollierte Website umzuleiten, und wird als Sicherheitsrisiko angesehen.
Referenzen	Multi-SSO (SAML 2.0) – Fehler und Korrekturen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Excel-Formeln mit Escape-Zeichen versehen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.export.escape_formulas`, um die Excel-Einschleusung zu verhindern, die auch als Formeleinschleusung bezeichnet wird.

Excel-Injektion erfolgt, wenn Websites nicht vertrauenswürdige Einträge in Excel-Dateien einbetten. Wenn Sie eine Tabellenkalkulationsanwendung wie Microsoft Excel oder LibreOffice Call verwenden, um eine Datei zu öffnen, werden alle Zellen, die mit +, -, = oder @ beginnen, als Formel interpretiert. Wenn Sie die Eigenschaft `glide.export.escape_formulas` auf **true**festlegen, werden Zeichenfolgenwerte, die mit +, -, = oder @ beginnen, beim Export in CSV-, XLS- oder XLSX-Dateien mit einem einzelnen Apostroph versehen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.export.escape_formulas`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um die Anwendung gegen die Excel- oder Formeleinschleusung zu verhindern.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	(Niedrig) Böswillig erstellte Formeln können dazu verwendet werden, den Computer des Benutzers zu kapern, indem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Schwachstellen in der Tabellenkalkulationssoftware ausgenutzt werden.
Sicherheitsrisiko	(Mittel) Böswillige Formeln stellen ein Risiko dar, auch wenn die eingebettete Tabelle keine vertraulichen Informationen enthält, da sie dazu verwendet werden können, den Computer des Betrachters zu gefährden.
Workaround	Alternativ können Sie nach Möglichkeit alle Leerzeichen entfernen und alle vom Client bereitgestellten Daten auf alphanumerische Zeichen beschränken.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

HTML in Listenansichten mit Escape-Zeichen versehen

Verwenden Sie die Eigenschaft *glide.ui.escape_html_list_field*, um HTML-Escape-Zeichen für HTML-Felder in einer Listenansicht zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Die Zuweisung von HTML-Feldern zu einem beliebigen Feldtyp bietet die Funktionalität zum Formatieren von Inhalten mit HTML-Codes (z. B. <p>, <a href>, <b>, <font>, <img>). Ein böswilliger Benutzer kann HTML-Code innerhalb des Formularfelds einfügen, um unerwünschte Skripts in verschiedenen Client-/Benutzersitzungen auszuführen.

- Legen Sie diese Eigenschaft auf „ **false** “ fest, um ein HTML-Escaping durchzuführen, bevor die Datensätze/Felder im Browser gerendert werden, wenn die Tabelle als Listenansicht angezeigt wird.
- Wenn diese Option auf **true**gesetzt ist und Sie diese Spalte in einer Listenansicht auswählen, wenn Sie eine Tabelle oder Datensatzliste anzeigen, werden diese HTML-formatierten Felder möglicherweise angezeigt.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.escape_html_list_field*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um die Anwendung gegen websiteübergreifende Skripting-Angriffe zu schützen
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die HTML-Codierung in der Benutzeroberfläche auf HTML-Parser-Ebene und gibt dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Benutzer codierte Ergebnisse zurück. Sie kann sich basierend auf der Interaktion des Instanzbenutzers mit den resultierenden Daten auf die Funktionalität auswirken.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Benutzersitzungen im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

JavaScript mit Escape-Zeichen versehen

Verwenden Sie die Eigenschaft `glide.html.escape_script`, um in Listenansichten Escape-Zeichen für JavaScript-Tags (<script></script>) in HTML-Feldern zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Die Zuweisung von HTML-Feldern zu einem beliebigen Feldtyp bietet dem Benutzer die Funktionalität, den Inhalt mit HTML-Codes zu formatieren (z. B. <p>, <a href>, <b>, <font>, <img>). Wenn Sie `glide.html.escape_script` auf **false**festlegen, werden die Tags (<script></script>) möglicherweise angezeigt, wenn Sie diese Spalte in einer Listenansicht auswählen, während Sie eine Tabellen- oder Datensatzauflistung anzeigen.

Ein böswilliger Angreifer kann JavaScript-Code einfügen, indem er ihn in die Tags (<script></script>) einbettet. Der Angreifer kann dies ausnutzen, indem er einen ausgefeilten JS-Vektor einfügt, der ausgeführt werden kann, wenn ein Benutzer den Tabellendatensatz öffnet.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.html.escape_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um websiteübergreifende Skripting-Angriffe auf eine Anwendung zu verhindern.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt JavaScript-Escaping in der Benutzeroberfläche und rendert codierte Ergebnisse für den Benutzer. Dies kann sich basierend auf der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Instanzbenutzerinteraktion mit den resultierenden Daten auf die Funktionalität auswirken
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Verfügbare Systemeigenschaften Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Escape-Jelly-Skript

Verwenden Sie die Eigenschaft `glide.ui.escape_all_script`, um die Escape-Zeichen aller in Jelly eingefügten Skripts zu erzwingen.

Alle in enthaltenen JS- und HTML-Zeichenfolgen werden mit Escape-Zeichen versehen<j:jelly> ... </j:jelly> bevor sie in den Ausgabestrom geschrieben werden, wodurch das Auftreten mehrerer XSS-Probleme verhindert wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.escape_all_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung

Zweck	Wenn die Eigenschaft nicht auf **true**festgelegt ist, müssen Entwickler für jedes benutzerdefinierte Jelly-Skript mehrere Schritte ausführen, um XSS-Probleme zu vermeiden. Diese Schritte umfassen das Suchen der Jelly-Variablen, die an den Ausgabestream gesendet werden, um sie auf Webseiten zu rendern, und das Ausführen von Escaping für jedes der folgenden Tags:
	
	`$ à {JS:Ausdruck}`
	
	`$ à {HTML: Ausdruck}`
	
	ODER
	
	`$à {JS,HTML:Ausdruck}`

Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	7.3

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt Jelly-Escaping auf Parser-Ebene. Sie kann Auswirkungen auf die Funktionalität der Benutzerinteraktion mit den resultierenden Daten haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss für alle Benutzereingaben erfolgen, die in der Anwendung eingegeben werden. Auf diese Weise können Einschleusungsangriffe auf die Plattform verteidigt und geschützt werden.
Workaround	Die Benutzeroberfläche kann beeinträchtigt werden, da einige der Skripts und HTML-Tags, die für das Rendern auf einer Webseite entwickelt wurden, möglicherweise fehlerhaft erscheinen. Diese Korrektur sendet die codierte Ausgabeseite zum Rendern an den Browser. Beispielsweise kann anstelle von „meine Zeichenfolge hier“ „meine Zeichenfolge hier“<u>angezeigt werden</u>, da das Tag <u> ordnungsgemäß mit Escape-Zeichen versehen wurde. Um in diesem Fall ein Escaping zu verhindern, fügen Sie dem Jelly-Ausdruck das NOESC-Präfix hinzu, um ein JS-Escaping zu verhindern. Beispiel: • Vorher: ($[jvar_context_menus]); • Nach: ($[NOESC:jvar_context_menus]); • Vorher: $[jvar_ui_policy_scripts] • Nach: $[NOESC:jvar_ui_policy_scripts]
Referenzen	Strenge Sicherheitseinstellungen Jelly Tags

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Escape-Skripts in Scratchpad

Erfahren Sie, wie sich das Scratchpad in die Sicherheitslage Ihrer Instanz einfügt und wie Sie es so verwalten, dass keine schädlichen Skripts darauf ausgeführt werden können.

Das Scratchpad ist eine einfache Möglichkeit, Informationen auf dem Server festzulegen, auf die Sie im Browser zugreifen können. Ein Administrator kann alles skripten, einschließlich beliebiger Datensätze. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können schädliche Skripts wie eine websiteübergreifende Skripting-Schwachstelle ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.escape_scratchpad*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	Wahr
Standardwert	Wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn die Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können schädliche Skripts wie eine websiteübergreifende Skripting-Schwachstelle ausgeführt werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Workflow administration

XML-Markup mit Escape-Zeichen versehen

Verwenden Sie die Eigenschaft *glide.ui.escape_text*, um Escape-Zeichen für XML-Werte auf Parser-Ebene zu erzwingen, bevor sie an den Browser des Clients übertragen werden.

Siteübergreifendes Skripting tritt auf, wenn ein Angreifer schädliches JavaScript in einen Einstiegspunkt einfügt. Die Plattform/Anwendung kann das schädliche JavaScript nicht mit Escape-Zeichen versehen, bevor es zur Ausführung an den Browser des Opfers übermittelt wird. Escaping bedeutet in diesem Kontext Folgendes:

- **&** -> `&`
- **<** --> `<`
- **>** --> `>`
- **„** --> `“`
- **'** --> `'`
- **/** --> `/`

Beispiel: <![CDATA[<script> `alert('XSS-Angriff');`</script>]]>

Escaping: <script>alert('XSS Attack');</script>

Stellen Sie sicher, dass die Eigenschaft *glide.ui.escape_text* in der Tabelle „sys_properties“ vorhanden und auf „true“ festgelegt ist.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.escape_text`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Durch das Escaping von XML wird sichergestellt, dass Browser das in nicht vertrauenswürdige Daten eingebettete schädliche JavaScript nicht analysieren und als JavaScript ausführen. • Ein böswilliger Benutzer kann einen XSS-Angriff versuchen, um entweder die Sitzung anderer Benutzer zu kapern oder den Benutzer auf eine schädliche Website umzuleiten. • Die Now Platform enthält Code zum Sichern von Cookies. Um ihn jedoch zu maskieren, muss diese Eigenschaft auf **true**festgelegt werden.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur erzwingt die XML-Codierung auf XML-Parser-Ebene in der Benutzeroberfläche. Dadurch werden die codierten Ergebnisse für den Benutzer gerendert, was sich je nach Instanzbenutzerinteraktion mit den resultierenden Daten auf die Funktionalität auswirken kann.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

Workaround	Nachdem Sie diese Eigenschaft auf **true**festgelegt haben, wird das Rendern der HTML-Tags in der Katalogelementbeschreibung oder im Hilfetext der Katalogelementvariablen angehalten. Möglicherweise können Sie die HTML-Formatierung für einige Felder nicht verwenden.
	Wenn jedoch die Eigenschaft `glide.ui.escape_text` deaktiviert ist, wird allen JEXL-Ausdrücken ein Ausgabe-Encoder vorangestellt:
	`${JS:Ausdruck}`
	`${HTML:Ausdruck}`
	oder
	`${JS,HTML:Ausdruck}`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

XML-Antwort mit Escape-Zeichen versehen

Verwalten Sie, wie XML-Escape-Zeichen in Ihrer Instanz behandelt werden.

Verwenden Sie diese Eigenschaft, um zu verwalten, ob XML-Antworten mit Escape-Zeichen versehen sind. Wenn die Eigenschaft auf den empfohlenen Wert **false**festgelegt ist, werden XML-Antworten nicht mit Escape-Zeichen versehen, was zu einem XML-Injektionsangriff führen kann. Die Einschleusung von unbeabsichtigtem XML-Inhalt in eine XML-Nachricht kann die beabsichtigte Logik einer Anwendung ändern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.soaprequest.unescape_xml_response*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	false
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,4 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **falsch** “ festgelegt wird, wird das XML-Escaping deaktiviert, was zu einem XML-Injektionsangriff führen kann.
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung aktivieren [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft *glide.html.sanitize_all_fields*, um die HTMLSanitizer-Skripteinbindung zu aktivieren, die HTML-Eingaben basierend auf den in einem Skript konfigurierten Ausschluss- und Aufnahmeattributen bereinigt.

Die mit Dictionary/Fields verfügbaren Feldtypen umfassen HTML und übersetztes HTML. Mit diesen HTML-Eingabefeldern können Benutzer HTML-formatierte Eingaben schreiben, z. B.:

<h1>Test</h1>) mit den einfachsten HTML-Tags wie <img>, <a href ⋯>und <iframe>.

Sie kann einem böswilligen Angreifer die Möglichkeit geben, schädliche Vektoren mit HTML-Tags einzuschleusen, z. B.:

[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href="" onclick=alert(/xss/)].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.html.sanitize_all_fields`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert, dass die Anwendung Cross Site Scripting und HTML-Injektionsangriffe durchführt
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Benutzerdaten an den Benutzer zurückgegeben werden. Wenn der Kunde eine Anpassung hat, die das Rendern der HTML-Attribut- oder Inhaltsdaten umfasst, hat dies Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Hoch) Benutzereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden. Dadurch werden clientseitige Cross-Site-Scripting-Angriffe durch Ausgabecodierung der Daten reduziert.
Workaround	Diese Eigenschaft bereinigt alle HTML-Felder im System. Wenn Sie die HTML-Bereinigung für einzelne Felder aktivieren müssen, finden Sie weitere Informationen unter Bereinigung einzelner Felder aktivieren. Sie können auch die Aufnahme- oder Ausschlussliste konfigurieren, um HTML-Tags und -Attribute gemäß den Richtlinien Ihrer Organisation zu bereinigen.
Referenzen	Aktivieren der HTML-Bereinigung HTML-Bereinigung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Beschränken zulässiger Java-Pakete

Durch die Konfiguration dieser Eigenschaften wird verhindert, dass gefährliche APIs für die Skript-Engine verfügbar gemacht werden.

Konfigurieren Sie die Systemtabellen, und installieren Sie das empfohlene Plugin entsprechend.

Wenn die Tabellen `sys_whitelist_member` und `sys_whitelist_package` keine leeren Werte sind, können gefährliche APIs für die Skript-Engine verfügbar gemacht werden. Einträge entsprechen dem Java-Namespace, die nicht von ServiceNow Sicherheitsteams genehmigt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren Sie das Tool zum Entfernen von Paketaufrufen. Details siehe Tool zur Paketaufrufentfernung.

Wenden Sie sich an Kundenservice und Support, um diese Tabellen zu bearbeiten.

Weitere Informationen

Attribut	Beschreibung
Tabelle, Plugin-Name	Tabellen: • *sys_whitelist_member* • *sys_whitelist_package* Plugin: com.glide.script.packages_call_removal
Konfigurationstyp	Tabellarische Konfiguration, Plugins
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Schützen Sie vor gefährlichen APIs, die der Skript-Engine ausgesetzt sind.
Empfohlener Wert	Leer
Konfigurationstyp	Tabellenliste, Plugin
Funktionale Auswirkung	
Sicherheitsrisiko	(Hoch) Gefährliche APIs sind möglicherweise für die Skript-Engine verfügbar. Diese unterstützten APIs führen wahrscheinlich zu Instabilität und Ungewissheit innerhalb der Instanz.
Sicherheitsrisikobewertung	8.2

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Tool zur Paketaufrufentfernung

Aktivieren Sie das Plugin „Packages Call Removal Tool“ (*com.glide.script.packages_call_removal*), und führen Sie es aus, und überlegen Sie dann, ob jede der vorgeschlagenen Änderungen abgeschlossen oder abgelehnt werden soll.

Das Tool zur Paketaufrufentfernung ist ein Plugin, das:

- Durchsucht Skripts nach Paketaufrufen für Now Platform Java-Klassen.
- Schlägt Änderungen vor, um sie durch bevorzugte GlideScriptable-Namen zu ersetzen.
- Erleichtert die Skriptänderungen.

Hinweis:
Wenn es sich bei diesem Datensatz um einen Basissystemdatensatz handelt, wird das Element bei Verwendung der Empfehlung des Tools als customer_update markiert. Es kann jedoch dennoch nützlich sein, dieses Tool zu verwenden, da es Packages,xxx-Aufrufe kennzeichnet.

Das Tool zur Paketaufrufentfernung meldet möglicherweise einige Paketaufrufe, die in „sa_mapping_ext_commands“ und „sa_custom_operation“verwendet werden. Diese Paketaufrufe gehören zum MID Server. Da keine Klassen vorhanden sind, wird der Code

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in MID Server ausgeführt. Wenn Sie einen der folgenden aufgelisteten Paketaufrufe im Abschnitt „Fehler“ finden, markieren Sie ihn als Abgelehnt (Ignoriert). Das Tool meldet diesen Paketaufruf nicht mehr.

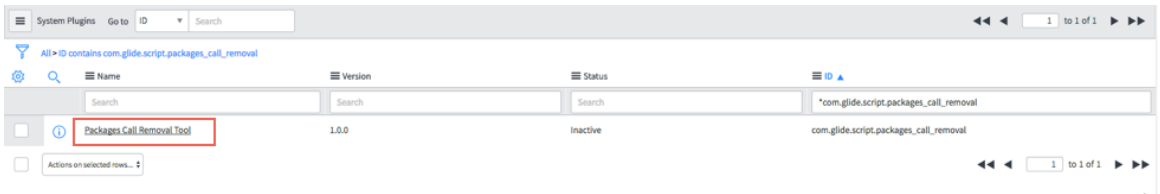
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
- `Packages.com.snc.sw.commands.HttpCallHandler;`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.script.packages_call_removal
Konfigurationstyp	Systemdefinition > Plugins
Zweck	Zum Entfernen/Ersetzen nicht autorisierter Paket-/Mitgliedsaufrufe mit von Glide akzeptierten Namen (GlideScriptable), die nur autorisierten Zugriff auf Daten zulassen.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Paketaufrufe durch `GlideScriptable-` APIs ersetzen und kann sich auf die Anpassungen auswirken, die Paketaufrufe enthalten. Das Tool ersetzt Paketaufrufe nicht automatisch. Stattdessen werden Vorschläge bereitgestellt, die in der Tabelle „packages_call_item“ gespeichert werden. Ihr Administrator kann dann entscheiden, ob er die vorgeschlagene Änderung akzeptiert oder ablehnt.
Sicherheitsrisiko	(Mittel) Clientseitige API-Aufrufe, die zum Datenabruf oder Objektzugriff auf dem Server führen, gelten aus Sicherheitsgründen als gefährlich. Sie sollten auf Autorisierung und Einschränkung für den Zugriff auf vertrauliche Objekte validiert werden.

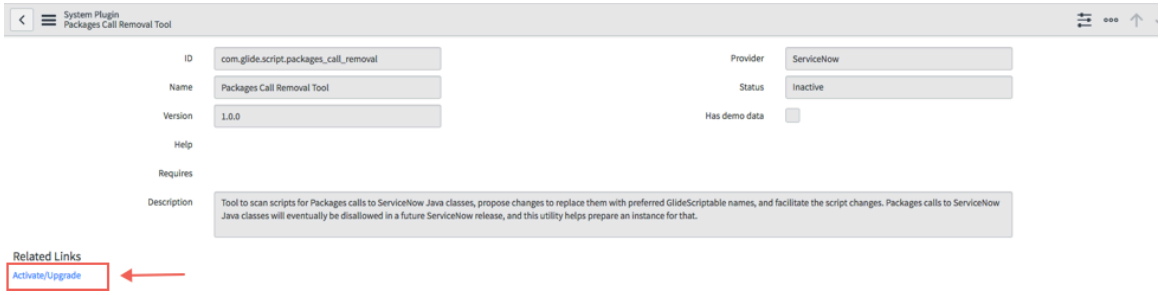
Schritte zum Konfigurieren von

1. Navigieren zu **Systemdefinition** > **Plugins**

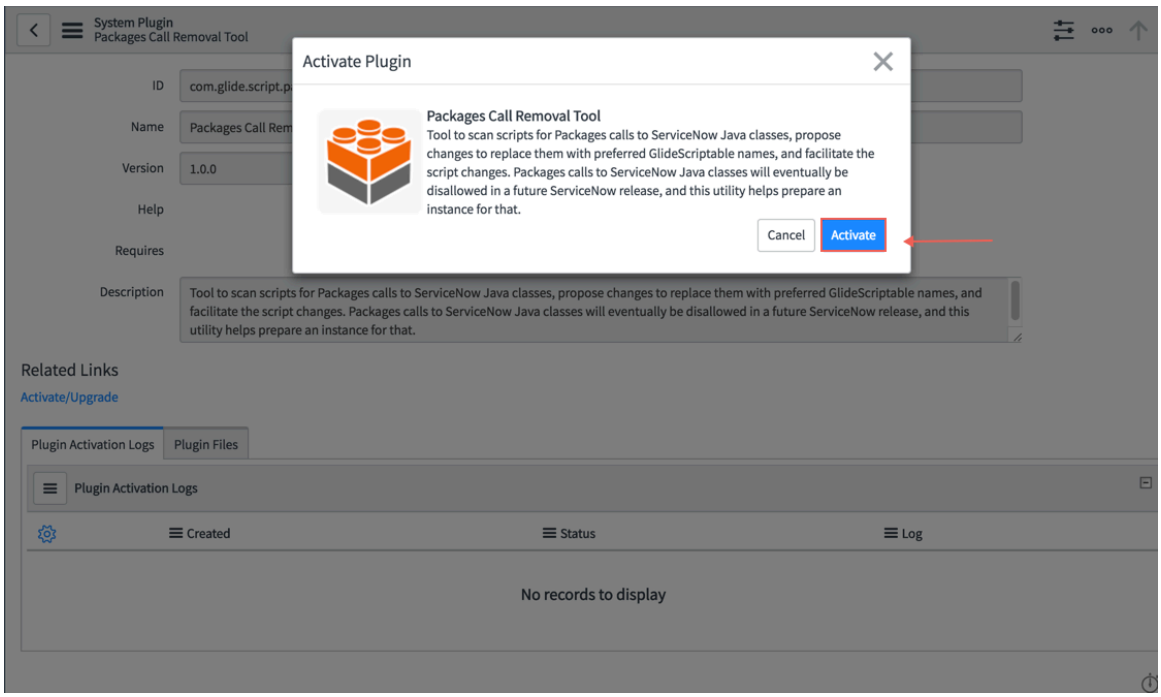


2. Suchen Sie nach der Plugin-ID = `com.glide.script.packages_call_removal`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Aktivieren/Aktualisieren**, um das Plugin zu aktivieren.



4. Um Aufrufe von Aufnahmelistenpaketen und Aufnahmelistenmitgliedern zu überprüfen, führen Sie die Aktionen aus, die in den Abschnitten „Schritte zum Konfigurieren“ in den folgenden Themen beschrieben sind:
   - Aktivieren Sie Listenmitgliedsaufrufe zulassen
   - Aktivieren Sie die Allow-Liste für Paketaufrufe

Anfänglicher eindeutiger LDAP-Name aufheben [Aktualisiert in Security Center 1.3]

Verwenden Sie diese Eigenschaft, um den eindeutigen Namen eines LDAP-Server-Datensatzes zu verwalten.

Diese Eigenschaft steuert den eindeutigen Namen eines LDAP-Server-Datensatzes, der eingefügt wird, wenn ein sofort einsatzbereites Korrekturskript ausgeführt wird. Wenn der Wert auf den empfohlenen Wert „“ festgelegt oder leer gelassen wird, können LDAP-Serverdaten von einem Benutzer mit geringeren Berechtigungen aufgezählt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ldap.initial.dn`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	leer
Standardwert	leer
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn der Eigenschaftswert auf „“ festgelegt oder leer gelassen wird, sind LDAP-Serverdaten möglicherweise für einen Benutzer mit geringeren Berechtigungen zugänglich.
Abhängigkeiten und Voraussetzungen	Keine

Strikte Sicherheit von Sitzungscookies erzwingen

Verwenden Sie die Eigenschaft `glide.ui.secure_cookies`, um ordnungsgemäß formatierte Cookies zu erfordern

Wenn Sie die Eigenschaft auf „true“ festlegen, lehnt Ihre Instanz eine Sitzung ab, wenn das zugeordnete Cookie nicht das erwartete Format aufweist.

⚠ Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.secure_cookies`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft auf „true“ festgelegt ist, werden falsch formatierte Cookies abgelehnt. Wenn ein solches Cookie abgelehnt wird, muss sich der Benutzer erneut anmelden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Schwellenwert für Entitätserweiterung minimieren [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft `glide.xmlutil.max_entity_expansion`, um die maximale Entitätserweiterungsgrenze in eine kleinere Zahl zu ändern.

Now Platform verarbeitet keine weiteren Entitätserweiterungen, die größer als der in dieser Eigenschaft angegebene zulässige Grenzwert sind.

Hinweis:
500 ist das von Now Platformfestgelegte Standardminimum, das als sicherer Schwellenwert gilt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.xmlutil.max_entity_expansion`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich vor XML-Entitätserweiterungs-/Billion-Lach-Angriffen zu schützen.
Empfohlener Wert	3000
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung die Erweiterung großer Entitäten verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Mittel) Ein Angreifer kann diese Schwachstelle verwenden, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Hochgeladene MIME-Typen beschränken [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft `glide.security.file.mime_type.validation`, um die MIME-Typprüfung für Uploads zu aktivieren. Sie können die MIME-Typvalidierung für Dateianhänge aktivieren (setzen Sie die Eigenschaft auf **true**) oder deaktivieren (setzen Sie sie auf **false**).

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, legen Sie die Eigenschaft `glide.attachment.extensions` fest. Nur die in `glide.attachment.extensions` angegebenen Erweiterungen werden während des Uploads auf den MIME-Typ überprüft. Weitere Informationen finden Sie unter Restrict file extensions .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.file.mime_type.validation`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Erzwingt die Überprüfung des MIME-Typs/der „Magic Byte“ beim Datei-Upload.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Mittel) Diese Fehlerkorrektur ermöglicht die Überprüfung des MIME-Typs für die Anhänge der Anwendung. Keine Auswirkungen auf die Funktionalität, es sei denn, es liegt eine böswillige Absicht beim Hochladen der Dateien vor, da bei dieser Validierung lediglich nach Synchronisierungsfehlern zwischen dem MIME-Typ und den Daten gesucht wird.
Sicherheitsrisiko	(Mittel) Um Schwachstellen wie Dateieinschluss und Uploads schädlicher Dateien zu reduzieren, sollte die MIME-Typverifizierung aktiviert sein.
Referenzen	Administering attachments

Weitere Informationen zum Konfigurieren von Eigenschaften für die Härtung finden Sie unter Härtungseinstellungen für die Instanzsicherheit.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Beschränken Sie externe XML-Entitäten

Verwenden Sie die Eigenschaft `glide.security.file.mime_type.validation`, um die MIME-Typprüfung für Uploads zu aktivieren. Sie können die MIME-Typvalidierung für Dateianhänge aktivieren (setzen Sie die Eigenschaft auf **true**) oder deaktivieren (setzen Sie sie auf **false**).

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, legen Sie die Eigenschaft `glide.attachment.extensions` fest. Nur die in `glide.attachment.extensions` angegebenen Erweiterungen werden während des Uploads auf den MIME-Typ überprüft.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.xml.entity.whitelist`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XXE-Angriffe zu schützen.
Empfohlener Wert	Wahr
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine externe Entität verwendet, die nicht in der Eigenschaft `glide.xml.entity.whitelist` aufgeführt ist, blockiert die NOW-Plattform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Kritisch) Ein Angreifer kann die DTD verwenden, um beliebige HTTP-Anforderungen einzuschließen, die der Server ausführen könnte. Dies kann zu anderen Angriffen führen, die die Vertrauensstellung des Servers zu anderen Entitäten nutzen.

Erfordert XMLdoc2-Entitätsvalidierung mit allowlistDisable-Entitätserweiterung

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie die Eigenschaft `glide.xmlutil.max_entity_expansion`, um die Erweiterung externer Entitäten vollständig zu deaktivieren. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

- Wenn Sie diese Eigenschaft auf **true**festlegen, versuchen alle externen Entitäten, abhängig von der Einstellung der Eigenschaft `glide.stax.whitelist_enabled`, Betreffentitäten aufzulösen oder zu erweitern.
- Wenn Sie diese Eigenschaft auf „ **false**“ festlegen, werden alle Entitätsauflösungen und -erweiterungen blockiert. Weitere Informationen finden Sie unter XMLdoc2-Entitätsvalidierung mit Allow-Liste.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaften `glide.xml.entity.whitelist.enabled` und `glide.stax.whitelist_enabled` auf „true“ fest. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste und XMLdoc2-Entitätsvalidierung mit Allow-Liste.
- Definieren Sie eine Liste von kommagetrennten FQDNs in der Eigenschaft `glide.xml.entity.whitelist`. Dies sind die einzigen URLs, die über die Verarbeitungseigenschaft XML-Entität erreicht werden können. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

Warnung:
Dies ist eine Safe-Harbor-Eigenschaft, was bedeutet, dass der Wert nicht mehr geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.xmlutil.max_entity_expansion`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen XML-Entitätserweiterungs-/Billion-Lach-Angriff zu schützen.
Empfohlener Wert	false
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Kritisch) Ein Angreifer kann diese Schwachstelle verwenden, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.
Workaround	Wenn die Anpassung eine Entitätserweiterung erfordert, legen Sie diese Eigenschaft auf „true“ fest, und führen Sie die in XMLdoc2-Entitätsvalidierung mit Allow-Listedokumentierten Schritte aus.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Weitere Informationen zu OWASp-Ressourcen finden Sie unter OWASp .

Sicherheitsrichtlinie für sichere Inhalte für SVG-Dateien festlegen [Neu in Security Center 1.3]

Die Eigenschaft `com.glide.csp.self_script_src_svg` fügt dem HTTP Content-Security-Policy-Header die Direktive „ **script-src none** “ hinzu, wenn über die Dateierweiterung Translation Memory Index (IIX) auf skalierbare Vektorgrafiken (SVGs) zugegriffen wird.

Die Eigenschaft `com.glide.csp.self_script_src_svg` verhindert, dass schädliche Dateianhänge, die Cross Site Scripting-Angriffe (XSS) speichern, in einer Instanz ausgeführt werden. Ohne diese Richtlinie könnte ein schlechter Akteur einen Benutzer dazu veranlassen, beliebigen JavaScript-Code in seinem Webbrowser auszuführen, was zu Sicherheitsschwachstellen wie Datenexfiltration und Sitzungsübernahme führen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.csp.self_script_src_svg`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	Wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt wird, kann dies dazu führen, dass ein Benutzer beliebigen JavaScript-Code von einem fehlerhaften Akteur ausführt.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft verhindert, dass skalierbare SVG-Dateien (Vektorgrafiken) auf externe Skripts zugreifen.

Encryption and Key Management

Verschlüsselung ist ein kryptografisches Verfahren, das Klartext in Geheimtext umwandelt, um die Offenlegung von Informationen zu steuern.

Übersicht

ServiceNow Die Schlüsselverwaltung umfasst die Aktivitäten im Zusammenhang mit dem Umgang mit kryptografischen Schlüsseln und zugehörigen Sicherheitsparametern während des End-to-End-Schlüssellebenszyklus und ist eine effektive Kontrolle basierend auf den Richtlinien 800-57 des National Institute of Standards and Technology (NIST).

Die Verschlüsselung wird verwendet, um Klartextzeichenfolgen in Geheimtext zu konvertieren, der ohne Zugriff auf den richtigen Schlüssel nicht entschlüsselt werden kann. Die Sicherheitsvorteile der Verschlüsselung ergeben sich aus der Kombination von robusten Algorithmen und hochwertiger Schlüsselverwaltung.

Die Verschlüsselung aller Informationen ist möglicherweise nicht für alle Daten erforderlich und würde die Verarbeitungszeit aufgrund der großen Anzahl von Daten, die in allen Anwendungen unterstützt werden, erheblich verlängern. Wenn Sie feststellen, dass für Daten eine Verschlüsselung erforderlich ist, sind diese Now Platform Optionen verfügbar:

Erste Schritte

Key Management Framework (KMF)	Verschlüsselung auf Spaltenebene (CLE)	Verschlüsselung auf Spaltenebene Enterprise (CLE_Ent)
Mit der [qa: BEGIN review][End] Key Management Framework (KMF) API/UX können	Eine integrierte Anwendung, die die Verschlüsselung von Zeichenfolgen-, Datums-, Datums-/Uhrzeit- oder Anhangsfeldern mit AES-128 oder AES-256 in	Bietet eine umfangreichere Verschlüsselungslösung als die Verschlüsselung auf Spaltenebene, z. B.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie die kryptografischen Vorgänge in Ihrer [qa: BEGIN review][End] ServiceNow-Instanz vollständig anpassen und verwalten.	Verschlüsselungsmodulen ermöglicht.	vom Kunden bereitgestellte Schlüssel, Skriptzugriff über APIs, zusätzliche kryptografische Module und Modulzugriffsrichtlinien und vieles mehr.
Cloud-Verschlüsselung Mit Cloud Encryption können Sie einen von [qa: BEGIN review][End] ServiceNow generierten Schlüssel verwenden oder einen von Ihnen erstellten und verwalteten Schlüssel angeben.	**Platform Encryption-Berechtigungspaket** Führen Sie ein Upgrade auf Column Level Encryption Enterprise, Cloud Encryption und Database Encryption mit unbegrenzter Nutzung durch.	**Full Disk Encryption (FDE)** Die vollständige Festplattenverschlüsselung wendet die Verschlüsselung nur auf das gesamte Speichersystem innerhalb des Datenbankservers an. Dies ist die einzige Komponente, die Kundendaten speichert.
	Edge Encryption Verschlüsselt vertrauliche Daten in Ihrem Unternehmen, bevor Daten über das Internet an Ihre [qa: BEGIN review][End] ServiceNow-Instanz gesendet werden. Daten bleiben in der Instanz im Ruhezustand verschlüsselt.	

Aktivierungsinformationen

Das Abonnementpaket ServiceNow Platform Encryption ist eine kommerzielle Gruppenberechtigung, die Verschlüsselung auf Spaltenebene Enterprise, Cloud-Verschlüsselungund Datenbankverschlüsselung enthält.

Verschlüsselung auf Spaltenebene Enterprise ist die unbegrenzte Lizenz von Verschlüsselung auf Spaltenebene. Das Plugin Verschlüsselung auf Spaltenebene Enterprise ist mit der Aktivierung des Plugins com.glide.now.platform.encryption verfügbar. Weitere Informationen finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

Key Management Framework erkunden

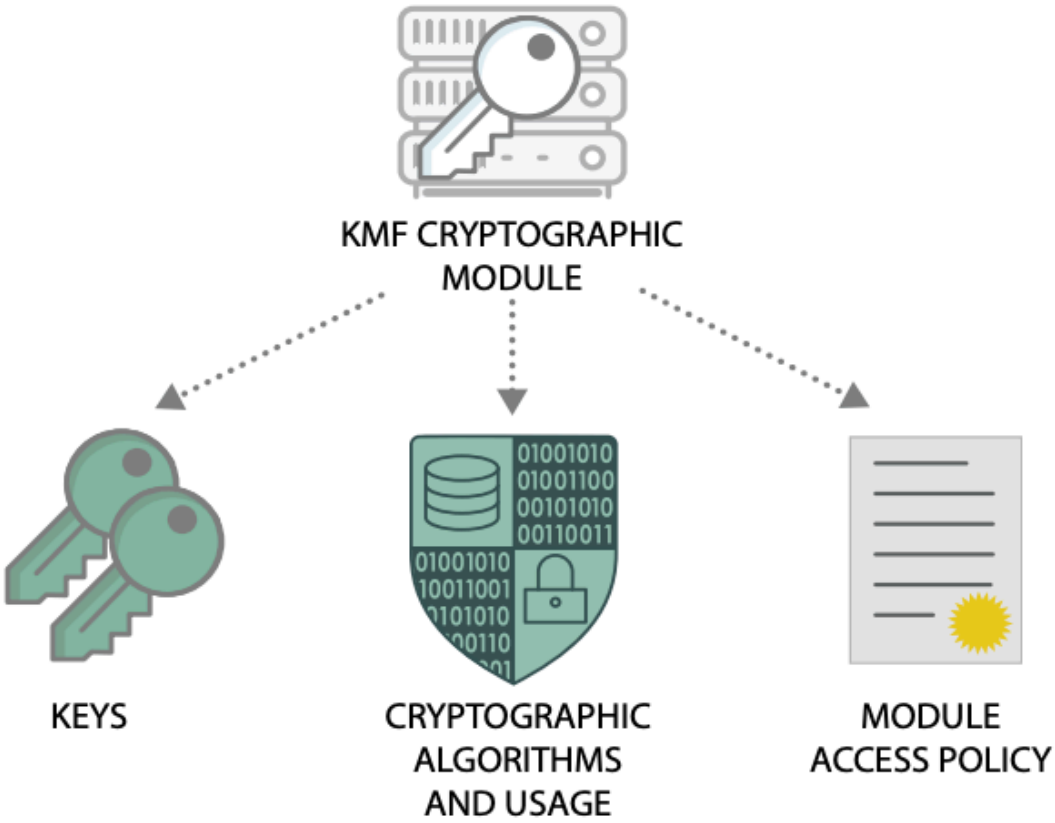
Mit der KMF-API/UX (Key Management Framework) können Sie die Ausführung kryptografischer Vorgänge in Ihrer Instanz vollständig anpassen und verwalten. KMF bietet

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine sichere und umfassende Schnittstelle für kryptografische Schlüsselverwaltungsservices auf der Instanzseite.

Key Management Framework – Übersicht



Diese Grafik zeigt die Komponenten, aus denen die KMF besteht.

KMF-Kryptografiemodule

Kryptografische Module sind das Herzstück der KMF. Jedes kryptografische Modul in Ihrer Instanz definiert eine Verschlüsselungsmethode für einen bestimmten Anwendungsfall. Weitere Informationen zu diesen Modulen finden Sie unter Übersicht über das kryptografische Modul.

Schlüssel

Kryptografische Schlüssel sind Zeichenfolgen, die in der Kryptografie verwendet werden. Wenn sie zusammen mit einem kryptografischen Algorithmus verwendet werden, können sie kryptografische Daten codieren oder decodieren. Diese Schlüssel werden von Ihren kryptografischen Modulen verwendet. Sie können einen generierten Schlüssel verwenden oder Ihren eigenen vom Kunden bereitgestellten Schlüssel mit Column Level Encryption Enterprise hochladen. Weitere Informationen zu -Schlüsseln finden Sie unter Schlüssel auf Instanzebene im Key Management Framework.

Kryptografische Algorithmen

Kryptografische Algorithmen sind Berechnungsverfahren, die einen kryptografischen Schlüssel zum Codieren oder Decodieren Ihrer Daten verwenden. Diese Algorithmen werden durch die Konfiguration der kryptografischen Spezifikation in Ihrer Instanz definiert.

Modulzugriffsrichtlinien

Modulzugriffsrichtlinien sind die Zugriffskontrollmechanismen, die auf kryptografische Module angewendet werden, um Steuerungen auf Instanzebene zu definieren. Diese Richtlinien legen die Bedingungen fest, unter denen der Zugriff auf kryptografische Module gewährt oder verweigert wird. Weitere Informationen finden Sie unter Übersicht über die Modulzugriffsrichtlinie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Key Management Framework-Workflow

1. Weisen Sie KMF Administratoren zu, die ihrerseits andere KMF Rollen zuweisen können.
2. Konfigurieren Sie Ihre Feldverschlüsselungseinstellungen, um entweder die von ServiceNow bereitgestellten Schlüssel oder Ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auszuwählen.
3. Erstellen Sie kryptografische Module, um die für kryptografische Vorgänge verwendeten Mechanismen zu definieren.
4. Erstellen Sie eine kryptografische Spezifikation, in der Sie einen Algorithmus für die Verschlüsselung definieren und einen Schlüssel generieren.
5. Erstellen Sie Modulzugriffsrichtlinien, die bestimmen, in welchen Kontexten Ihre Daten verschlüsselt oder entschlüsselt werden können.
6. Erstellen Sie eine Lebenszyklusrichtlinie für kryptografische Module. Diese Richtlinien begrenzen kryptografische Module auf Instanzebene, z. B. wie lange der Schlüssel gültig ist. Diese Richtlinien können kryptografische Module schützen, indem sie deren Gefährdung begrenzen.

Weitere Informationen zu diesen Prozessen finden Sie unter .

Vorteile von Key Management Framework

Vorteil	Funktion	Benutzer
Schützen Sie Ihre vertraulichen und geschützten Daten.	Verschlüsselung und Schlüsselverwaltung	Alle
Sorgen Sie für Compliance mit den NIST 800-57- Richtlinien. Diese Richtlinien werden vom National Institute of Standards and Technology bereitgestellt, um das Cybersicherheitsrisiko für Ihre Netzwerke und Daten zu reduzieren.	Verschlüsselung und Schlüsselverwaltung	Sicherheitsadministratoren
Verwenden Sie das Key Management Framework, um Ihre kryptografischen Schlüssel zu generieren, hochzuladen, anzuzeigen und zu verwalten. Verwenden Sie die Schlüsselrotation für die manuelle oder geplante Rotation Ihrer Schlüssel, um die Sicherheit zu erhöhen.	Key Management Framework	Sicherheitsadministratoren

Abonnementpaket für Verschlüsselung und Schlüsselverwaltung

Mit der Schlüsselverwaltung wird die Verschlüsselung auf Spaltenebene ohne zusätzliche Kosten auf die hochgradig konfigurierbaren Verschlüsselungsmodule aktualisiert. Sie haben auch die Möglichkeit, ein Upgrade auf die unbegrenzt nutzbare Lizenz durchzuführen. Abonnieren Sie das neue Verschlüsselungsberechtigungspaket Platform Encryption, das Verschlüsselung auf Spaltenebene Enterprise und Cloud-Verschlüsselungenthält.

Funktionen der Verschlüsselung auf Spaltenebene

Die Verschlüsselung auf Spaltenebene mit Verschlüsselungsmodulen ist in Ihrer Instanz kostenlos enthalten und umfasst die Schlüsselverwaltung NIST 800-57 . Dabei wird Folgendes unterstützt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ServiceNow verwaltete Schlüssel werden unterstützt (vom Kunden bereitgestellte Schlüssel werden nicht unterstützt).
- Der Zugriff auf Verschlüsselungsmodule ist nur rollenbasiert.
- Unbegrenzte manuelle Schlüsselrotation.
- Es können maximal fünf Verschlüsselungsmodule gleichzeitig vorhanden sein.
- Es können maximal fünf Modulzugriffsrichtlinien gleichzeitig vorhanden sein.
- Vorhandene Feldtypen werden unterstützt. (Neue Feldtypen, die in späteren Versionen erstellt wurden, werden in der Nicht-Enterprise-Version nicht unterstützt.)
- API-Support kann basierend auf dem Rollenzugriff verwendet werden.
- Audit von Verschlüsselungsaktionen.
- Guided Tour zur Verschlüsselung auf Spaltenebene.

ServiceNow Gruppenfunktionen der Plattformverschlüsselung

Die Gruppe „Plattformverschlüsselung“ fügt die folgenden Funktionen und Angebote hinzu:

- Column Level Encryption Enterprise:
  - Vom Kunden bereitgestellte Schlüssel.
  - Automatische Schlüsselrotation.
  - Erweiterte Unterstützung für Feldtypen und zukünftige Updates.

    Hinweis:
    Die Unterstützung erweiterter Feldtypen umfasst die Feldtypen **Journal**, **Journalliste**, **Journaleingabe**sowie **HTML und übersetzt (Feld/Text/HTML)**.

  - Erweiterte Unterstützung von Anhängen.
  - Der Zugriff auf das Verschlüsselungsmodul kann mit einer Modulzugriffsrichtlinie gewährt werden, die auf Folgendem basiert:
    - Systemanwender
    - Skript
    - Spezifische Anwendungsbereiche
  - Unbegrenzte Verschlüsselungsmodule und Modulzugriffsrichtlinien.
  - Importieren Sie einen Schlüssel aus einem Webservice.
  - Legen Sie ein zukünftiges Rotationsdatum für Verschlüsselungsschlüssel fest.
- Cloud-Verschlüsselung mit Schlüsselverwaltung.

Zusätzliche Informationen

Weitere Informationen zur Schlüsselverwaltung finden Sie unter Key Management Framework verstehen.

Key Management Framework verstehen

Mit der Key Management Framework (KMF) API/UX können Sie die Ausführung kryptografischer Vorgänge in Ihrer ServiceNow -Instanz vollständig anpassen und verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Key Management Framework bietet eine sichere und umfassende Schnittstelle für kryptografische Schlüsselverwaltungsservices auf der Instanzseite.

Gemäß NIST 800-57- Richtlinien bietet KMF die folgenden Funktionen:

- Aufgabentrennung mit dedizierten Rollen für kryptografische Verwaltung und Vorgänge, Audits und Integration
- Kryptografische Module ermöglichen die Konfiguration von kryptografischen Spezifikationen für eindeutige kryptografische Zwecke und Schlüsseltypen
  - Symmetrischer Schlüssel: Verschlüsselung und Entschlüsselung, Schlüssel einpacken und entpacken und Authentifizierung
  - Asymmetrischer Schlüssel: Generierung und Überprüfung digitaler Signaturen, Verschlüsselung und Entschlüsselung, Schlüsselumschließung und -entnahme
- Schlüssellebenszyklusverwaltung zum Generieren, Rotieren, Widerrufen und Anhalten von Schlüsseln, einschließlich Unterstützung mehrerer Schlüssellebenszyklusstatus
- Durchsetzung von Zugriffskontrollen mit Modulzugriffsrichtlinien, um sicherzustellen, dass der Zugriff nur auf die in den Richtlinien konfigurierten kryptografischen Module gewährt wird.
- Schlüsselschutz: Federal Information Processing Standard (FIPS) 140-2-L3 Hardware Root of Trust (RoT), Public Key Infrastructure (PKI), Schlüsselhierarchie und Umschlagverschlüsselung
- Auditing, das wichtige Nutzungsstatistiken enthält

KMF-Aktivierung

KMF ist standardmäßig aktiviert.

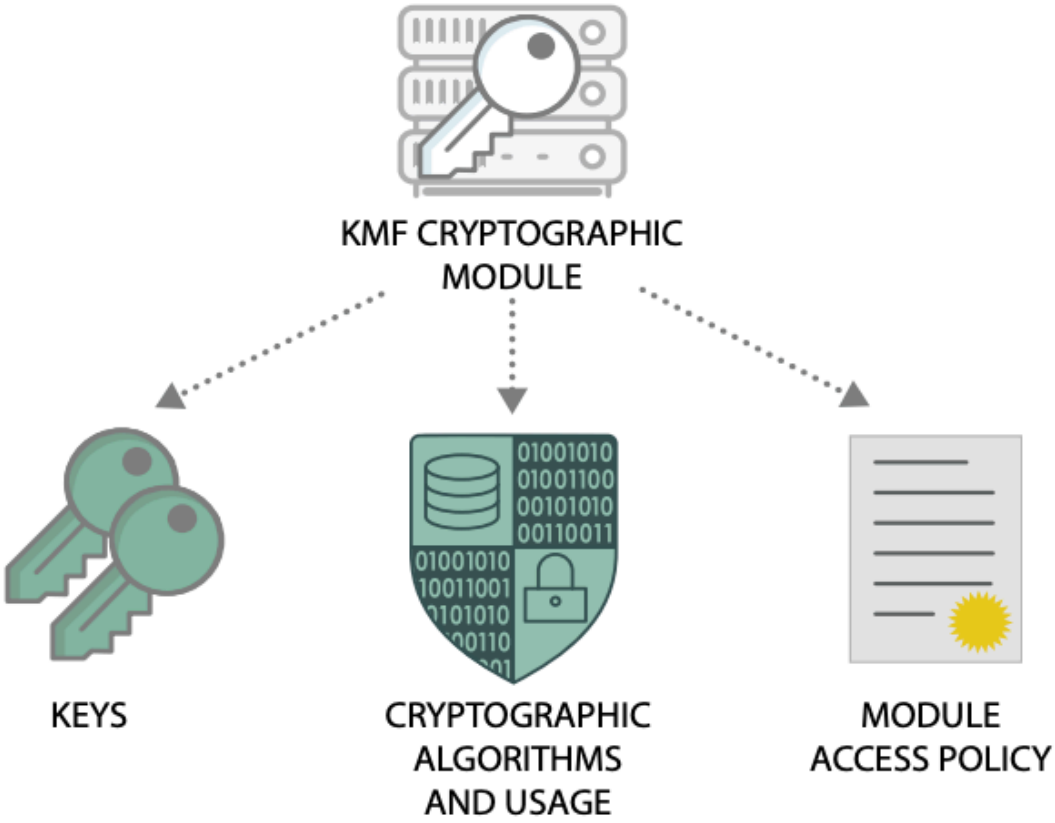
Hinweis:
KMF unterstützt keine Domänentrennung, kann jedoch mit lokalen Instanzen verwendet werden.

Funktionsweise von KMF

Diese Grafik zeigt die Komponenten, aus denen KMF besteht:

- Die kryptografischen Module werden verwendet, um die Verschlüsselungsmethode zu definieren.
- Die kryptografische Spezifikation ist eine Konfiguration, die einen Algorithmus für die Verschlüsselung definiert.
- Mit der Spezifikation können Sie auch den Schlüssel für das Modul, einen ServiceNow -Schlüssel oder Ihren eigenen vom Kunden bereitgestellten Schlüssel definieren.
- Eine Modulzugriffsrichtlinie ist eine Richtlinie auf Instanzebene, die die Bedingungen regelt, unter denen der Zugriff auf kryptografische Module gewährt oder verweigert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen zu KMF erhalten Sie, wenn Sie mit Übersicht über das kryptografische Modulbeginnen.

Das Key Management Framework (KMF) führt bestimmte Rollen für kryptografische Module und Konfigurationen im Zusammenhang mit der Schlüsselverwaltung ein. Nur KMF-Administratoren können Benutzer anderen KMF-Rollen zuweisen. Weitere Informationen finden Sie unter Mit Key Management Framework installierte Rollen.

Weitere Informationen zum Verschlüsselungs-Framework, das der Nachfolger von CLE ist, finden Sie unter Column Level Encryption Enterprise.

Übersicht über das kryptografische Modul

Kryptografische Module sind das Herzstück von (KMF). Sie definieren die spezifischen kryptografischen Mechanismen, die für kryptografische Vorgänge für einen bestimmten Anwendungsfall verwendet werden.

Ein kryptografisches Modul wendet den kryptografischen Mechanismus Ihrer Wahl auf einen von Ihnen definierten Anwendungsfall an. Wenn Sie beispielsweise die Daten in Ihrer HR-Anwendung mit einem AES-CBC mit einem symmetrischen 256-Bit-Schlüssel sichern möchten, können Sie zu diesem Zweck ein Modul erstellen.

Kryptografische Module unterstützen auch die Schlüssellebenszyklusverwaltung. Sie können Ihre kryptografischen Schlüssel erstellen und rotieren und Ihre Verschlüsselungsmethode definieren. Kryptografische Module bestehen aus den folgenden Komponenten:

Kryptografische Spezifikation

Definiert Aspekte Ihres Moduls, einschließlich seines kryptografischen Zwecks und der zu verwendenden Algorithmen.

Kryptografische Schlüssel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Schlüssel, den Ihr Modul zum Codieren oder Decodieren von kryptografischen Daten verwendet. Dies kann ein von Ihrer Instanz generierter Schlüssel oder ein vom Kunden bereitgestellter Schlüssel sein, den Sie erstellen und hochladen.

Modulzugriffsrichtlinien

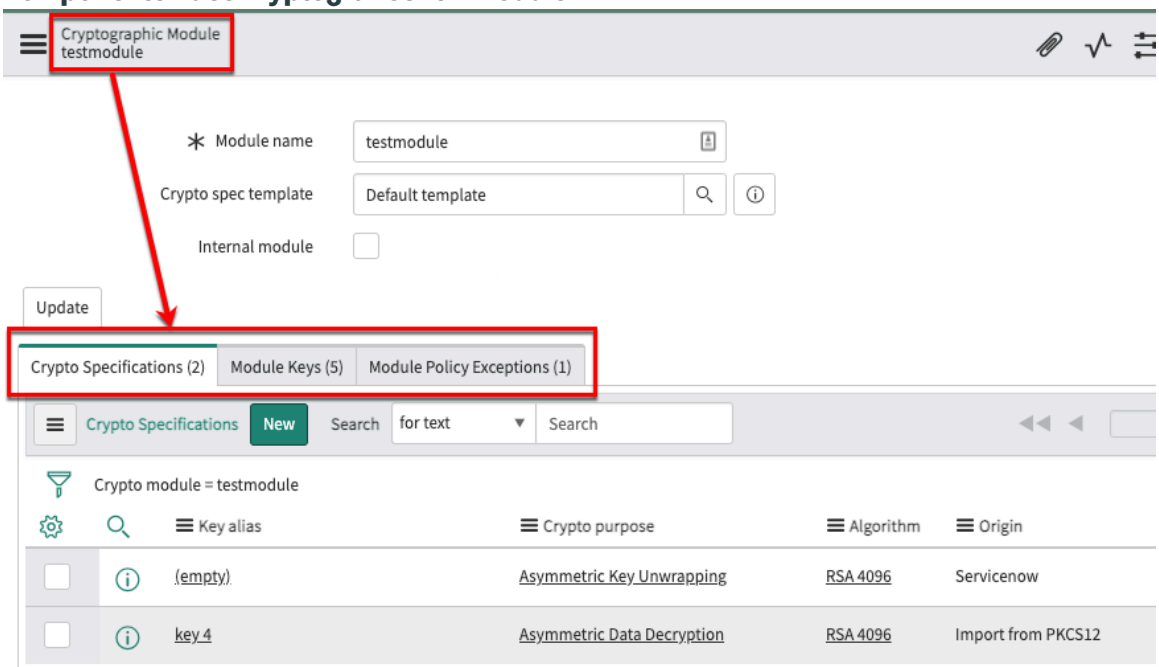
Modulzugriffsrichtlinien sind die Zugriffskontrollmechanismen, die einschränken, ob Daten verschlüsselt oder entschlüsselt werden können.

Modulrichtlinienausnahmen

Ein Steuerungsmechanismus zum Definieren von Ausnahmen für eine Modulzugriffsrichtlinie.

Der folgende Bildschirm zeigt diese allgemeinen Komponenten in einem kryptografischen Modul:

Komponenten des kryptografischen Moduls



Weitere Informationen zum Erstellen von kryptografischen Modulen finden Sie unter Erstellen Sie ein kryptografisches Modul.

Übersicht über die Modulzugriffsrichtlinie

Modulzugriffsrichtlinien sind die Zugriffskontrollen, die Sie auf Ihre kryptografischen Module anwenden, um Steuerungen auf Instanzebene zu definieren.

Modulzugriffsrichtlinien

Modulzugriffsrichtlinien werden mit Key Management Framework (KMF) im Basissystem eingeführt.

Hinweis:
Für die Nutzung der Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist ein -Abonnement erforderlich. Weitere Informationen zu [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Modulzugriffsrichtlinien erweitern die rollenbasierten Bezeichnungen, die mit den Verschlüsselungsmodulen bereitgestellt wurden. Modulzugriffsrichtlinien können auf Folgendem basieren:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

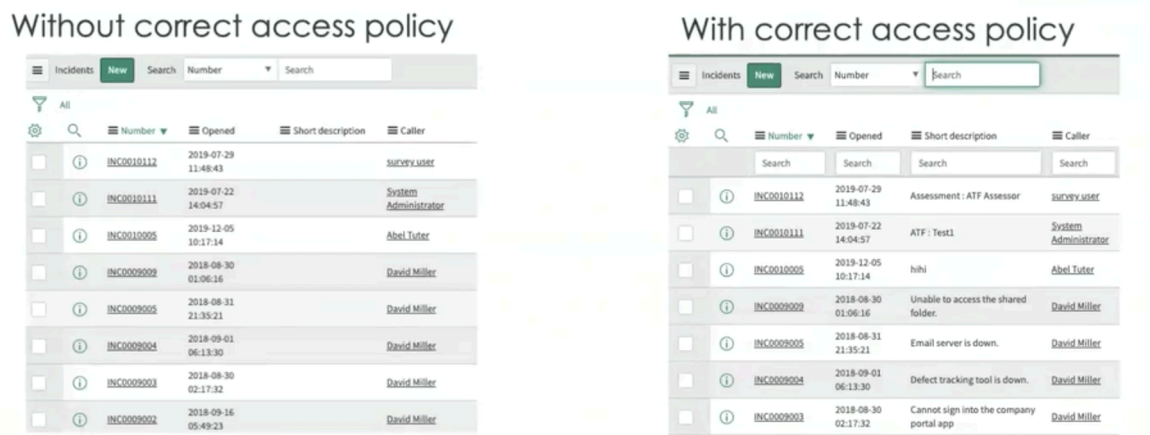
- Standard (Umfang)
- Rolle
- Systemanwender
- Skript
- Ressourcenaustausch

Hinweis:
Details siehe Key Management Framework Ressourcenaustausch.

In einem kryptografischen Modul müssen Sie die richtigen Modulzugriffsrichtlinien konfigurieren, um den Zugriff auf verschlüsselte Daten zuzuweisen. Ohne eine Modulzugriffsrichtlinie, die einem kryptografischen Modul zugeordnet ist, sind verschlüsselte Daten für Benutzer nicht sichtbar, und zugehörige Felder und Spalten in Listen werden leer angezeigt.

In dieser Abbildung wird der Inhalt für alle Benutzer ausgeblendet, die auf die Incident-Tabelle zugreifen, wenn im verschlüsselten Feld „Kurzbeschreibung“ keine Modulzugriffsrichtlinie vorhanden ist. Wenn eine Modulzugriffsrichtlinie vorhanden ist, können Benutzer mit der zulässigen Rolle die verschlüsselten Daten anzeigen.

Verschlüsselte Kurzbeschreibungen mit und ohne Modulzugriffsrichtlinien



Hinweis:
Die Daten in der Spalte werden auch Benutzern ohne die richtige Rolle angezeigt, die in der Modulzugriffsrichtlinie angegeben ist.

Informationen zum Setup finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

Autogen-Richtlinien

Autogen-Richtlinien werden automatisch vom System basierend auf der Standardmodulzugriffsrichtlinie generiert, die für das angegebene kryptografische Modul definiert ist. Dies sind Richtlinien auf globaler Ebene, die generiert und angewendet werden, wenn keine Richtlinien auf granularer Ebene definiert sind, wenn das System oder Skript versucht, auf das angegebene kryptografische Modul zuzugreifen.

Wichtig:

Autogen-Richtlinienregeln werden nicht für geplante Aufgabentypen oder Feldverschlüsselungsmodule (Module, bei denen das übergeordnete Modul „Verschlüsselung auf Spaltenebene“ ist) angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüssel auf Instanzebene im Key Management Framework

Die Key Management Framework (KMF)-Architektur führt eine Schlüsselstruktur ein, die unter Berücksichtigung der Sicherheit entwickelt wurde. Mit einem Hardware-Sicherheitsmodul (HSM) verwendet KMF eine Umschlagverschlüsselung, um sicherzustellen, dass alle Plattformschlüssel unter der Verwaltung von KMF durch eine Schlüsselkette geschützt sind. Von KMF erstellte Kundendaten-Verschlüsselungsschlüssel (Customer Data Encryption Keys, CDEKs) sind ebenfalls enthalten.

Auf Instanzebene definiert KMF mehrere Schlüssel, die intern für unterschiedliche kryptografische Zwecke in Now Platformverwendet werden.

Bei der Umschlagverschlüsselung wird ein Schlüssel mit einem anderen Schlüssel verschlüsselt. Die folgende Abbildung zeigt ein Beispiel für die Umschlagverschlüsselung. Hier werden CDEKs vom IKEK mit einem Umschlag verschlüsselt, der wiederum vom IRK mit einem Umschlag verschlüsselt wird, der schließlich vom RK mit einem Umschlag verschlüsselt wird. Da nur vom HSM auf den IRK zugegriffen werden kann, muss der IKEK zur Entschlüsselung hochgeladen werden.

Diese Tabelle enthält Beispiele für eine Teilmenge der verfügbaren Kunden-/App-Schlüssel, die von KMFverwaltet und geschützt werden.

Schlüssel	Standort	Beschreibung
Stammschlüssel (RK)	Hardware-Sicherheitsmodell (HSM)	Stammschlüssel, der zum Entschlüsseln des IRK verwendet wird.
Instanzstammschlüssel (IRK)	HSM	Ein für Ihre Instanz eindeutiger Schlüssel, der zum Verschlüsseln mehrerer interner Schlüssel der Instanz verwendet wird.
Instanz-HMAC-Schlüssel (IHK)	Instanz	Eindeutig pro Instanz. Der IHK wird intern für HMAC-Zwecke (Hash-Based Message Authentication Code) verwendet. Der IHK trägt zur Sicherstellung der Authentizität und Integrität von Modulschlüsseln bei und wird entweder in KeySecure oder den Dateischlüsselspeicher eingeschlossen.
Instance Key Encryption Key (IKEK)	Instanz	Der IKEK umschließt die Modulschlüssel und wird entweder in KeySecure oder den Dateischlüsselspeicher eingeschlossen.
Asymmetrischer Instanzverschlüsselungsschlüssel (IAEK)	Instanz	Ein für Ihre Instanz eindeutiger Schlüssel, der intern für asymmetrische Verschlüsselungszwecke verwendet wird. Die IAEK wird verwendet, um vertrauliche Nachrichten zwischen einer Instanz während der Verbrauchergenehmigung von Key Exchange oder Instanzübergreifende Datenreplikation zu übertragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüssel	Standort	Beschreibung
Instanzsignaturschlüssel (ISK)	Instanz	Ein für Ihre Instanz eindeutiger Schlüssel, der intern zum Signieren verwendet wird.
Password2 (PW2)	Instanz	Mit KMFwird der Schlüssel für Felder von [PW2 vollständig von KMFverwaltet.
Verschlüsselungsschlüssel für Kundendaten (CDEK)	Instanz	Mit KMF erstellte Verschlüsselungsschlüssel werden vom IKEK mit einem Umschlag verschlüsselt.
Instanzdatenreplikation (IDR) Datenverschlüsselungsschlüssel (DEK)	Instanz	Spezifische Verschlüsselungsschlüssel, die für den IDR-Prozess verwendet werden.

Kryptografischer Zweck, Algorithmen und Schlüsselinformationen

Kryptografische Spezifikationen können auf einen bestimmten kryptografischen Zweck zugeschnitten werden und decken sowohl asymmetrische als auch symmetrische schlüsselbasierte kryptografische Vorgänge ab. Die Auswahl eines kryptografischen Zwecks bietet weitere Auswahlmöglichkeiten, nämlich eine Reihe unterstützter Algorithmen und Schlüssellängenkonfigurationen.

Kryptografische Zwecke, Algorithmen und Schlüsselinformationen

Kryptografischer Zweck	Algorithmus	Schlüsselinformationen
Asymmetrische Datenentschlüsselung	RSA	Asymmetrisch – 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Asymmetrische Datenverschlüsselung	RSA	Asymmetrisch – 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Entpacken des asymmetrischen Schlüssels	RSA	Asymmetrisch – 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Asymmetrisches Schlüssel-Wrapping	RSA	Asymmetrisch – 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Signaturerzeugung	RSA	Asymmetrisch – 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Signaturverifizierung	RSA	Asymmetrisch – 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Symmetrische Authentizität	HMAC	Symmetrisch – 256-Bit-, 384-Bit- und 512-Bit-Schlüssel
Symmetrische Datenverschlüsselung/-entschlüsselung*	AES-CBC *	Symmetrisch – 128-Bit-, 192-Bit-, 256-Bit-Schlüssel
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	
Wrapping/Unwrapping symmetrischer Schlüssel*	AES-CBC *	Symmetrisch – 128-Bit-, 192-Bit-, 256-Bit-Schlüssel
	AES-CFB	
	AES-OFB	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kryptografische Zwecke, Algorithmen und Schlüsselinformationen (Fortsetzung)

Kryptografischer Zweck	Algorithmus	Schlüsselinformationen
	AES-CTR	
	AES-GCM **	

* AES-CBC unterstützt Optionen zur Gleichstellungserhaltung. Verschlüsselung auf Spaltenebene Enterprise verwendet AES-CBC.

** AES-GCM verfügt über eine integrierte Datenintegrität.

Die Konfiguration dieser Parameter wird in Erstellen Sie ein kryptografisches Modulbehandelt.

Schlüssel-Lebenszyklusstatus des Key Management Framework

KMF unterstützt mehrere kryptografische Schlüssel-Lebenszyklusstatus durch die Erzwingung bestimmter zulässiger Aktionen. Beispielsweise können nur Schlüssel, die sich im aktiven Status befinden, vollständig für den beabsichtigten kryptografischen Zweck verwendet werden. Die folgende Tabelle enthält weitere Details zu den verschiedenen Lebenszyklusstatus der Schlüssel.

Status oder Aktion des Schlüssellebenszyklus	Beschreibung
Aktiv	Es kann nur einen aktiven Schlüssel für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul geben.
Gefährdet	Mehrere Schlüssel können im gefährdeten Status für den Widerruf in einer bestimmten kryptografischen Spezifikation in einem kryptografischen Modul vorhanden sein. Jeder aktive oder ausgesetzte Schlüssel kann in einen gefährdeten Status verschoben werden. Gefährdete Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln oder Signieren, können jedoch dennoch verwendet werden, um den Zweck vorhandener Inhalte zu identifizieren, z. B. Entschlüsselung oder Überprüfung.
Deaktiviert	Jeder aktive Schlüssel kann deaktiviert werden. Für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul können sich mehrere Schlüssel in einem deaktivierten Status befinden. Wenn beispielsweise der Schlüssel rotiert wird, wird der aktuell aktive Schlüssel deaktiviert. Deaktivierte Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln und Signieren. Sie können jedoch weiterhin verwendet werden, um Zwecke vorhandener Inhalte zu identifizieren, z. B. Entschlüsselung oder Überprüfung. **Hinweis:** Gefährdete und widerrufene Schlüssel werden als deaktivierte Schlüssel behandelt.
Zerstört	Wenn ein Schlüssel vernichtet wird, wird das Schlüsselmaterial dauerhaft entfernt und kann nicht mehr für kryptografische Zwecke verwendet werden. Jeder deaktivierte Schlüssel kann mithilfe der Lebenszyklusautomatisierung vernichtet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status oder Aktion des Schlüssellebenszyklus	Beschreibung
	werden, wenn er im konfigurierten festgelegten Zeitrahmen nicht verwendet wurde. Für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul können sich mehrere Schlüssel im Status „Zerstört“ befinden. **Warnung:** Auf Daten, die einem zerstörten Schlüssel zugeordnet sind, kann nicht mehr zugegriffen werden. Daher ist bei der Aktion „Schlüssel vernichten“ äußerste Vorsicht geboten.
Generiert	Im generierten Status können mehrere Schlüssel für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul vorhanden sein. Ein generierter Schlüssel kann in einen aktiven Status verschoben werden, wenn für die angegebene kryptografische Spezifikation kein aktiver Schlüssel vorhanden ist. Der zuerst generierte Schlüssel wird automatisch auf „Aktiv“ gesetzt. **Hinweis:** Wenn die Auswahl besteht darin, einen neuen Schlüssel zu generieren, wird ein neuer Schlüssel generiert und aktiviert, obwohl Schlüssel in einem generierten Status für die angegebene kryptografische Spezifikation vorhanden sind.
Erneuert	Ein aktiver Schlüssel mit einem Ablaufdatum kann beliebig oft erneuert werden, um den Lebenszyklus des Schlüssels zu verlängern. **Hinweis:** Die Differenz zwischen dem Aktivierungsdatum und dem Ablaufdatum wird berechnet, und das Ablaufdatum wird um diese Dauer ab dem aktuellen Tag verschoben.
Fortfahren	Die UI-Aktion ist für ausgesetzte Schlüssel verfügbar, um sie wieder in einen aktiven Status zu verschieben, wenn kein anderer aktiver Schlüssel für die angegebene kryptografische Spezifikation vorhanden ist.
Widerrufen	Jeder aktive oder ausgesetzte Schlüssel kann in den widerrufenen Status verschoben werden. Widerrufte Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln oder Signieren, können jedoch dennoch verwendet werden, um den Zweck vorhandener Inhalte zu identifizieren, z. B. zur Entschlüsselung oder Überprüfung. Für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul können mehrere Schlüssel in einem widerrufenen Status vorhanden sein.
Rotiert	Die Schlüsselrotation führt dazu, dass der derzeit aktive Schlüssel deaktiviert und ein anderer Schlüssel aktiviert wird. Wählen Sie den neuen aktiven Schlüssel aus den folgenden aus: • Generierung eines neuen Schlüssels. • Zeigen Sie auf einen vorhandenen importierten Schlüssel. Jeder aktive Schlüssel kann rotiert werden.

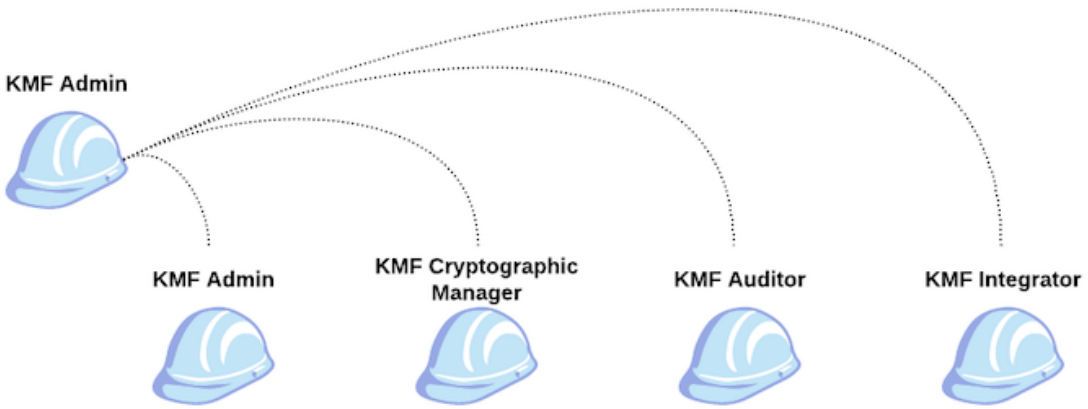
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status oder Aktion des Schlüssellebenszyklus	Beschreibung
Angehalten	Für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul können sich mehrere Schlüssel im Status „Angehalten“ befinden. Wenn der Schlüssel angehalten wurde, kann der Schlüssel fortgesetzt und einem aktiven Status zugewiesen werden, wenn kein anderer aktiver Schlüssel für diese kryptografische Spezifikation vorhanden ist.

Mit Key Management Framework installierte Rollen

Mit Key Management Framework (KMF) werden bestimmte Rollen für kryptografische Module und Konfigurationen im Zusammenhang mit der Schlüsselverwaltung eingeführt.

Wichtig:
Um die KMF-Administratorrolle zuzuweisen, benötigen Sie die Rollen „admin“, „security_admin“ und „sn_kmf_admin“. Verwenden Sie die KMF-Administratorrolle, um andere KMF-Rollen zuzuweisen. Weitere Informationen zum Zuweisen von KMF-Rollen finden Sie unter Weisen Sie KMF Rollen zu.



KMF-Administrator [sn_kmf.admin]

Weist anderen Benutzern Rollen zu, um Vorgänge rund um ServiceNow Key Management Frameworkdurchzuführen.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Wichtig:
Vermeiden Sie es, eine Administratorrolle zu gewähren, wenn spezialisiertere Rollen verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Diese Rolle wird über den in Weisen Sie KMF Rollen zugezeigten Prozess zugewiesen.
- Sie müssen über diese Rolle verfügen, um KMF-Rollen zuweisen zu können. Darüber hinaus können alle Funktionen des kryptografischen KMF-Managers ausgeführt werden.

KMF-Kryptografiemanager [sn_kmf.cryptographic_manager]

Erstellen, lesen und aktualisieren Sie Vorgänge für kryptografische Module (Zuordnung von Schlüsseln zu kryptografischen Verwendungs- und Algorithmuskonfigurationen) und Modulzugriffsrichtlinien. Außerdem können kryptografische KMF-Manager Schlüsselverwaltungs- (generieren, rotieren, widerrufen) und Lebenszyklusvorgänge durchführen.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

KMF-Kryptografieauditor [sn_kmf.cryptographic_auditor]

Zeigen Sie kryptografische Modulinformationen, Schlüsselmetadaten und lebenszyklusbezogene Details sowie MAP-Informationen (Modul Access Policy) an.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

KMF-Kryptografieintegrator [sn_kmf.cryptographic_integrator]

Integrieren Sie Key Management Framework mit externen Schlüsselspeichern oder Systemen.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Kryptografischer KMF-Operator [sn_kmf.cryptographic_operator]

Greifen Sie auf einen Teil des Schlüssellebenszyklus von ServiceNow Key Management Framework zu: Erneuerung, Rotation, Widerruf.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Weisen Sie KMF Rollen zu

Weisen Sie Administratoren KMF Rollen zu, die ihrerseits andere KMF Rollen zuweisen können.

Vorbereitungen
Erforderliche Rolle: admin und security_admin

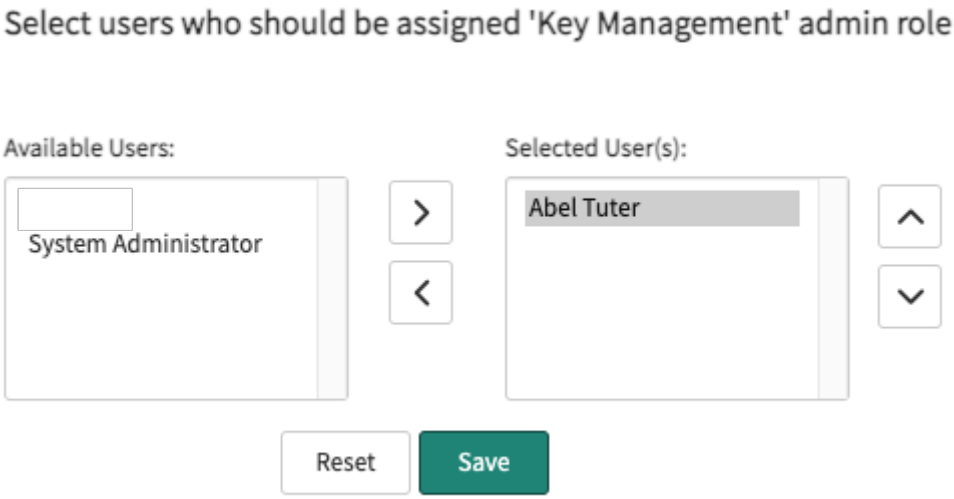
Sie müssen eine Erhöhung auf die Rolle „security_admin“ durchführen, bevor Sie die Administratorrolle KMF zuweisen. Anweisungen finden Sie unter Auf eine privilegierte Rolle erhöhen

Eine vollständige Liste der verfügbaren Rollen für KMF und ihre Beschreibungen finden Sie unter Mit Key Management Framework installierte Rollen.

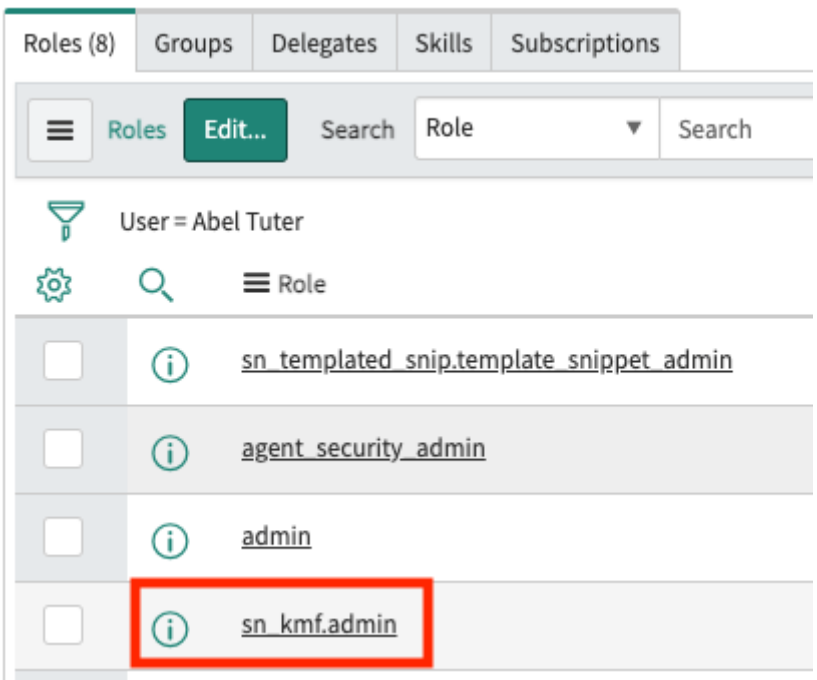
Prozedur

1. Erhöhen Sie auf die Sicherheitsadministratorrolle.
2. Navigieren zu **Benutzeradministration** > **Benutzer** und wählen Sie den Benutzer aus, der der KMF -Administrator sein soll.
3. Vergewissern Sie sich, dass der Benutzer bereits über die Rollen „admin“ und „security_admin“ verfügt. Wenn nicht, wählen Sie **Bearbeiten** in der zugehörigen Liste Rollen aus, und fügen Sie **admin** und **security _admin hinzu**.
4. Navigieren zu **Systemsicherheit** > **Administration der Schlüsselverwaltung**.
5. Wählen Sie in der Spalte **Verfügbare Benutzer** den Benutzer aus, den Sie als Administrator KMF festlegen möchten, und verschieben Sie ihn in die Spalte **Ausgewählter Benutzer**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie **Speichern**.
7. Navigieren zu **Benutzeradministration** > **Benutzer** und wählen Sie den Benutzer aus, dem Sie gerade die Rolle sn_kmf.admin zugewiesen haben.
   Der Benutzer hat die Rolle sn_kmf.admin in der zugehörigen Liste „ **Rollen** “ und kann andere KMF-Rollen zuweisen.

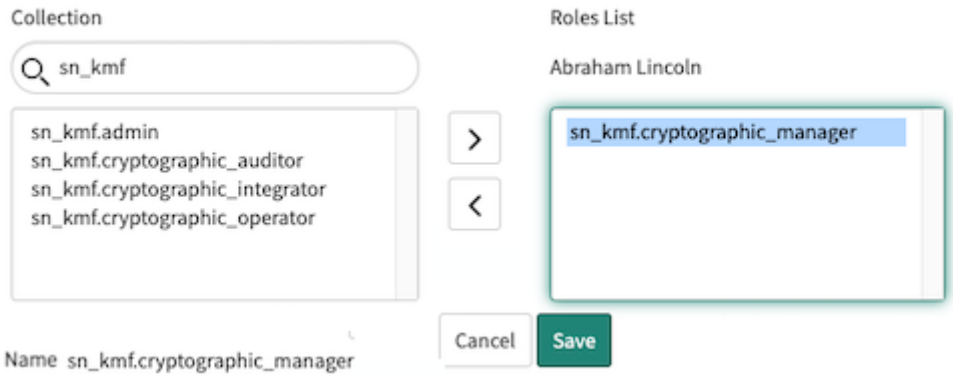


Nächste Maßnahme
Wenn Sie über die KMF-Administratorrolle verfügen, führen Sie die folgenden Schritte aus, um andere KMF-Rollen zuzuweisen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Benutzeradministration** > **Benutzer** und wählen Sie den Benutzer aus, dem Sie eine weitere KMF-Rolle zuweisen möchten, z. B. KMF-Kryptografiemanager.
2. Wählen Sie in der zugehörigen Liste „Rollen“ die Option **Bearbeiten** und dann die KMF-Rollen aus, die Sie den Benutzern zuweisen möchten. Alle KMF-Rollen beginnen mit sn_kmf.



Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen

Konfigurieren Sie Ihre Feldverschlüsselungseinstellungen so, dass die von ServiceNow bereitgestellten Schlüssel oder Ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auf der Now Platform verwendet werden.

Vorbereitungen

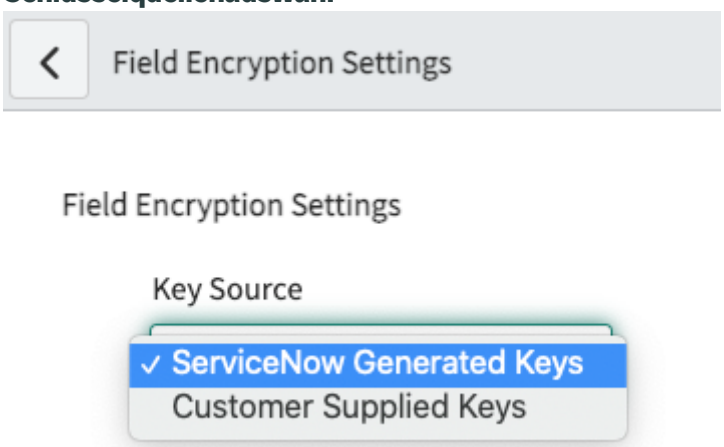
Vom Kunden bereitgestellte Schlüssel werden nur mit Verschlüsselung auf Spaltenebene Enterpriseunterstützt.

Erforderliche Rolle: sn_kmf.cryptographic_manager und security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Einstellungen für Feldverschlüsselung**.
2. Wählen Sie in den Feldverschlüsselungseinstellungen entweder von **ServiceNow generierte Schlüssel** oder vom **Kunden bereitgestellte Schlüssel** aus der Liste **Schlüsselquelle** aus.

Schlüsselquellenauswahl



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Option ändert die Eigenschaft com.glide.encryption.cle_kmf.key_source entweder in von **ServiceNow generierte Schlüssel** oder in vom **Kunden bereitgestellte Schlüssel**.

3. Wählen Sie **Speichern**.

Nächste Maßnahme

- Wenn Sie Ihre eigenen vom Kunden bereitgestellten Schlüssel verwenden, finden Sie weitere Informationen unter Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
- Wenn Sie die von ServiceNow bereitgestellten Schlüssel verwenden, beginnen Sie mit der Erstellung Ihres kryptografischen Moduls. Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul.

Erstellen Sie ein kryptografisches Modul

Erstellen Sie ein kryptografisches Modul, um die für kryptografische Vorgänge verwendeten Mechanismen zu definieren. Nachdem Sie das Modul erstellt haben, erstellen Sie eine kryptografische Spezifikation, in der Sie einen Algorithmus für die Verschlüsselung definieren und einen Schlüssel generieren.

Vorbereitungen

Wenn Sie Ihre eigenen Schlüssel angeben, wechseln Sie zu Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch.

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt Optionen, die mit KMF im Plattformbasissystem ServiceNow verfügbar sind. Die Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist nur verfügbar, wenn das Plugin *„com.glide.now.platform.encryption“* aktiv ist. Weitere Informationen zum Abrufen von [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise. Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene.

Hinweis:
Die Datensätze des kryptografischen Moduls [sys_kmf_crypto_module] können nicht gelöscht werden.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Neu erstellen**.
2. Füllen Sie die Felder im Formular aus.

Felder des kryptografischen Moduls

Feld	Beschreibung
Modulname	Alphanumerische Zeichenfolge, auf die beim Ausführen von Skripts verwiesen werden soll.
Krypto-Spezifikationsvorlage	Wählen Sie die Vorlage **Standard** aus, die zum Erstellen des kryptografischen Moduls verwendet werden soll, da sie Zuordnungen unterstützter Algorithmen für Krypto-Spezifikationen enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Standardwert der Modulzugriffsrichtlinie	○ Auf Systemstandard angewiesen: ○ Ablehnen ○ Titel
Tatsächliches Ergebnis der Modulzugriffsrichtlinie	Ablehnen oder nachverfolgen, basierend auf dem Standardrichtlinienwert oder dem Wert, der bei der Erstellung der Modulzugriffsrichtlinie ausgewählt wurde.
Name	Name des kryptografischen Moduls, dem der Name des Anwendungsbereichs vorangestellt ist.
Lebenszyklusstatus des kryptografischen Moduls	Der Lebenszyklus bezieht sich auf die Erstellung, Verwendung und Deaktivierung eines kryptografischen Moduls. Legen Sie während der Konfiguration anfänglich **Entwurf** fest. Wenn Sie das -Modul verwenden, legen Sie dieses Feld auf **Veröffentlicht**fest. Die Standardvorlage wird automatisch auf Veröffentlicht gesetzt.

3. Wählen Sie **Absenden**.

⚠ Warnung:

Für Benutzer des Supports für veraltete Verschlüsselung:

Wenn Sie die Nicht-Enterprise-Version von Column Level Encryption verwenden, sind Sie auf fünf Module beschränkt. Wenn Sie dieses Limit überschritten haben, erhalten Sie die folgende Warnung:

Diese Einfügung überschreitet die Anzahl der veröffentlichten Module, die für die Verschlüsselung auf Spaltenebene zulässig sind, mit dem Abonnementprodukt. Für zusätzliche Module ist das Enterprise-Abonnement für Verschlüsselung auf Spaltenebene erforderlich. Wenden Sie sich an Ihr Account-Team.

Nach der erfolgreichen Übermittlung wird Ihr kryptografisches Modul in der Tabelle „Kryptografische Module“ aufgeführt. Das System stellt dem Namen den Bereich voran, um Konflikte mit anderen bereichsbezogenen Anwendungen zu vermeiden. Wenn Sie beispielsweise ein Modul mit dem Namen `my_crypto_module` im globalen Anwendungsbereich erstellt haben, wird der Name als `global.my_crypto_module` gespeichert.

Nächste Maßnahme

Erstellen Sie eine kryptografische Spezifikation

.

Erstellen Sie eine kryptografische Spezifikation

Nachdem Sie ein kryptografisches Modul erstellt haben, erstellen Sie eine kryptografische Spezifikation, um die Modulalgorithmen zu definieren.

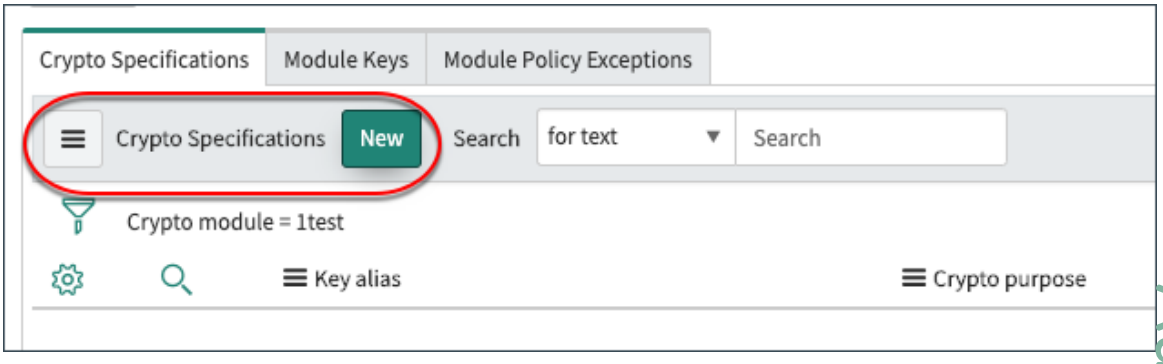
Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

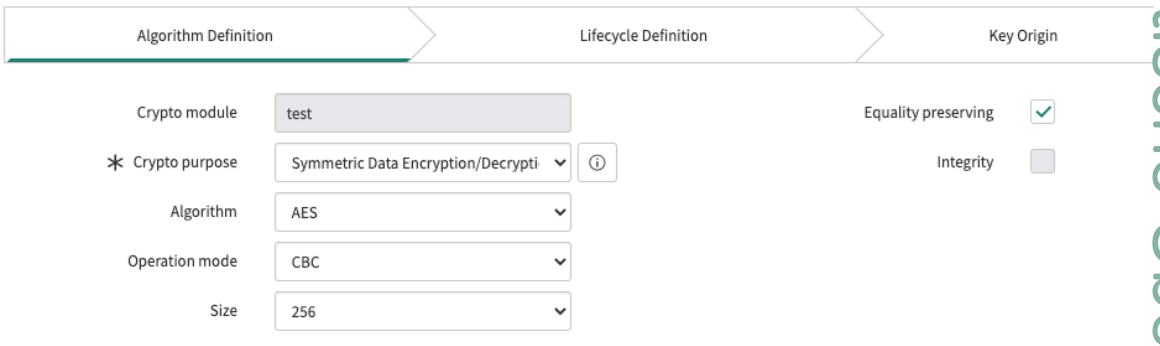
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**.
2. Wählen Sie das kryptografische Modul für die Definition aus, um die Konfigurationsoptionen zu öffnen.
3. Klicken Sie auf der Registerkarte **Krypto-Spezifikationen** auf **Neu**.



4. Füllen Sie das Formular „Algorithmusdefinition“ aus.
   Details siehe Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.



Der Bildschirm „Algorithmusdefinition“ wird geöffnet. Wählen Sie Optionen für die Schlüsselgenerierung aus. Wiederholen Sie diesen Schritt, um mehrere Schlüssel für das ausgewählte Krypto-Modul zu generieren.

Felder der Algorithmusdefinition

Feld	
Crypto-Modul	Schreibgeschützt. Der Name des ausgewählten kryptografischen Moduls wird angezeigt.
Kryptografischer Zweck	Wählen Sie den Zweck dieses Moduls aus. Sie können sie beispielsweise für Datenverschlüsselung, Signaturgenerierung oder Schlüsselumschließung verwenden. Die verfügbaren Algorithmen werden basierend auf dem ausgewählten Krypto-Zweck angepasst. Details siehe Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.
Algorithmus	Typ des Algorithmus, der zum Erfüllen des kryptografischen Zwecks verwendet wird. Der Algorithmus steuert auch den Schlüsselursprung. Wird automatisch basierend auf dem ausgewählten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	
	Krypto-Zweck angepasst. Kryptografischer Zweck, Algorithmen und Schlüsselinformationen für Details.
Betriebsmodus	Dieses Feld kann basierend auf dem ausgewählten Krypto-Zweck angezeigt werden.
Größe	Wählen Sie die Bitgröße aus.
Hash	Dieses Feld wird basierend auf dem ausgewählten Algorithmus verfügbar.
Gleichstellungserhaltung	Aktiviert die nicht deterministische Verschlüsselung. Diese Option wird angezeigt, wenn Sie **Symmetrische Datenverschlüsselung/-entschlüsselung** mit **AES** auswählen und sich im Modus **Cipher Block Chaining (CBC)** befindet. Wenn Sie diese Option auswählen, sind die codierten Daten jedes Mal identisch, wenn dieselben Daten erneut verschlüsselt werden. Die nicht deterministische Verschlüsselung unterstützt das Filtern einer Liste verschlüsselter Daten mit Gleichheitsvergleichsoperatoren nicht.
Integrität	GCM-Betriebsmodus stellt Integrität bereit.

5. Klicken Sie auf **Next (Weiter)**.
   Die Krypto-Spezifikation wird basierend auf den ausgewählten Algorithmen in der Tabelle „Schlüssellebenszyklus“ aufgelistet.

Nächste Maßnahme

Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Weitere Informationen zum Abschließen der Lebenszyklusdefinition für den Schlüssel finden Sie unter Konfigurieren Sie wichtige Lebenszyklusstatus.
- Klicken Sie auf **Weiter**, um einen kryptografischen Schlüssel zu erstellen. Informationen zur Schlüsselgenerierung finden Sie unter einer der folgenden Aufgaben:
  - Generieren Sie einen kryptografischen Schlüssel ServiceNow ..
  - Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
  - Importieren Sie das Schlüsselpaar zum Packen/Entpacken.

Konfigurieren Sie wichtige Lebenszyklusstatus

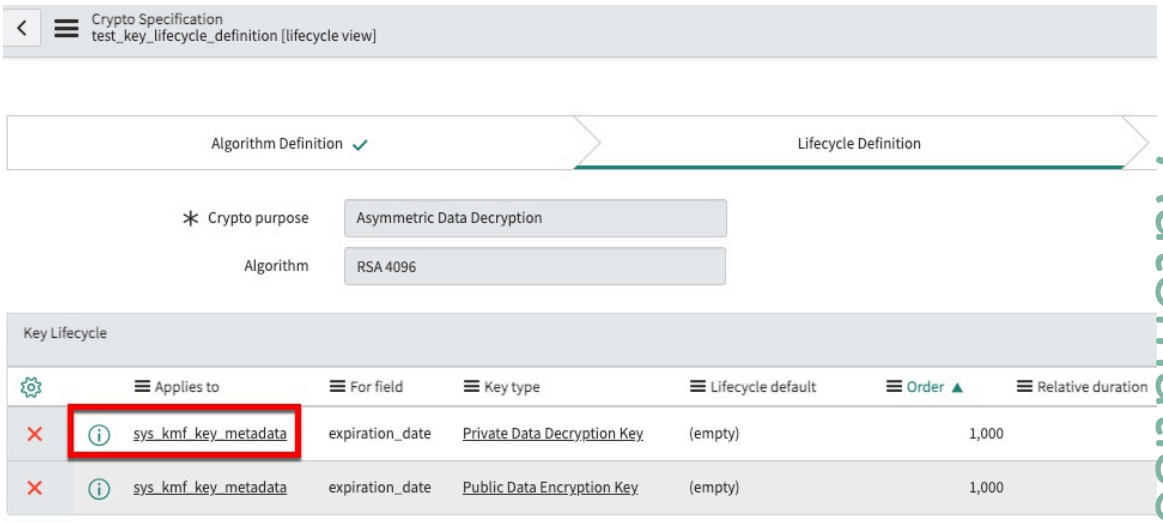
Nachdem Sie eine kryptografische Spezifikation erstellt haben, können Sie die Lebenszyklusaktionen für die Schlüssel in Ihrer Instanz konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_kmf.admin

Prozedur

1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**.
2. Wählen Sie das kryptografische Modul aus, um den Lebenszyklus eines Schlüssels zu konfigurieren.
3. Klicken Sie auf der Registerkarte Krypto-Spezifikationen auf einen Schlüsselalias.
   Das Formular „Algorithmusdefinition“ wird für den ausgewählten Schlüssel geöffnet.



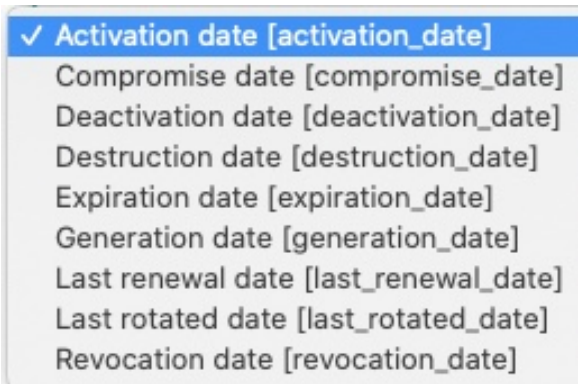
4. Klicken Sie auf **Next (Weiter)**.
   Die Feldlebenszyklus-Vorlage wird geladen. Standardwerte für Schlüssellebenszyklus werden basierend auf den ausgewählten Algorithmen für die definierte Krypto-Spezifikation erstellt.
5. Wählen Sie im Schritt „Lebenszyklusdefinition“ für die Krypto-Spezifikation **in** der Spalte Betrifft einen Schlüssellebenszyklus aus.

Schlüssellebenszyklus-Felder

Feld	Beschreibung
Betrifft	Ausgewählter Schlüssel, für den der Lebenszyklus gilt.
Für Feld	Wählen Sie die Art der Steuerung für den Schlüssel aus, für den der Lebenszyklus gilt. **Schlüssellebenszyklusverwaltung „Für Feld“-Werte** * For field ✓ Expiration date [expiration_date] Future activation date [future_activation_date] Future destruction date [future_destruction_date] Future renewal date [future_renewal_date] Future rotation date [future_rotation_date]
Typ	Wählen Sie aus, ob die Bewertung für den Schlüssellebenszyklus ein relativer Wert oder ein absoluter Wert ist:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Relativ**: Geben Sie einen Wert ein, der von anderen Dateneinträgen im System abhängt, z. B. Schlüsselgenerierung, Aktivierung und Deaktivierung. ○ **Absolut**: Geben Sie einen genauen Wert ein, z. B. ein Datum.
Lebenszyklusstandard	Schreibgeschützt. Zeigt einen Wert an, falls festgelegt.
Reihenfolge	Geben Sie die Sequenz ein, in der der Schlüssellebenszyklusstatus für die Krypto-Spezifikation verarbeitet werden soll.
Typ relative Dauer	Dauer des Lebenszyklus: **Jahre**, **Monate**oder **Tage**.
Relative Dauer	Anzahl der Jahre, Monate oder Tage, die der Schlüssel gültig ist.
Relativer Betrieb	**Vor**oder **Nach**.
Relativ zu	Feld, zu dem die Dauer relativ ist. Wird angezeigt, wenn eine relative Dauer oder ein Vorgang ausgewählt ist. 

Generieren Sie einen kryptografischen Schlüssel ServiceNow .

Befolgen Sie dieses Verfahren, um einen kryptografischen Schlüssel ServiceNow hochzuladen und zu konfigurieren, um vertrauliche Daten zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

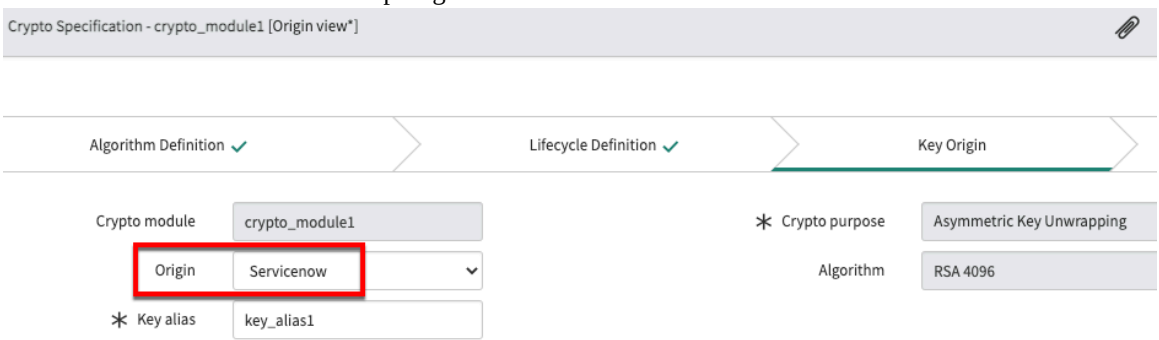
Kryptografische Manager haben die Möglichkeit, die von ServiceNow bereitgestellten Schlüssel oder ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auf dem Now Platform mit Verschlüsselung auf Spaltenebene Enterprisezu verwenden. Weitere Informationen zu CSK finden Sie unter Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.

Prozedur

1. Legen Sie die Feldverschlüsselungseinstellungen so fest, dass ServiceNow generierte Schlüssel verwendet werden.
   Details siehe Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen.
2. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**.
3. Wählen Sie das entsprechende Kryptografiemodul aus, um die Detailseite des Kryptografiemoduls zu öffnen.

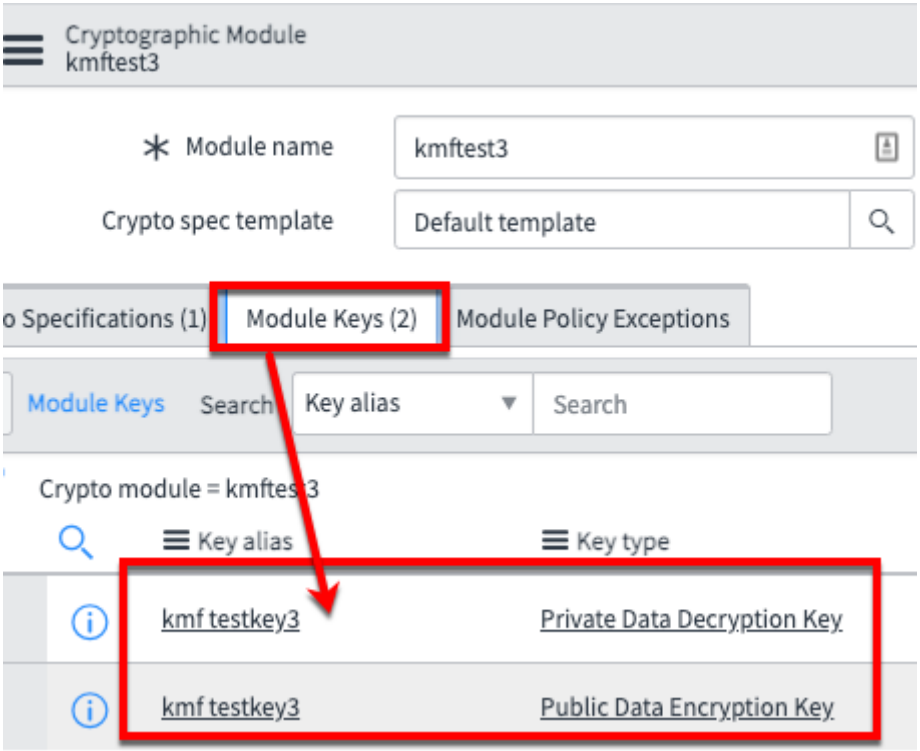
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf der Registerkarte Krypto-Spezifikationen auf die Zeile für den Eintrag „Schlüsselalias“. Wenn noch kein Schlüssel generiert wurde, ist das Feld „Schlüsselalias“ leer.
5. Klicken Sie auf **Weiter**, um zur Registerkarte Schlüsselursprung der Krypto-Spezifikationskomponenten zu navigieren.
   Die Registerkarte „Lebenszyklusdefinition“ wird zusammen mit der Tabelle „Schlüssellebenszyklus“ angezeigt und kann überprüft oder bearbeitet werden. Details siehe Konfigurieren Sie wichtige Lebenszyklusstatus.
6. Wählen Sie **ServiceNow** im Feld Ursprung



   aus.
   Dieses Feld variiert je nach den Feldverschlüsselungseinstellungen aus Schritt 1 und dem ausgewählten Algorithmus. Informationen zur Verwendung eines importierten Schlüssels finden Sie unter Importieren Sie das Schlüsselpaar zum Packen/Entpacken. Siehe Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel, wenn Sie Ihren eigenen Schlüssel verwenden.
7. Geben Sie einen Anzeigenamen für den Schlüsselalias ein.
8. Klicken Sie auf **Weiter**, um zur Registerkarte Schlüsselerstellung zu wechseln.
9. Klicken Sie auf **Schlüssel generieren**.
   Nachdem Sie den Schlüssel generiert haben, wird das Formular „Kryptografisches Modul“ neu geladen und die Krypto-Spezifikation angezeigt.
10. Klicken Sie auf die Registerkarte Modulschlüssel, um die **Schlüssel** anzuzeigen.
    Sichere Informationen für den Schlüssel werden auf der Registerkarte „Modulschlüssel“ zusammen mit der Anzahl der Schlüssel gespeichert, die für die Krypto-Spezifikation vorhanden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Wählen Sie einen Schlüssel aus, um Schlüsselverwaltungsaktionen auszuführen.
Details siehe Schlüsselverwaltungsaktionen.

Erstellen Sie eine Modulzugriffsrichtlinie

Erstellen Sie Modulzugriffsrichtlinien, um einzuschränken, ob Daten verschlüsselt oder entschlüsselt werden können.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

Column Level Encryption (CLE) unterstützt rollenbasierte Modulzugriffsrichtlinien, und zusätzliche Konfigurationsoptionen werden mit der Funktionalität (CLE_Ent) verfügbar.

- Konfigurieren Sie den spezifischen kryptografischen Vorgang in Modulzugriffsrichtlinien für kryptografische Module, die symmetrische Vorgänge unterstützen. Beispielsweise kann einem Benutzer erlaubt werden, Daten zu verschlüsseln, aber nicht zu entschlüsseln.
- Legen Sie einen Standardwert für die Modulzugriffsrichtlinie pro oder kryptografischem Modul fest.
- Ordnen Sie Skriptversionen zu, in denen Änderungen am Skript nachverfolgt werden, und machen Sie die Skriptrichtlinie ungültig, was eine bessere Sicherheit für Modulzugriffsrichtlinien vom Typ Skript bietet.

CLE_Ent -Funktionalität ist mit einem kostenpflichtigen Abonnement verfügbar. Informationen zu unterstützten Funktionen und Optionen, die für jedes Angebot verfügbar sind, finden Sie unter. Weitere Informationen finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

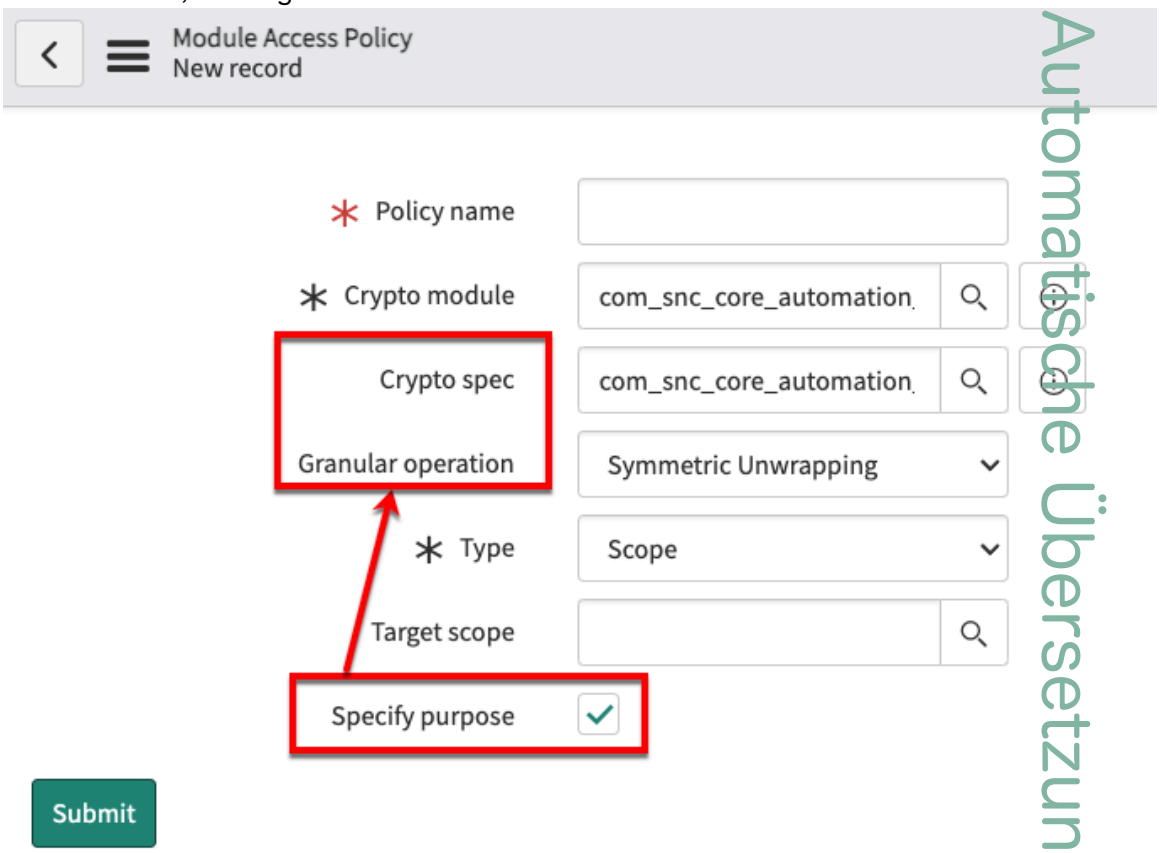
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Standardverhalten der Modulzugriffsrichtlinien (Module Access Policies, MAPs) ist „Ablehnen“, um nicht autorisierten Zugriff zu verhindern, sofern dies nicht ausdrücklich in MAP-Datensätzen deklariert ist.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**.
   Wenn Sie kein kryptografisches Modul erstellen, das für die symmetrische Datenverschlüsselung/-entschlüsselung konfiguriert ist, wird eine automatisch generierte Modulzugriffsrichtlinie erstellt und in der Tabelle aufgelistet.
2. Klicken Sie auf **Neu**.
   - Wählen Sie **Zweck angeben** aus, um eine **Krypto-Spezifikation** auszuwählen, und legen Sie den **Granular-**



Vorgangfest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit kryptografischen Spezifikationen für symmetrische Datenverschlüsselung/-entschlüsselung und symmetrisches Packen/Entpacken ist das Feld **Granularer Vorgang** verfügbar, wenn Sie das Kontrollkästchen **Zweck** angeben aktivieren.

3. Füllen Sie das Formular aus.

Felder „Modulzugriffsrichtlinien“.

Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein.
Crypto-Modul	Klicken Sie auf das Suchsymbol ( ), um ein Modul auszuwählen.
Krypto-Spezifikation	Wählen oder erstellen Sie beim Generieren der Modulzugriffsrichtlinie eine neue kryptografische Spezifikation. Dieses Feld wird verfügbar, wenn das Kontrollkästchen **Zweck** angeben aktiviert wird.
Granularer Vorgang	Wählen Sie den kryptografischen Zweck für die kryptografische Spezifikation aus. Die verfügbaren Werte hängen vom Typ der ausgewählten kryptografischen Spezifikation ab. Weitere Informationen zu kryptografischen Zwecken finden Sie unter Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	○ **Bereich**: Steuert den Zugriff nach Anwendungsbereich. ○ **Systemanwender**: Ermöglicht Systemanwendern den Zugriff auf Krypto-Module. ○ **Skript**: Steuern Sie den Zugriff per Skript. Weitere Informationen finden Sie unter Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten. ○ **Rolle**: Steuert den Zugriff nach Benutzerrolle. ○ **Ressourcenaustausch**: Steuern Sie den Zugriff mit Ressourcenaustausch. Weitere Informationen finden Sie unter Key Management Framework Ressourcenaustausch. **Hinweis:** Nur der Rollentyp wird mit Verschlüsselung auf Spaltenebene unterstützt. Alle anderen Typen sind mit Verschlüsselung auf Spaltenebene Enterpriseverfügbar.
Zielbereich	Feld ist als Bezeichner für den **Umfangstyp** sichtbar. Bezieht sich auf die Funktionalität für die Richtlinie. Wählen Sie die Anwendungen aus dem Suchmenü aus. **Hinweis:** Zielumfang wird nicht unterstützt und kann nur mit festgelegt werden Verschlüsselung auf Spaltenebene Enterprise
Zielrolle	Das Feld ist als Bezeichner für den **Rollentyp** sichtbar. Rolle, für die diese Richtlinie gilt.
Skripttabelle Zielskript	Diese Felder werden angezeigt, wenn Sie Skript als Typ auswählen. Feld ist als Bezeichner für den **Skripttyp** sichtbar. Wählen Sie eine Tabelle aus, für die diese Richtlinie gilt. Dokument, für das diese Richtlinie gilt. Wählen Sie den **Tabellennamen** und dann das zugehörige Dokument für die Richtlinie aus. Wenn ein Skript zum ersten Mal ein kryptografisches Modul aufruft, wird der Zugriff auf das Modul verweigert, und der Entwickler erhält einen Fehler. Dies gibt dem Modulbesitzer die Möglichkeit, den Zugriff auf das Modul zu gewähren oder zu verweigern.
Ressourcenaustausch: ○ Krypto-Spezifikation ○ Freigabetyp ○ Zielinstanz-Host	Diese Optionen werden angezeigt, wenn Sie Ressourcenaustausch als Typ auswählen. Ressourcenaustausch wird sowohl von KMF als auch von Verschlüsselung auf Spaltenebene Enterprise unterstützt, wenn das übergeordnete Modul **column_level_encryption**ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie die Krypto-Spezifikation, Einmalig oder Wiederkehrend, und die URL der Zielinstanz aus. Weitere Informationen finden Sie unter Key Management Framework Ressourcenaustausch.
Identitätswechsel	In rollenbasierten Modulzugriffsrichtlinien können Benutzer über eine Identitätswechselsitzung auf verschlüsselte Daten zugreifen. Wenn Benutzer, z. B. Administratoren, die Identität anderer Benutzer annehmen, werden solche für Identitätswechsel aktivierten Modulzugriffsrichtlinien angewendet.
Zweck angeben	Auswählen, um das Feld Krypto-Spezifikation als verfügbares Feld für die Richtlinie umzuschalten.
Aktiv	Wählen Sie diese Option aus, um die Richtlinie zu aktivieren.
Ergebnis	Wählen Sie eine der folgenden Optionen aus: ○ **StrictReject** lehnt den Zugriff unter allen Umständen ab. ○ **Ablehnen** lehnt Benutzer mit der **Zielrolle** oder dem **Zielbereich** vom Zugriff auf dieses kryptografische Modul ab, es sei denn, eine andere Richtlinie gewährt ihnen Zugriff. ○ **Nachverfolgen**, um Zugriff zu gewähren und die Verwendung des Moduls zu überwachen.

4. Wählen Sie **Absenden**.

⚠ Warnung:

Für Benutzer des Supports für veraltete Verschlüsselung:

Wenn Sie die Nicht-Enterprise-Version von Column Level Encryption verwenden, sind Sie auf fünf Module beschränkt. Wenn Sie dieses Limit überschritten haben, erhalten Sie die folgende Warnung:

Diese Einfügung überschreitet die Anzahl der veröffentlichten Module, die für die Verschlüsselung auf Spaltenebene zulässig sind, mit dem Abonnementprodukt. Für zusätzliche Module ist das Enterprise-Abonnement für Verschlüsselung auf Spaltenebene erforderlich. Wenden Sie sich an Ihr Account-Team.

5. Wählen Sie den Richtliniennamen aus, der dem kryptografischen Modul zugeordnet ist, das Sie untersuchen möchten.
Verwenden der Modulzugriffsrichtlinie vom Typ „Skript“:

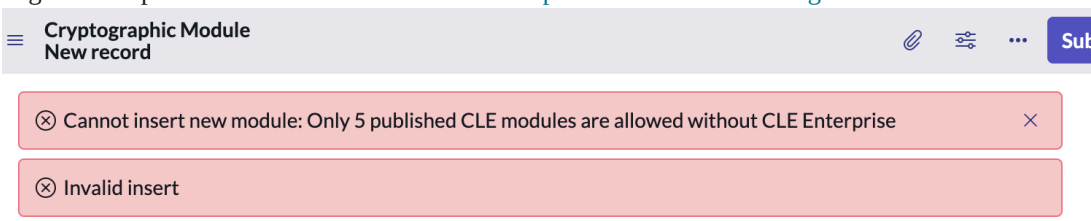
Eine Modulzugriffsrichtlinie wird basierend auf der Standardzugriffseinstellung automatisch generiert, wenn das Skript ausgeführt wird. Dem Modulnamen wird „AutoGen-“ vorangestellt. Beispielsweise wird das Modul „Module-TestPolicy“ als „AutoGen-Module-TestPolicy“ in der Spalte „Richtlinienname“ aufgeführt.

Im Formular „Krypto-Aufruferrichtlinie“ wird die von Ihnen ausgewählte Anruferrichtlinie aufgelistet. Das Feld Zielbereich gibt den Bereich des Skripts an, das versucht, das Modul

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

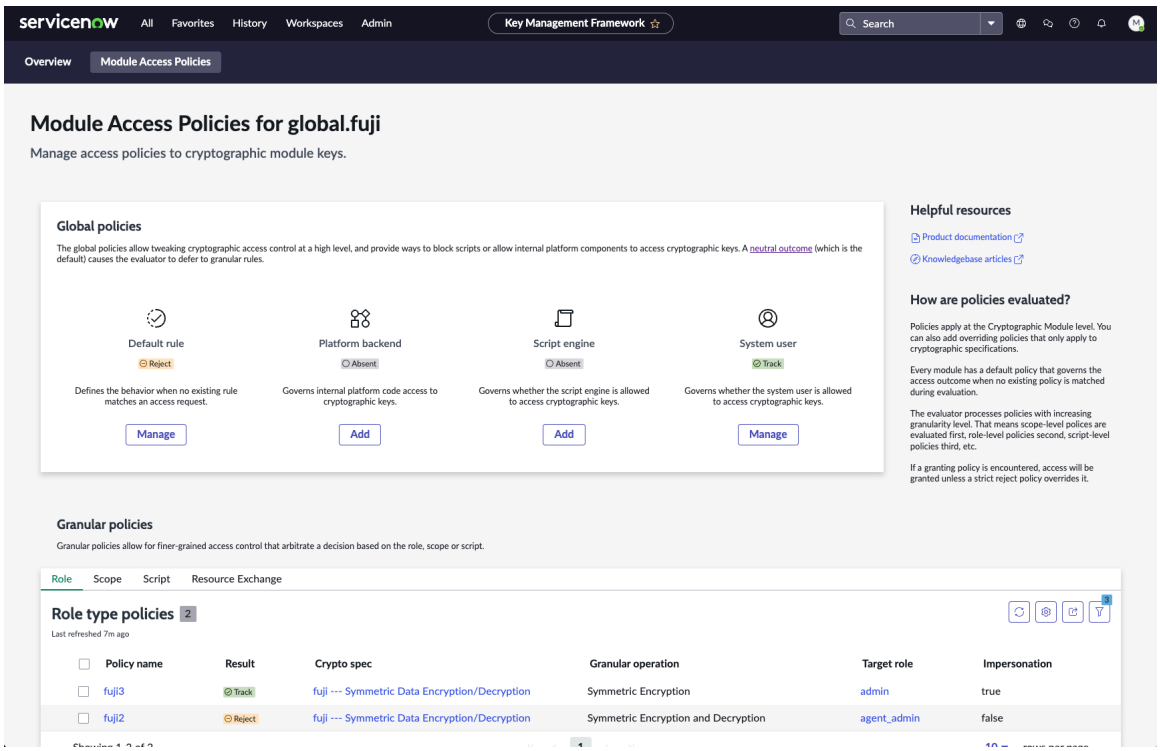
zu verwenden. Weitere Informationen finden Sie unter Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten.

Hinweis:
Bei Verschlüsselung auf Spaltenebene sind maximal fünf Modulzugriffsrichtlinien zulässig. Weitere Informationen zu Konfigurationsoptionen finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.



Visualisierung der Modulzugriffsrichtlinie

Verwenden Sie die Visualisierung der Modulzugriffsrichtlinie, um alle relevanten kryptografischen Modulinformationen auf einer einzelnen UI-Seite anzuzeigen.



Key Management Framework-Administratoren und Kryptografiemanager können die UI-Seite der Modulzugriffsrichtlinie verwenden, um alle Zugriffskontrollmechanismen anzuzeigen, die sich auf ein einzelnes Kryptografiemodul beziehen. Verwenden Sie die auf dieser UI-Seite erfassten Informationen, um schnell zu bestimmen, wer Zugriff auf verschlüsselte Informationen in Ihrer Instanz hat.

Benutzer mit den Rollen *sn_kmf.admin* oder *sn_kmf.cryptographic_manager* können auf die UI-Seite der Modulzugriffsrichtlinienvisualisierung zugreifen, indem sie zu navigieren **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**.

Ergebnisbezeichnungen

Modulzugriffsrichtlinien enthalten ein **Ergebnisfeld**, das bestimmt, ob Zugriff auf das ausgewählte kryptografische Modul gewährt werden soll. Die UI-Seite zeigt eine Bezeichnung für Elemente auf der UI-Seite basierend auf dem Wert dieses Felds an.

Automatische Übersetzung

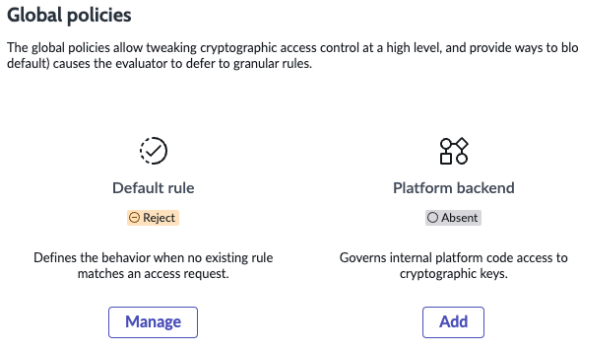
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Bezeichnung	Ergebnisfeldwert	Definition
Track	`Track` oder `Allow`	Zugriff wird allen Benutzern gewährt, einschließlich Skripts.
Reject	`Reject`	Der Zugriff wird verweigert, es sei denn, eine Nachverfolgungsmodul-Zugriffsrichtlinie wird gefunden.
StrictReject	`StrictReject`	Der Zugriff wird verweigert.
Absent	`N/A`	Die Modulzugriffsrichtlinie ist in der Instanz nicht vorhanden. Der Zugriff wird allen verweigert.

Globale Richtlinien

Verwenden Sie den Abschnitt **Globale Richtlinien**, um die Modulzugriffsrichtlinien zu überprüfen, die den Zugriff auf Plattformebene steuern.

Wählen Sie die Schaltfläche **Verwalten** unter einer der Richtlinien aus, um zu diesem Richtliniendatensatz zu navigieren. Wenn die Richtlinie nicht vorhanden ist, wird unter diesem Eintrag die Schaltfläche **Hinzufügen** angezeigt. Klicken Sie auf die Schaltfläche **Hinzufügen**, um zu einem neuen Richtliniendatensatz zu navigieren, in dem Sie die Richtlinie definieren können.

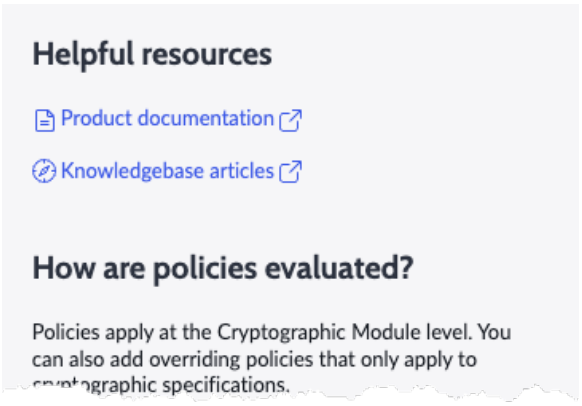


Richtlinie	Definition
Standardregel	Die Standardregelrichtlinie definiert das Verhalten, wenn keine vorhandene Regel mit einer Zugriffsanforderung übereinstimmt.
Plattform-Back-End	Die Back-End-Richtlinie der Plattform regelt den internen Plattformcodezugriff auf kryptografische Schlüssel.
Skriptmodul	Die Skript-Engine-Richtlinie regelt, ob die Skript-Engine auf kryptografische Schlüssel zugreifen darf.
Systemanwender	Die Systembenutzerrichtlinie regelt, ob der Systembenutzer auf kryptografische Schlüssel zugreifen darf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hilfreiche Ressourcen

Im Abschnitt „ **Hilfreiche Ressourcen** “ finden Sie Links zu Produktdokumentation, relevanten Wissensartikeln und eine kurze Beschreibung, wie Modulzugriffsrichtlinien auf der Plattform ausgewertet werden. Weitere Informationen zur Auswertung von Modulzugriffsrichtlinien finden Sie unter Debugger für Modulzugriffsrichtlinien.

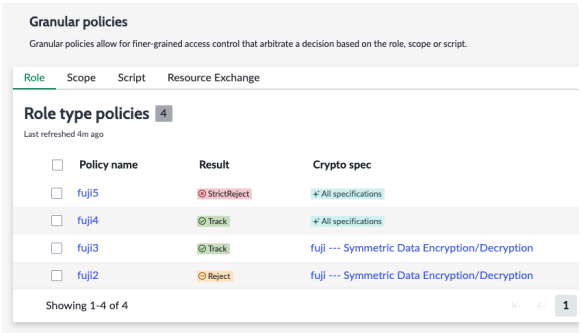


Granulare Richtlinien

Verwenden Sie den Abschnitt „ **Granulare Richtlinien** “, um Listen von Modulzugriffsrichtlinien anzuzeigen, getrennt nach Richtlinientyp. Verwenden Sie die Registerkarten über der Liste, um eine Richtlinienkategorie auszuwählen, die angezeigt werden soll.

- Rolle
- Umfang
- Umfang und Domäne (wenn Domänentrennung aktiv ist)
- Skript
- Ressourcenaustausch (wenn das kryptografische Modul ein Passwort2- oder Verschlüsselungs-Submodul auf Spaltenebene ist)
- Identität (wenn Geheimnisverwaltung Enterprise aktiv ist)

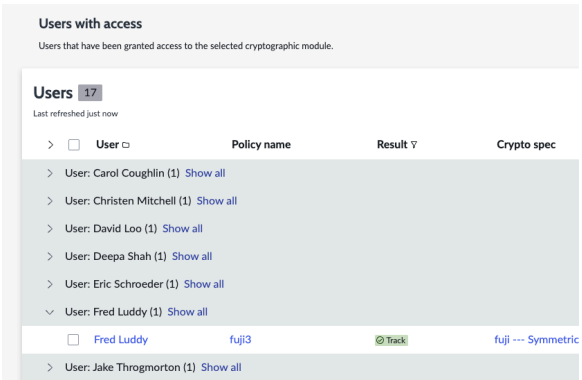
Standardmäßig werden in der Liste nur aktive Richtlinien angezeigt. Verwenden Sie das Filtersymbol, um den Standardfilter für die Liste zu ändern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer mit Zugriff

Verwenden Sie den Abschnitt **Benutzer mit Zugriff**, um eine Liste aller Benutzer anzuzeigen, die Zugriff auf das ausgewählte kryptografische Modul haben. Die Liste ist nach Benutzern gruppiert, da einzelne Benutzer mehrere Rollen übernehmen können, die Zugriff auf ein kryptografisches Modul gewähren.

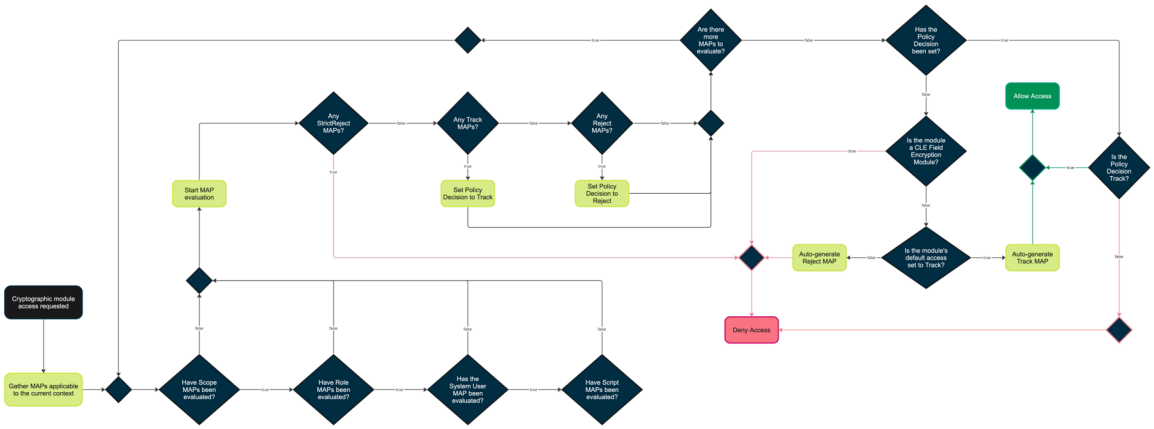


Debugger für Modulzugriffsrichtlinien

Verwenden Sie den Debugger für Modulzugriffsrichtlinien, um Protokollierungsinformationen zu überprüfen und nachzuvollziehen, warum Ihren Benutzern der Zugriff auf einen Verschlüsselungskontext gewährt wird.

Modulzugriffsrichtlinien (MAPs) definieren Steuerungen auf Instanzebene für den Zugriff auf kryptografische Module. Aufrufer (z. B. ein Benutzer oder ein Skript) benötigen expliziten Zugriff, um ein kryptografisches Modul für die Verschlüsselung und Entschlüsselung zu verwenden. Es ist nicht immer klar, welche MAPs ausgewertet werden, wenn Aufrufer versuchen, auf ein kryptografisches Modul zuzugreifen. Verwenden Sie den Debugger, um zu sehen, welche Richtlinien ausgewertet werden, wenn ein Aufrufer versucht, auf ein kryptografisches Modul zuzugreifen, und um zu erfahren, warum der Zugriff gewährt wird oder nicht.

Dieses Flussdiagramm zeigt, wie Ihre Instanz Anforderungen für den Zugriff auf ein kryptografisches Modul auswertet.



Steuern Sie den Zugriff auf die Debug-Protokolle

Der Zugriff auf die Debug-Protokolle des Modulzugriffs wird durch die Rolle bestimmt. Benutzer mit den Rollen *sn_kmf.admin* und *sn_kmf.cryptographic_manager* haben immer Zugriff auf den Debugger. Gewähren Sie Zugriff auf andere Rollen mithilfe der Systemeigenschaft *glide.kmf.module_access_policies.debugger.authorized.roles*. Der Wert dieser Eigenschaft ist eine durch Kommas getrennte Liste von Rollen, die auf die Debug-Protokolle zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren oder deaktivieren Sie den Debugger

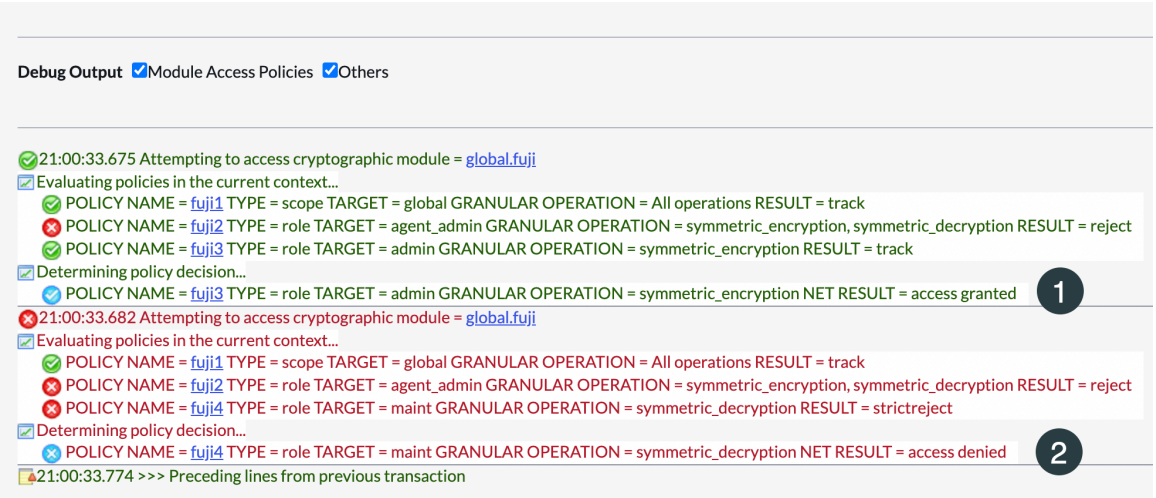
Um Debug-Protokollierungsnachrichten für Modulzugriffsrichtlinien zu aktivieren, navigieren Sie zu **Alle** > **Diagnosen** > **Sitzung debuggen** > **Modulzugriffsrichtlinien debuggen** > **.**

Wenn Sie mit dem Debuggen fertig sind, können Sie die Protokollierung von Nachrichten deaktivieren, indem Sie zu navigieren **Alle** > **Diagnosen** > **Sitzung debuggen** > **Alle deaktivieren** > **.**

Greifen Sie auf die Protokolle zu

Navigieren Sie nach dem Aktivieren des Debugging zu einer Seite, die eine MAP-Auswertung auslöst, um die MAP-Debug-Protokolle anzuzeigen. Debug-Meldungen werden unten auf der Seite angezeigt.

Tipp:
Sie können Identitätswechsel verwenden, um Zugriffsprobleme für andere Benutzer zu beheben. Weitere Informationen zum Identitätswechsel finden Sie unter Impersonating users . Um die Debug-Protokolle aus der Perspektive eines anderen Benutzers anzuzeigen, stellen Sie sicher, dass für Ihre **Modulzugriffsrichtlinien** vom Typ `role` das Feld Identitätswechsel auf **true**festgelegt ist.



In diesem Beispiel ruft ein Aufrufer zwei Zugriffsanforderungen für das kryptografische Modul `global.fuji` auf. Eine symmetrische Verschlüsselung, die gewährt wird, und eine symmetrische Entschlüsselung, die verweigert wurde.

Protokolleinträge verstehen

Debugging-Informationen werden in diesem Format strukturiert.

1. In dieser ersten Zeile wird das kryptografische Modul angezeigt, das die Zugriffsanforderung erhält.
2. Die Zeilen zwischen der ersten und letzten Zeile zeigen die ausgewerteten MAPs in der Reihenfolge an, in der sie ausgewertet wurden, und enthalten Name, Typ, Ziel, granularen Vorgang und Ergebnis.
3. In der letzten Zeile werden die Richtlinienentscheidung (falls zutreffend) und das Nettozugriffsergebnis für den Anrufer angezeigt (ob dem Anrufer Zugriff gewährt wird).

Jede Zeile beginnt mit einem Symbol, das den Nachrichtentyp angibt.

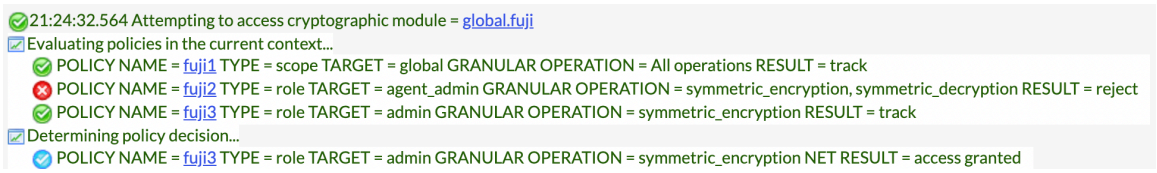
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachrichtensymbole

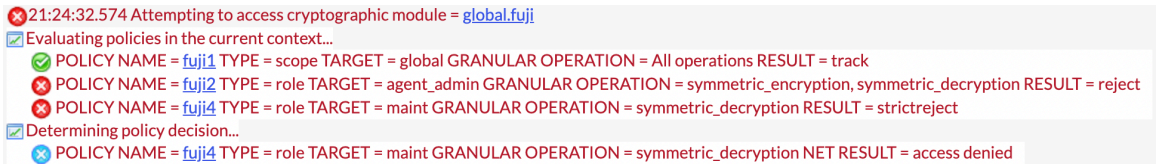
Symbol	Nachrichtentyp
	Informationsnachricht
	Die Modulzugriffsrichtlinie gewährt Zugriff
	Die Modulzugriffsrichtlinie verweigert den Zugriff
	Dem Aufrufer wird Zugriff gewährt
	Dem Anrufer wird der Zugriff verweigert
	Keine Modulzugriffsrichtlinie zum Auswerten vorhanden

Beispiele für Debug-Protokolle

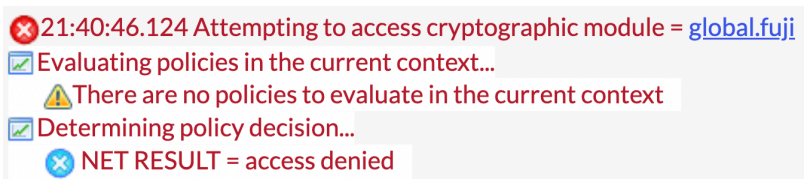
Nachricht „Zugriff gewährt“.



Nachricht „Zugriff verweigert“.



Zugriff verweigert (keine Modulzugriffsrichtlinien zum Auswerten



Zugriff verweigert (unzureichende Berechtigungen)

Erstellen Sie eine Lebenszyklusrichtlinie für kryptografische Module

Erstellen Sie eine Lebenszyklusrichtlinie für kryptografische Module, um Grenzwerte für kryptografische Module festzulegen, z. B. wie lange der Schlüssel gültig ist. Erstellen Sie Richtlinien, um kryptografische Module zu schützen, indem Sie deren Gefährdung begrenzen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Eine Lebenszyklusrichtlinie für kryptografische Module ist eine Richtlinie auf Instanzebene. Je angreifbarer ein kryptografischer Schlüssel ist, desto wahrscheinlicher ist es, dass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

er gefährdet ist. Schützen Sie Schlüssel, indem Sie begrenzen, wie lange die Schlüssel verwendet werden können und wer sie verwenden kann.

Die folgenden Funktionen steuern kryptografische Module:

- Instanzrichtlinien legen Grenzen für die Instanz fest. Wenn Sie beispielsweise in einer Instanzrichtlinie angeben, dass das Ablaufdatum nie mehr als zwei Jahre nach dem Aktivierungsdatum liegen darf, können Sie die Lebenszyklusregeln nicht verwenden, um ein Ablaufdatum fünf Jahre nach dem Aktivierungsdatum festzulegen.

- Mit Instanzlebenszyklusvorlagen können Sie verschiedene Richtlinien für verschiedene Schlüssel festlegen. Vorlagen bieten Standardlebenszyklusregeln für kryptografische Module, sodass sie nicht für jedes Modul neu erstellt werden müssen. Sie können beispielsweise andere Ablaufdaten für symmetrische Datenverschlüsselungsschlüssel festlegen als für Schlüssel zum Umschließen öffentlicher Schlüssel.

- Lebenszyklusregeln wirken sich direkt auf die Schlüssel aus. Wenn Sie beispielsweise in den Lebenszyklusregeln angeben, dass das Ablaufdatum zwei Jahre nach dem Aktivierungsdatum liegen soll, laufen die Schlüssel zwei Jahre nach dem Aktivierungsdatum ab.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Lebenszyklusrichtlinien** > **Instanzrichtlinien**.
2. Auswahlvorgang **Neu**.
3. Füllen Sie das Formular aus.

   Felder Kryptografische Lebenszyklusrichtlinien

Nächste Maßnahme

Wenn Sie dieser Lebenszyklusrichtlinie Ausnahmen auf Modulebene hinzufügen möchten, finden Sie weitere Informationen unter Erstellen Sie Ausnahmen für Modullebenszyklusrichtlinien.

Erstellen Sie Ausnahmen für Modullebenszyklusrichtlinien

Erstellen Sie eine Modulrichtlinienausnahme, um die Lebenszyklusrichtlinie eines Schlüssels auf Modulebene für eine Instanz zu ändern. Die Ausnahmen gelten nur für dieses Modul und nicht für die gesamte Instanz. Beispiel: Wenn der Administrator symmetrische Schlüssel so konfiguriert hat, dass sie auf Instanzebene auf ein Jahr beschränkt sind, kann auf Modulebene eine Ausnahme von zwei Jahren festgelegt werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager und sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module Alle**.
2. Wählen Sie das kryptografische Modul aus, das die Richtlinienausnahmen verwendet.
3. Wählen Sie in der Tabelle „Kryptografisches Modul“ die Option aus **Modulrichtlinienausnahmen** Registerkarte.
4. Klicken **Neu**.
5. Füllen Sie das Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder „Modulrichtlinienausnahmen“

Feld	Beschreibung
Krypto-Modul	Schreibgeschützt, Name des ausgewählten Moduls.
Betrifft	Der angegebene Schlüssel wird automatisch ausgefüllt.
Schlüsseltyp	Wählen Sie den Schlüsseltyp aus, da sich die Ausnahmerichtlinien auf einen bestimmten Schlüssel beziehen. Pro Krypto-Modul können mehrere Ausnahmerichtlinien erstellt werden.
Richtlinienbedingung	Wählen Sie die Qualifizierungsbedingungen aus der Dropdown-Liste aus, und schließen Sie die zusätzlichen Einschränkungskriterien ab.
Neue Kriterien	Wählen Sie nach Bedarf zusätzliche Richtlinienbedingungen aus.
Ergebnis	Wählen Sie **Ablehnen**, um die Verwendung des Schlüssels abzulehnen, oder **Nachverfolgen**, um die Verwendung zuzulassen, wenn die Kriterien erfüllt sind.

6. Klicken **Absenden** an die Tabelle „Kryptografisches Modul“ zurückgegeben werden soll.

Schlüsselverwaltungsaktionen

Eine der Hauptfunktionen von KMF ist die Möglichkeit zur Verwaltung von Schlüsseln, z. B. Widerrufen oder Rotieren von Schlüsseln. KMF sichert vertrauliche Daten ordnungsgemäß mit den neuesten Verschlüsselungsmaterialien und Lebenszyklusvorgängen.

Die folgende Tabelle enthält eine Zusammenfassung der wichtigsten Lebenszyklusvorgänge und Verwaltungsaktionen. Der Zweck des kryptografischen Moduls wird mit der Konfiguration des kryptografischen Moduls auf die Daten angewendet und hat keine Auswirkungen auf die Daten.

Schlüsselverwaltungsaktion	Beschreibung
Schlüssel generieren	Generiert einen neuen Schlüssel für das angegebene kryptografische Modul. Ein zuerst generierter Schlüssel wird auf „ `active`“ gesetzt.
Schlüssel rotieren	Deaktiviert den aktuellen Schlüssel und generiert einen neuen. Der neue Modulschlüssel wird auf aktuell (aktiv) festgelegt.
Schlüssel widerrufen	Markiert den aktuellen Schlüssel und den Lebenszyklusstatus als widerrufen. Das kryptografische Modul generiert automatisch einen neuen Schlüssel für neue Daten und legt den Schlüsselstatus auf „Aktiv“ fest. Widerrufen bedeutet, dass der Schlüssel nicht mehr für die Verschlüsselung verwendet wird. Sie kann jedoch weiterhin zur Entschlüsselung verwendet werden. Sie können einen Schlüssel nicht vernichten.
Schlüssel anhalten	Markiert den aktuellen Schlüssel als angehalten. Setzen Sie den ausgesetzten Schlüssel manuell fort, oder widerrufen Sie den ausgesetzten Schlüssel, um einen neuen Modulschlüssel zu generieren, bevor Sie das kryptografische Modul erneut verwenden.
Schlüssel fortsetzen	Markiert einen ausgesetzten Schlüssel als aktiven Schlüssel.
Schlüssel verlängern	Verlängert die Lebensdauer des aktuellen Schlüssels. Die **Schaltfläche Verlängern** wird unter den folgenden Umständen verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselverwaltungsaktion	Beschreibung
	• Ihnen ist die Kryptografiemanager-Rolle zugewiesen. • Der Lebenszyklusstatus wird entweder als **Aktiv** oder **Verlängert**markiert. • In der Modullebenszyklusdefinition wird ein Ablaufdatum festgelegt.

Schlüssel anzeigen und verwalten

Überprüfen Sie den Status eines Schlüssels, um weitere wichtige Aktionen zu bestimmen, z. B. wann ein aktueller Schlüssel erneuert, rotiert, angehalten, deaktiviert oder vernichtet werden soll.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**.
2. Wählen Sie ein kryptografisches Modul aus.

   Das kryptografische Modul<module-name> Das Formular „“ wird angezeigt.
3. Wählen Sie auf der Registerkarte Modulschlüssel den Schlüsselalias aus, um den Schlüsselstatus im Lebenszyklus zu überprüfen<key name> Formular.
4. Überprüfen Sie das Formular, da alle Felder schreibgeschützt sind.

Schlüsselfelder des kryptografischen Lebenszyklus

Feld	Beschreibung
Generierungsdatum	Zeigt das Datum an, an dem der Schlüssel generiert wurde.
Aktivierungsdatum	Zeigt das Datum an, an dem der Schlüssel aktiviert wurde.
Letztes Verlängerungsdatum	Zeigt das Datum an, an dem der Schlüssel zuletzt verlängert wurde.
Letztes Rotationsdatum	Zeigt das Datum an, an dem der Schlüssel zuletzt rotiert wurde.
Deaktivierungsdatum	Zeigt das Datum an, an dem der Schlüssel deaktiviert wurde.
Zerstörungsdatum	Zeigt das Datum an, an dem der Schlüssel vernichtet wurde.
Status des Schlüssellebenszyklus	Zeigt den Lebenszyklusstatus des Schlüssels an.
Künftiges Aktivierungsdatum	Zeigt das zukünftige Schlüsselaktivierungsdatum an.
Künftiges Verlängerungsdatum	Zeigt das zukünftige Schlüsselverlängerungsdatum an.
Künftiges Rotationsdatum	Zeigt das zukünftige Datum für die Schlüsselrotation an.
Künftiges Zerstörungsdatum	Zeigt das zukünftige Datum an, an dem der Schlüssel vernichtet wird.
Ablaufdatum	Zeigt das Datum an, an dem der Schlüssel abläuft.

5. Um eine Aktion für die Taste auszuführen, wählen Sie eine der folgenden Optionen aus, die sofort wirksam wird:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Schlüssel widerrufen**: Wählen Sie diese Option aus, um den Schlüssel zu deaktivieren und einen neuen Schlüssel zu generieren. Geben Sie den Grund ein, warum Sie den Schlüssel widerrufen.
- **Schlüssel rotieren**: Wählen Sie diese Option aus, um den aktuellen Schlüssel zu deaktivieren und stattdessen einen neuen Schlüssel zu generieren. Der neue Schlüssel wird in der Modulschlüsseltabelle aufgelistet, und die Schlüsselversionsnummer wird um 1 erhöht. Weitere Informationen finden Sie unter.
- **Schlüssel aussetzen**: Wählen Sie diese Option aus, um den aktuellen Schlüssel zu deaktivieren.
- **Schlüssel fortsetzen**: Wählen Sie diese Option aus, um einen ausgesetzten Schlüssel als aktiven Schlüssel zu markieren. Diese Option ist nur verfügbar, nachdem der aktive Schlüssel angehalten wurde.

Schlüssel rotieren

Um die Sicherheit zu erhöhen, können Sie Ihre kryptografischen Schlüssel nach einem vordefinierten Zeitplan rotieren. Bei der Schlüsselrotation wird ein Verschlüsselungsschlüssel gelöscht und der alte Schlüssel durch Generieren eines neuen kryptografischen Schlüssels ersetzt.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

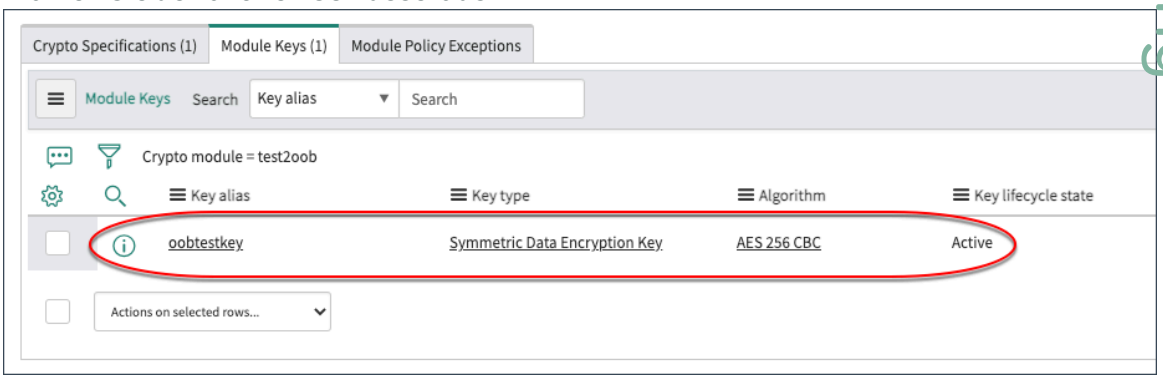
Warum und wann dieser Vorgang ausgeführt wird

Verschlüsselungsmodule unterstützen im Gegensatz zu Verschlüsselungskontexten eine erneute Schlüsselung von Datensätzen für die erneute Verschlüsselung mit einem neuen Schlüssel. Im Folgenden wird gezeigt, wie ein Schlüsselrotationsvorgang für ein kryptografisches Modul manuell ausgeführt wird.

Prozedur

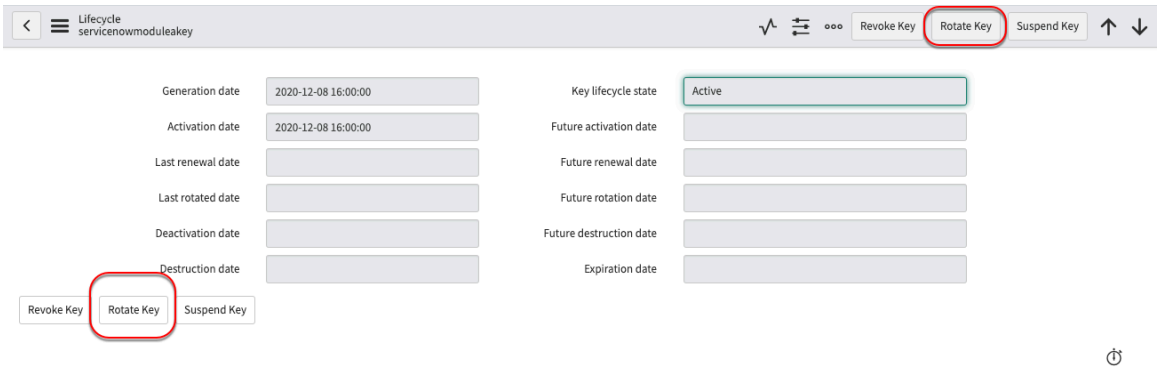
1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**.
2. Wählen Sie das kryptografische Modul für die Schlüsselrotation aus.
3. **Wählen** Sie auf der Registerkarte „Modulschlüssel“ den Schlüssel Aktiv aus.

Wählen Sie den aktiven Schlüssel aus

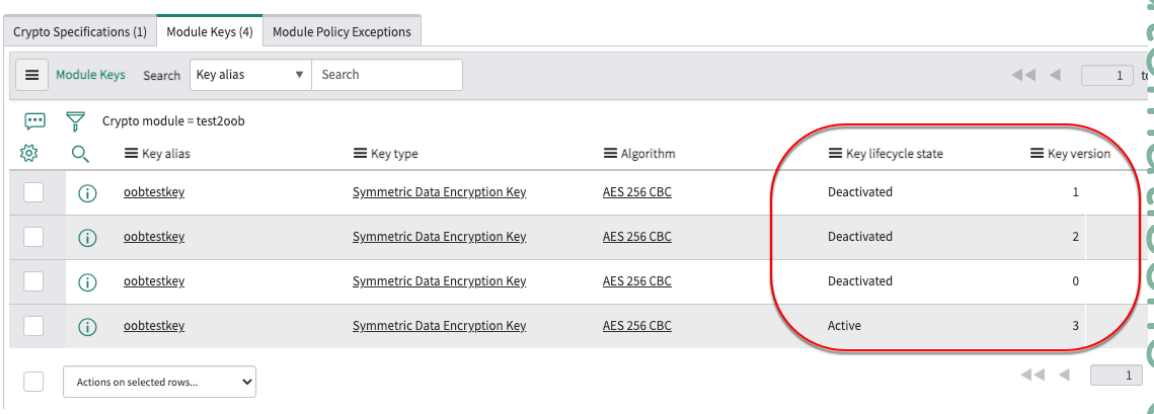


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie **Schlüssel rotieren aus**.
   Der Lebenszyklusstatus des Schlüssels ändert sich in „Deaktiviert“. Die Felder **Datum der letzten Rotation**, **Deaktivierungsdatum**und **Schlüsselversion** werden aktualisiert.
5. Zurück zu **Kryptografisches Modul** > **Modulschlüssel**.



In der Tabelle ist ein zusätzlicher Modulschlüssel aufgeführt. Der neu rotierte Schlüssel wird „Aktiv“ und der letzte Schlüssel wird „Deaktiviert“.

Importieren Sie einen Schlüssel aus einem Webservice

Laden Sie einen externen Kundenschlüssel sicher in Ihre Instanz hoch, indem Sie einen Schlüssel aus einem Webservice importieren (z. B. die Schlüssel-REST-API). Sowohl symmetrische als auch asymmetrische öffentliche Schlüssel können in ein kryptografisches Zielmodul KMF importiert werden.

Der zu importierende Schlüssel (der Zielschlüssel) muss mit einem Schlüssel zum Umschließen verschlüsselt werden, bevor er in das kryptografische Zielmodul der Instanz hochgeladen wird. Dieser Schlüssel zum Umschließen ist die öffentliche Komponente eines öffentlichen/privaten Schlüsselpaars, das in der Instanz vorhanden sein muss. Der Schlüssel ist eine Voraussetzung, bevor der umschlossene Zielschlüssel über Aus Webservices importieren hochgeladen werden kann.

Diese beiden separaten Verfahren (Import des umschlossenen Schlüsselpaars und Import des umschlossenen Zielschlüssels aus einem Webservice) werden in der folgenden Dokumentation beschrieben. Dieses Schlüsselpaar muss generiert und hochgeladen werden, damit es im internen kryptografischen Modul „Schlüsselimport“ der Instanz verfügbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In diesem Beispiel wird OpenSSL für die Schlüssel- und Zertifikatgenerierung und das Postman-API-Testtool verwendet, um die Verwendung der REST-API zu zeigen. Ersetzen Sie andere vergleichbare Tools basierend auf Ihren Unternehmensanforderungen.

Importieren Sie das Schlüsselpaar zum Packen/Entpacken

Konfigurieren Sie Key Management Framework Importeinstellungen, bevor Sie einen Schlüssel importieren.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager

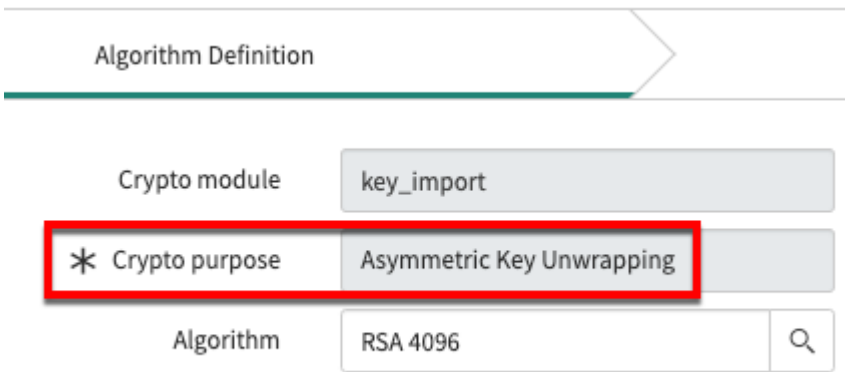
Warum und wann dieser Vorgang ausgeführt wird
In diesem Beispiel wird OpenSSL für die Schlüssel- und Zertifikatgenerierung verwendet. Ersetzen Sie andere vergleichbare Tools basierend auf Ihren Unternehmensanforderungen.

Prozedur

1. Verwenden Sie in Ihrer lokalen Umgebung das Terminal, um ein Zertifikat zu erstellen.
   Beispiel: `openedssl req -x509 -sha256 -nodes -days 365 -newkey rsa:4096 -keyout wrap_private.key -out wrap_public.crt`

   Dieses Zertifikat ist eine öffentliche Komponente, die einen Schlüssel enthält. Das Zertifikat wird verwendet, um einen symmetrischen AES-Schlüssel zu umschließen.

2. Verwenden Sie in Ihrer lokalen Umgebung das Terminal, um einen Schlüsselspeicher zu erstellen, der ein öffentliches Zertifikat (mit dem Schlüssel zum Packen) und einen privaten Schlüssel zum Entpacken enthält.
   Beispiel:`openedssl pkcs12 -export -in wrap_public.crt -inkey wrap_private.key -name "wrapping_key_alias" -out wrap_keystore.p12`
3. Navigieren Sie in Ihrer Instanz zu **Alle** > **Schlüsselverwaltung** > **Einstellungen importieren** > **Schlüsselimporteinstellungen**.
4. Vergewissern Sie sich im Abschnitt „Algorithmusdefinition“, dass der **kryptografische Zweck** auf *`Asymmetrische Schlüsselentnahme festgelegt`*



   `ist`.
5. Wählen Sie einen geeigneten Algorithmus aus, der dem asymmetrischen Schlüsselmaterial für den importierten Schlüsselspeicher entspricht.
   Weitere Informationen finden Sie unter Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.
6. Wählen Sie **Weiter**.
7. Wählen Sie im Abschnitt „ **Lebenszyklusdefinition** “ **Weiter** aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie im Abschnitt **Schlüsselursprung** entweder **Import aus PKCS12** oder **Import aus BCFKS** im Feld **Ursprung** aus.

   Hinweis:
   Wenn Sie den Beispielschlüsselspeicher aus Schritt 1 verwenden, wählen Sie **Aus PKCS12 importieren aus**.

9. Geben Sie einen **Schlüsselalias** ein, um den Schlüssel zu identifizieren.
   Dieser Alias muss mit dem Schlüsselalias (oder „Anzeigename“) übereinstimmen, der beim Generieren des hochzuladenden Zertifikats oder Schlüsselspeichers angegeben wurde. Wenn wir das obige Beispiel fortsetzen, wäre dies `wrap_key_alias`.

10. Wählen Sie **Weiter**.
    Der Abschnitt „ **Schlüsselerstellung** “ enthält den Link **Schlüssel** importieren, über den ein Dialogfeld zum Hochladen des Schlüsselspeichers angezeigt wird. Wenn wir das Beispiel fortsetzen, wäre dies `wrap_keystore.p12`.

Importieren Sie einen umschlossenen Schlüssel aus einem Webservice

Laden Sie Ihren umschlossenen Schlüssel mithilfe der Funktion „Schlüssel aus Webservice importieren“ in ein kryptografisches Modul hoch. In diesem Beispiel wird ein symmetrischer Schlüssel verwendet. Ähnliche Schritte können zum Importieren eines asymmetrischen Schlüssels verwendet werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager (Modulkonfiguration), sn_kmf.cryptographic_operator (REST-Vorgang Basic Authentication)

Warum und wann dieser Vorgang ausgeführt wird

KMF Importschlüssel-Endpunktzugriff ist erforderlich, um den Schlüsselimportvorgang abzuschließen.

In diesem Beispiel wird OpenSSL zum Generieren von Schlüsseln und Zertifikaten verwendet. Sie können andere vergleichbare Tools basierend auf Ihren Anforderungen ersetzen.

Prozedur

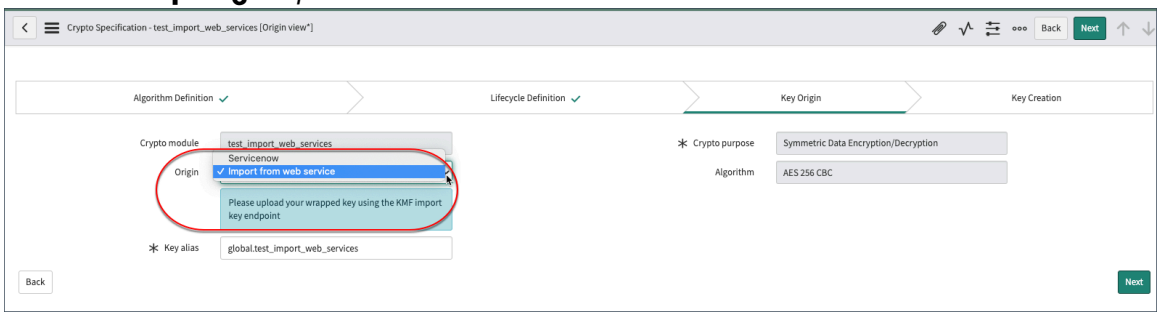
1. Verwenden Sie das Terminal auf Ihrem lokalen Gerät, umschließen Sie Ihren symmetrischen Schlüssel mit dem öffentlichen Schlüssel des Moduls „Schlüsselimport“.
   Beispiel: `openedssl pkeyutl -encrypt -pubin -inkey public_wrapping_key.pem -in metric_key.bin -pkeyopt rsa_papping_mode:oaep -pkeyopt rsa_oaep_md:sha256 -out wrap_symmetrisch_key.txt`
   In diesem Beispiel wird eine umschlossene Schlüsseldatei mit dem Namen `wrap_symmetrisch_key.txt` erstellt.

2. Erstellen Sie ein kryptografisches Modul, das an die API gebunden werden soll.
   Weitere Informationen finden Sie unter oder.

3. Fügen Sie eine kryptografische Spezifikation mit den folgenden Auswahlmöglichkeiten hinzu.

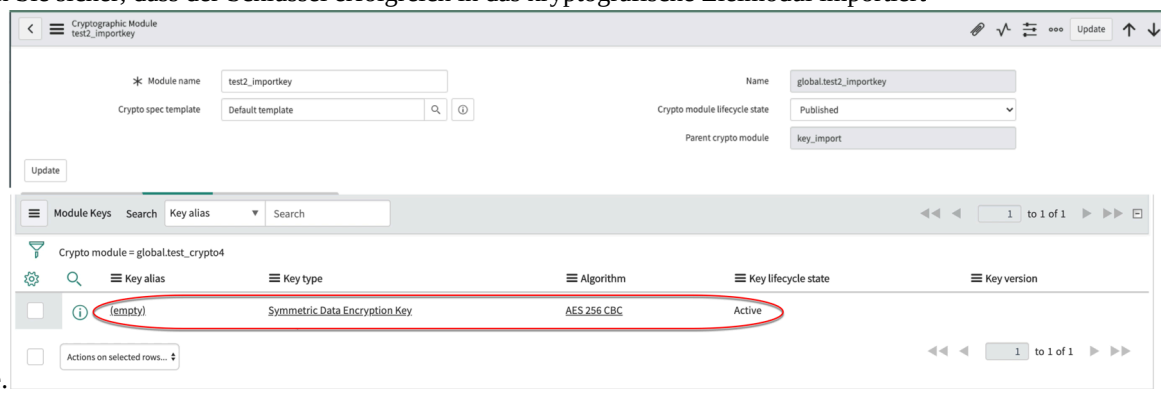
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kryptografischer Zweck**: *Symmetrische Datenverschlüsselung/-entschlüsselung*.
- **Schlüsselursprung**: *Import aus Webservice*



Weitere Informationen finden Sie unter oder.

4. Führen Sie eine *HTTP-POST-Anforderung* für den Import aus einem Webservice-REST-Endpunkt aus. Ein erfolgreicher Import des öffentlichen Schlüssels führt zu einer HTTP-Antwortnachricht mit dem *Status 200*.
5. Stellen Sie sicher, dass der Schlüssel erfolgreich in das kryptografische Zielmodul importiert



wurde.

Key Management Framework Gesundheit

Greifen Sie bei Bedarf auf Integritätsstatusinformationen für Key Management Frameworkzu. Warnungs- und Fehlfunktionsfehler enthalten eine detaillierte Meldung.

Vorbereitungen

Erforderliche Rolle: sn_kmf_cryptographic Auditor oder sn_kmf_admin oder sn_kmf_cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Jede Komponente von Key Management Framework ist umrissen und meldet die folgenden Status und Farben:

- Grün/Funktionsfähig: Die Komponente ist betriebsbereit, es sind keine Fehler zu melden.
- Grau/Deaktiviert: Die Komponente ist inaktiv, daher wird keine Integritätsprüfung durchgeführt.
- Gelb/Verschlechtert: Warnung, die Komponente funktioniert, aber es können Verzögerungen/vorübergehende Probleme auftreten.
- Rot/Störung: Ein schwerwiegender Fehler verhindert, dass die Komponente funktioniert, was wahrscheinlich zu teilweisen Ausfällen führt.

Komponenten können Unterkomponenten mit einzelnen Berichten enthalten, und ihr eigener Integritätsstatus wirkt sich wie folgt auf das übergeordnete Element aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn alle Unterkomponenten inaktiv sind, wird das übergeordnete Element als inaktiv angezeigt. Inaktive Unterkomponenten wirken sich nicht auf die Integrität ihrer übergeordneten Elemente aus.
- Wenn eine oder mehrere Unterkomponenten beeinträchtigt sind oder eine Fehlfunktion aufweisen, wird die übergeordnete Integrität als verschlechtert angezeigt.
- Wenn alle Unterkomponenten eine Fehlfunktion melden, wird auch die übergeordnete Komponente als fehlerhaft gemeldet.

Weitere Informationen zu Unterkomponenten finden Sie unter Schlüssel auf Instanzebene im Key Management Framework.

Hinweis:
Integritätsprüfungen werden alle 15 Sekunden ausgeführt. Aktualisieren Sie die Integritätsseite, um den Bericht erneut auszuführen.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > > **Diagnosen**.
2. Überprüfen Sie die folgenden Integritätsstatusinformationen:

Diagnoseinformationen

Kategorie	Details
Schlüssel sicher	Überprüft, ob eine Verschlüsselung versucht wird.
Dateischlüsselspeicher	Überprüft, ob ein Instance Root Key (IRK)-Abrufversuch auftritt. **Hinweis:** Der Dateischlüsselspeicher ist eine Offline-Alternative zu Key Secure, die für lokale Instanzen und Entwicklerinstanzen verwendet wird.
GlideEncrypter	Überprüft, ob ein kryptografisches Modul, eine Spezifikation und ein Schlüssel auf GlideEncrypter-Instanzebene vorhanden sind. **Hinweis:** GlideEncrypter ist eine skriptfähige Komponente, die die transparente Verschlüsselung von Password2 -Feldern und andere veraltete Verschlüsselungsanwendungen über den Key Management Frameworkermöglicht.
Instance Key Encryption Key (IKEK)	Überprüft, ob der Schlüssel aus dem Dateischlüsselspeicher oder KeySecure abgerufen werden kann.
HMAC-Schlüssel der Instanz	Überprüft, ob der Schlüssel aus dem Dateischlüsselspeicher oder KeySecure abgerufen werden kann.
Vault-PKI	Überprüft die Vault-Konnektivität, um sicherzustellen, dass der asymmetrische Verschlüsselungsschlüssel der Instanz (IAEK) und der Signaturschlüssel der Instanz (ISK) verwendet werden können und aus Vault abgerufen werden können.
EJBCA PKI	Überprüft die LDAP-Konnektivität, um sicherzustellen, dass IAEK und ISK verwendbar sind und aus dem Cache und LDAP abgerufen werden können.
Instanz-PKI	Überprüft den Dateischlüsselspeicher und KeySecure auf einen Schlüssel und ob das Zertifikat vorhanden ist und mit dem symmetrischen Schlüssel übereinstimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Details
	Hinweis: Instanz-PKI ist nur für Instanzen innerhalb eines ServiceNow -Rechenzentrums verfügbar.

Wenden Sie sich an Kundenservice und Support, um Unterstützung bei der Problembehandlung zu erhalten.

Bereiten Sie Ihre Instanz auf die Einstellung von GlideEncrypter vor

Verwenden Sie ein Instanz-Scan-Skript, um GlideEncrypter-API-Aufrufe in Ihrer Instanz zu finden und zu entfernen. Das Entfernen dieser Aufrufe ist ein notwendiger Schritt, um die 3DES-Verschlüsselung in Ihrer Instanz veraltet zu machen.

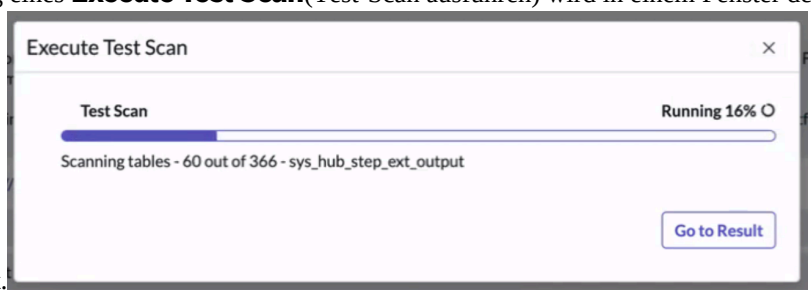
Vorbereitungen

Erforderliche Rolle: admin

Die GlideEncrypter-API soll ab dem Xanadu-Release von ServiceNoweingestellt werden. Das Entfernen von GlideEncrypter-Aufrufen aus Ihrem Skript ist ebenfalls ein notwendiger Schritt, bevor Sie die 3DES-Verschlüsselung in Ihrer Instanz als veraltet festlegen.

Prozedur

1. Navigieren zu **Alle** > **Instanz-Scan** > **Suites**.
2. Wählen Sie in der Liste **Suites** die Option **Veraltete APIs**aus
3. Wählen Sie im Datensatz „ **Suites** “ in der zugehörigen Liste „ **Prüfungen** “ die **Option Veraltete API: GlideEncrypter** aus.
   Die **Überprüfung** des Spaltentyps wird angezeigt. Dieser Datensatz enthält eine Beschreibung der Prüfung sowie Informationen zu und Links dazu, wie die von der Prüfung gefundenen Datensätze aktualisiert werden.
4. **Wählen Sie** im Datensatz „Spaltentypprüfung“ die **Option Testprüfung** aus, um den Scan auszuführen.
   Während der Scan-Ausführung eines **Execute Test Scan**(Test-Scan ausführen) wird in einem Fenster der Fortschritt des Scans angezeigt.



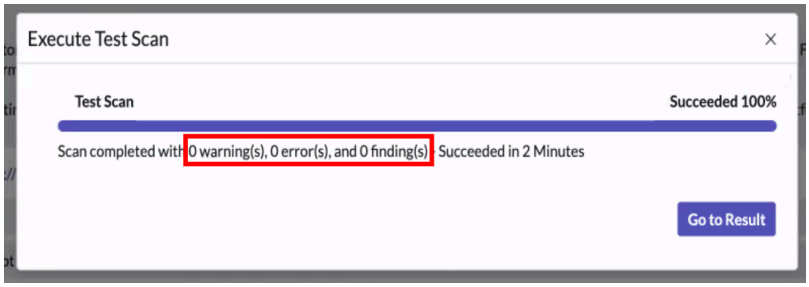
   Hinweis:
   Dieser Scan überprüft nur Datensätze, die vom Kunden erstellt oder geändert wurden.

5. Wenn der Scan abgeschlossen ist, wählen **Sie Zu Ergebnis wechseln**, um den **Scan-Ergebnisdatensatz** anzuzeigen.
   Im **Scan-Ergebnisdatensatz** zeigt die Liste „ **Scanfunde** “ eine Liste der Datensätze in Ihrer Instanz an, die die **GlideEncrypter-** API verwenden.
6. Wählen Sie in der Liste „ **Scanfunde** “ das Feld **Anzahl** aus, um zu einem Datensatz zu navigieren.
7. Ändern Sie alle Skripts im Datensatz, die die **GlideEncrypter-** API verwenden.
   Weitere Informationen zu Alternativen zu **GlideEncrypter**finden Sie unter Alternativen zu veralteten GlideEncrypter-APIs .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Nachdem **Sie GlideEncrypter-** Aufrufe aus Ihren Skripts entfernt haben, führen Sie den Scan erneut aus, um sicherzustellen, dass keine Aufrufe an die API mehr vorhanden sind.



Nächste Maßnahme

GlideEncrypter-Nutzung von 3DES für Passwort2-Felder veraltet

GlideEncrypter-Nutzung von 3DES für Passwort2-Felder veraltet

Stellen Sie sicher, dass Ihre Instanz ausschließlich den sichereren Advanced Encryption Standard (AES) für die Verschlüsselung und Entschlüsselung Ihrer Password2-Daten verwendet.

Ab Romewerden Passwort2-Daten mit Key Management Frameworkgeschützt, der den moderneren AES-Algorithmus (Advanced Encryption Standard) verwendet. Einige Konfigurationen und Fallbacks in Passwort2-Logik können jedoch weiterhin den 3DES-Algorithmus zur Verschlüsselung und Entschlüsselung verwenden.

Im Release Vancouver können Administratoren den 3DES-Algorithmus vollständig einstellen. Nach Abschluss dieser Änderung verwendet Ihre Instanz ausschließlich die AES-Verschlüsselung für alle Verschlüsselungs- und Entschlüsselungsaufgaben im Zusammenhang mit Passwort2-Daten. Diese Änderung bietet eine bessere Instanzsicherheit als die 3DES-Verschlüsselung und ist erforderlich, um NIST-konform zu bleiben.

Überlegungen vor der Einstellung

Übertragen von Passwort2-Daten zwischen Instanzen

Wenn Sie mit Passwort2 verschlüsselte Texte an andere Instanzen übertragen, müssen Sie sicherstellen, dass KMF Key Exchange zwischen Quell- und Zielinstanzen aktiviert ist. Diese Konfiguration stellt sicher, dass die zum Verschlüsseln von Passwort2-Texten verwendeten Schlüssel in beiden Instanzen zum Entschlüsseln der mit Passwort2 verschlüsselten Texte verfügbar sind. Berücksichtigen Sie vor der Einstellung von 3DES die folgenden Anwendungsfälle, die sich auf Passwort2-Daten zwischen Instanzen auswirken können.

- Wenn sich in Ihrer Instanz Anwendungen befinden, die Passwort2-Daten verwenden, stellen Sie sicher, dass KMF Ressourcenaustausch in dieser Instanz installiert ist. KMF Ressourcenaustausch stellt sicher, dass Schlüssel auf Instanzebene, die zum Verschlüsseln der password2-Daten in der Quellinstanz verwendet werden, in den Zielinstanzen zur Entschlüsselung verfügbar sind. Weitere Informationen finden Sie unter Key Management Framework Ressourcenaustausch.
- Wenn Sie password2-Daten über XML oder Datenquellen exportieren möchten, stellen Sie sicher, dass für die Zielinstanz KMF Key Exchange aktiviert ist. Diese Konfiguration stellt sicher, dass die Schlüssel auf Instanzebene,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die zum Verschlüsseln der password2-Daten in der Quellinstanz verwendet werden, in den Zielinstanzen zur Entschlüsselung verfügbar sind. Weitere Informationen zu dieser Konfiguration finden Sie unter Key Management Framework Schlüsselaustausch.

Wichtig:
Die obigen Beispiele zeigen häufigere Szenarien. Wenn Sie jedoch mit Passwort2 verschlüsselten Text auf andere Weise zwischen Instanzen übertragen, müssen Sie KMF Ressourcenaustausch konfigurieren, um sicherzustellen, dass die Zielinstanz Passwort2-Daten entschlüsseln kann.

Downgrade einer Instanz nach der 3DES-Einstellung

Folgendes gilt nur für Instanzen mit password2-Feldern mit Eingabelängen von mehr als 125 Zeichen, und Sie haben die 3DES-Verschlüsselung bereits veraltet.

Führen Sie die folgenden Schritte aus, bevor Sie den Klon initiieren, um ein Downgrade einer Instanz auf einen früheren Release als Vancouver durchzuführen.

1. Überprüfen Sie, ob die Datenerhaltung so konfiguriert ist, dass die Daten im Passwort2-Feld erhalten bleiben.
2. Wenn ja, wenden Sie sich vor der Anforderung eines Klons an den ServiceNow -Support, um die 3DES-Einstellung zu deaktivieren. Verwenden Sie im Feld **Grund** die Option „Klon-Downgrade erforderlich für Passwort2-Support“.

Veraltete password2-Felder

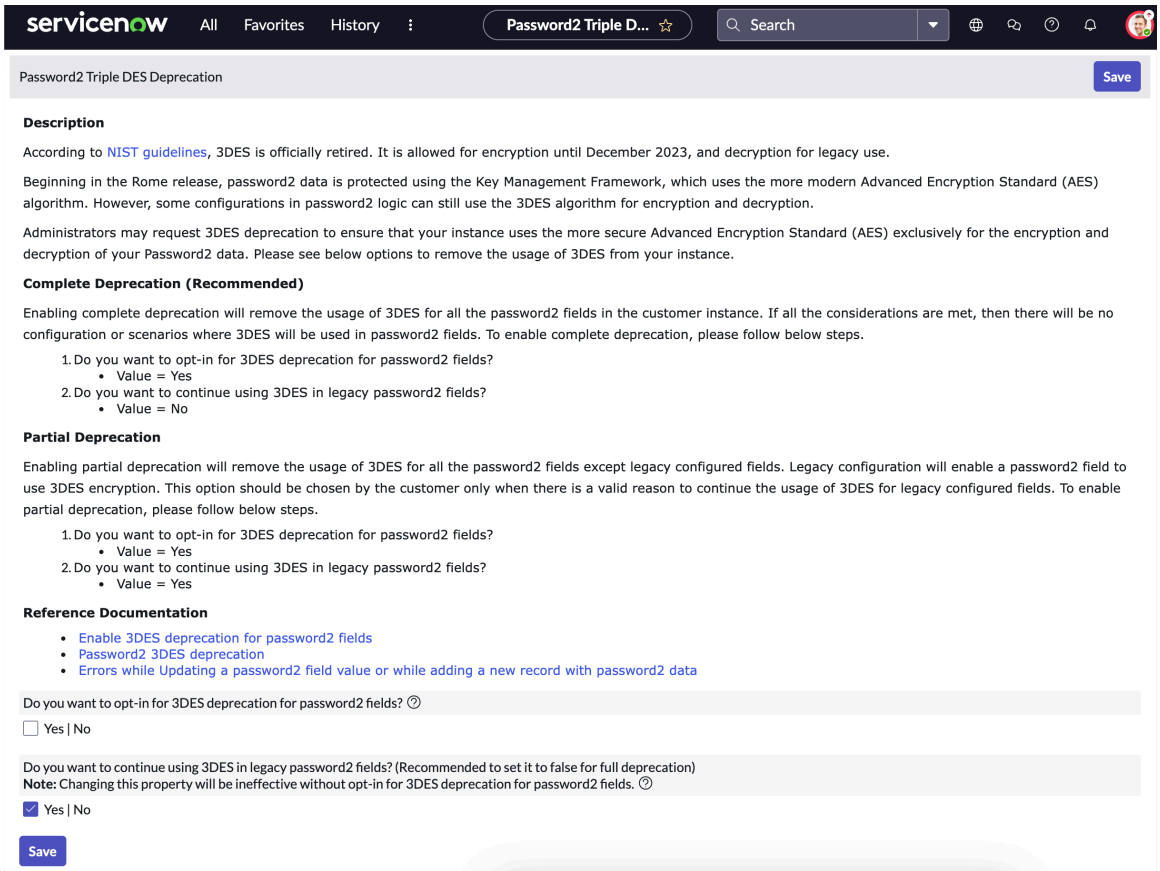
Ihre Instanz verwendet die 3DES-Verschlüsselung, um Passwort2-Daten in veraltete Passwort2-Daten (vorRome) zu konvertieren. Nach der Einstellung der Unterstützung der 3DES-Verschlüsselung ist diese Option nicht mehr verfügbar. Wenn Sie diese Funktion weiterhin benötigen, fordern Sie die teilweise Einstellung an (Details finden Sie im nächsten Abschnitt).

Vorgehensweise zur Einstellung der Unterstützung von 3DES

Nachdem Sie die vorherigen Anwendungsfälle überprüft haben, aktivieren Sie je nach Bedarf entweder die teilweise oder vollständige Einstellung. Bei beiden Optionen können Sie auf das Formular zugreifen, um die Einstellung zu steuern, indem Sie zu navigieren **Alle** > **Systemsicherheit** > **Sicherheitscompliance** > **Einstellung von Dreifach-DES für Passwort2**.

Wichtig:
Sie müssen zum Sicherheitsadministrator hochstufen, um das **Security Compliance** -Modul anzuzeigen und diese Schritte auszuführen. Details zu diesem Prozess finden Sie unter Führen Sie eine Erhöhung auf eine privilegierte Rolle durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Formular **„Passwort2-Dreifach-DES-Veraltung“** enthält Informationen zum Prozess für die vollständige und teilweise 3DES-Einstellung. Wählen Sie die Optionen für die vollständige oder teilweise Einstellung aus, und klicken Sie auf **Speichern**.

Vollständige Einstellung

Wenn Sie die vollständige Einstellung aktivieren, wird die Verwendung von 3DES für alle Passwort2-Felder in Ihrer Instanz entfernt. Wenn alle Voraussetzungen erfüllt sind, gibt es keine Konfigurationen oder Szenarien, in denen 3DES in Passwort2-Feldern verwendet wird.

So aktivieren Sie die vollständige Einstellung:

- Wählen **Sie Möchten Sie die Einstellung von 3DES für Passwort2-Felder aktivieren?**
- Deaktivieren **von Möchten Sie 3DES in Passwort2-Feldern von Vorgängerversionen weiterhin verwenden?**

Teilweise Einstellung

Wenn Sie die teilweise Einstellung aktivieren, wird die Verwendung von 3DES für alle Passwort2-Felder mit Ausnahme der in Vorgängerversionen konfigurierten Felder entfernt. Die Legacy-Konfiguration für password2-Felder verwendet weiterhin die 3DES-Verschlüsselung. Wählen Sie diese Option nur aus, wenn Sie 3DES für in Vorgängerversionen konfigurierte Felder weiterhin verwenden müssen.

So aktivieren Sie die teilweise Einstellung:

- Wählen **Sie Möchten Sie die Einstellung von 3DES für Passwort2-Felder aktivieren?**
- Wählen **Sie Möchten Sie weiterhin 3DES in veralteten Passwort2-Feldern verwenden?**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach Einstellung der Unterstützung von GlideEncrypter

Nach Abschluss des Veraltungsprozesses gelten die folgenden Informationen für Ihre Instanz.

- password2-Felder unterstützen weiterhin die Entschlüsselung (aber keine Verschlüsselung) von mit 3DES verschlüsselten Daten.
- Vorhandene mit 3DES verschlüsselte Daten in Passwort2-Feldern bleiben unverändert, bis der Feldwert von einem Benutzer oder Workflow aktualisiert wird.
- Bei jeder Aktualisierung des Werts eines password2-Felds wird 3DES-verschlüsselter Text entfernt und durch den von KMF mit AES verschlüsselten Text ersetzt.
- In einigen Situationen zeigt Ihre Instanz beim Speichern der Passwortdaten möglicherweise einen Fehler an:

  Aktion abgebrochen: Der Passwortwert kann aufgrund eines technischen Problems nicht gespeichert werden. Weitere Informationen finden Sie in KB1296997.

  Wenn dieser Fehler angezeigt wird, finden Sie weitere Informationen im Knowledge Base-Artikel KB1296997 .

Key Management Framework Ressourcenaustausch

ServiceNow® Ressourcenaustausch ist eine Funktion von KMF, mit der Sie Ressourcen zwischen Instanzen auf sichere Weise austauschen können.

Terminologie

Wenn Sie Ressourcenaustauschverwenden, verweisen Sie auf die folgende Terminologie:

Ressourcenaustausch Terminologie

Name	Beschreibung
Ressourcenaustausch	Der Prozess zum Austausch von Ressourcen zwischen Instanzen.
Key Exchange (KE)	Der Prozess zum Austausch von Schlüsseln über Instanzen.
Schlüsselquelleninstanz (Schlüsselquelle)	Die Instanz, die die Schlüssel besitzt.
Schlüsselzielinstanz (Schlüsselziel)	Die Instanz, die die Schlüssel anfordert.

Übersicht

Ressourcenaustausch verwendet die kryptografischen APIs von KMF, um Vertraulichkeit, Integrität, Authentifizierung und Nicht-Zurückweisung zu gewährleisten. Derzeit unterstützt RessourcenaustauschKey Exchange die Funktionalität []. Weitere Informationen finden Sie unter Key Management Framework Schlüsselaustausch.

Key Management Framework Schlüsselaustausch

KMF Key Exchange ist eine Teilmenge der Funktion von KMF Ressourcenaustausch. Key Exchange überträgt verschlüsselte Daten sicher über mehrere Instanzen hinweg.

Übersicht über Key Exchange

Key Exchange überträgt Schlüssel sicher zwischen Instanzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

KMF Key Exchange bietet Kunden eine sichere Möglichkeit, KMF -Schlüssel zwischen Instanzen auszutauschen. Ein Anwendungsanwendungsfall ist das Klonen von Daten. Mit Key Exchangewerden Krypto-Modulschlüssel während des Datenklons von KMF -Komponenten kopiert. Kryptografische Module, Modulschlüsselspezifikationen und Modulzugriffsrichtlinien sind im Klonvorgang enthalten. Die Übertragung von Schlüsseln ist nicht enthalten.

Arbeiten mit Key Exchange

Administratoren, die KMF für die Verschlüsselung auf Spaltenebene verwenden, können Key Exchange verwenden, um beim Datenklonen die Schlüssel zwischen Produktionsinstanzen zu klonen. Beim Klonen von Daten kann der Administrator/ KMF Kryptografiemanager Folgendes ausführen:

- Tauschen Sie alle Schlüssel für die anderen Instanzen aus.
- Tauschen Sie bestimmte Schlüssel einmal oder in regelmäßigen Abständen mit der anderen Instanz aus.
- Senden Sie bei Bedarf Anforderungen von der Zielinstanz an die Schlüsselquellinstanz.
- Tauschen Sie Schlüssel von Quelle zu Ziel aus, um den Geheimtext neu zu schlüsseln.
  - Verwalten Sie die Ablaufzeit der Anforderung mit der Möglichkeit, Schlüssel zu löschen oder die Schlüsselaustauschanforderung abzulehnen, wenn die Anforderung abgelaufen ist.
  - Nachdem die Anforderung abgeschlossen und der Schlüssel importiert wurde, wird der verwendete Schlüssel als abgelaufen und mit einem Zeitstempel versehen festgelegt.
  - Schlüsseltext in der Zielinstanz, der mit Schlüsseln aus der Quelle verschlüsselt wurde, erneut eingeben

Unterstützte Modi

Key Exchange unterstützt mehrere Modi auf der Krypto-Spezifikationsebene des Verschlüsselungsmoduls:

Modus	Beschreibung
Automatisch (keine Konfiguration, Standardverhalten)	Alle Schlüssel werden während des Datenklonvorgangs ohne zusätzliche Konfiguration automatisch gesendet.
Konfigurierbar (einmaliges Konfigurations-Setup)	Der Administrator konfiguriert die Schlüssel, die während des Datenklonvorgangs gesendet werden sollen.
Manuell (Person in der Schleife)	Der Administrator sendet eine On-Demand-Anforderung für die Zielinstanz an die Quelle. Die Anforderung muss von einem Administrator in der Schlüsselquelleninstanz genehmigt werden.
Schlüssel erneut eingeben (automatisierte Anforderung)	Der Administrator wählt während des Setup-Vorgangs für das Klonen die Option zur Schlüsselerneuung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie den Schlüsselaustausch

Key Management Framework (KMF) generiert während der Neuinstallation oder des Upgrades der Instanz automatische Schlüsselaustauschanforderungen für unterstützte kryptografische Module. verwaltet den Datenverschlüsselungsschlüssel lokal für die Instanz.

Vorbereitungen

Vor der Verwendung von Key Exchangemuss sowohl in der Ziel- als auch in der Quellinstanz ein kryptografisches Modul mit einem Schlüssel erstellt werden.

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Key Exchange -Anforderungen werden von der Zielinstanz initiiert.

Der automatische Schlüsselaustausch ist beim Klonen einer Instanz standardmäßig aktiviert, wobei die Eigenschaft in die Zielinstanz geklont wird. Konfigurieren Sie zusammen mit KMFSystemeigenschaften, um zu verwalten, wie Schlüssel während eines Instanzklons behandelt werden:

- **Automatischen Schlüsselaustausch deaktivieren:** Legen Sie die Eigenschaft `glide_encryption.auto_key_exchange.enabled` für wiederkehrende Klonanforderungen auf „ **false** “ fest.
- **Automatische Schlüsselaustauschanforderungen senden**: Legen Sie diese Eigenschaft auf **„wahr“ fest**.

Wichtig:
Die Basissystemeigenschaft ist standardmäßig auf „ **true** “ festgelegt, was bedeutet, dass beim Klonen einer Instanz der automatische Schlüsselaustausch aktiviert wird. Dieser Wert muss auf „ **false** “ festgelegt werden, wenn Sie die Funktion Schlüsseltext mit Schlüsselaustausch erneut schlüsseln oder den wiederkehrenden Schlüsselaustausch verwenden. Weitere Einzelheiten erhalten Sie unter Vorstellung des wiederkehrenden Schlüsselaustauschs.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen** > **Neu**.
2. Füllen Sie die Felder des Formulars aus.

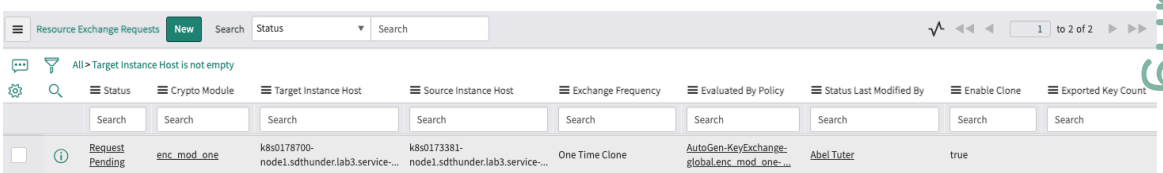
Ressourcenaustausch Felder des Anforderungsformulars

Name	Beschreibung
Austauschhäufigkeit	○ **Ad**-hoc: Sendet Anforderungen von der Schlüsselzielinstanz an die Quellinstanz. Geben Sie die sys_id der Instanz und die Hostinformationen für die Quelle ein. Nicht unterstützt mit „Rekey“ des Schlüsselaustauschs. ○ **Einmaliger Klon**: Einmaliger Austausch der Schlüssel von den Quellkrypto-Spezifikationen mit der Zielinstanz. ○ **Wiederkehrender Klon**: Tauschen Sie Schlüssel aus den ausgewählten Quellkrypto-Spezifikationen mit der Zielinstanz auf einem definierten wiederkehrenden Klon aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
<Source or Target> sys_id der Instanz	○ Ad-hoc: Geben Sie die **sys_id** für die Quellinstanz ein, von der die Schlüssel angefordert werden sollen. ○ **Einmaliger Klon**, **Wiederkehrender Klon**: Geben Sie die sys_id für die Zielinstanz ein, die die Anforderungen sendet. **Tipp:** Geben Sie im Anwendungsnavigator `stats.do` ein, um die Instanz-ID zu finden.
<Source or Target> Instanzhost	Geben Sie den Hoststandort oder den Namen der Quell- oder Zielinstanz ein. **Tipp:** Beispiel : `instanceA.service-now.com`
Krypto-Spezifikationen	Die Schlüssel aus der Krypto-Spezifikation in einem Krypto-Modul definieren die zu klonenden Schlüssel. Sowohl für einmalige als auch für wiederkehrende Klonanforderungen erstellt Ihre Instanz automatisch eine Zugriffsrichtlinie für das **Ressourcenaustauschmodul**. Sie müssen eine Richtlinie nicht manuell konfigurieren. **Hinweis:** Klicken Sie auf das Symbol „ “), um die verfügbaren kryptografischen Spezifikationen zu durchsuchen.
Erneute Schlüsselerstellung nach Schlüsselimport aktivieren	Option zum Aktivieren der automatischen Schlüsselerstellung.

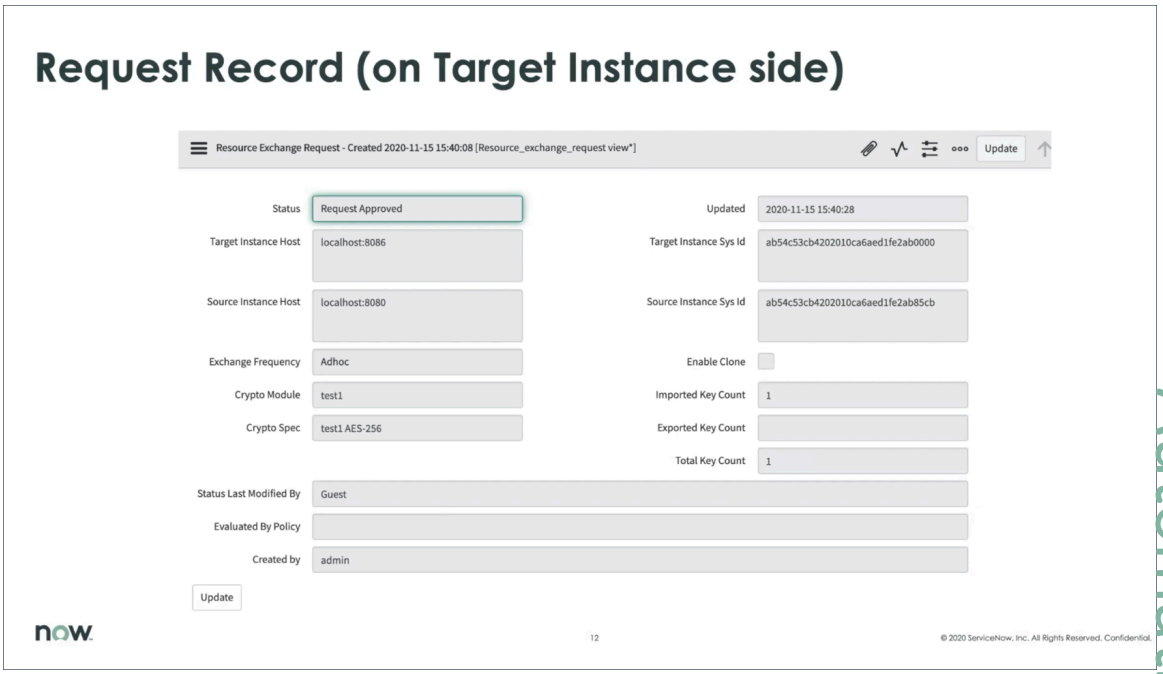
3. Wählen Sie **Absenden**.
   Bei Erfolg wird oben im Formular eine Bestätigung angezeigt. Die Tabelle „Anforderungen“ wird mit dem Eintrag **Anforderung ausstehend** sowohl in der Quellinstanz als auch in der Zielinstanz aktualisiert. Öffnen Sie den Anforderungsdatensatz, um den Status der Anforderung, die Anzahl der importierten Schlüssel und die Gesamtanzahl der Schlüssel auf dem Ziel- oder Quellhost anzuzeigen.



4. Die ausstehende Anforderung wird in der Quellinstanz akzeptiert, um den Austausch abzuschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Zeitpunkt des Klonens wird die Modulzugriffsrichtlinie in der Quellinstanz aufgerufen, um die Anforderung automatisch zu genehmigen und Schlüssel an das neu geklonte Ziel zu senden.



Ergebnisse
Nachdem versucht wurde, einen Schlüssel auszutauschen, aktualisiert Ihre Nicht-Produktionsinstanz die Systemeigenschaft *protected.script.values.kmf.rekeyed*. Diese Eigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] sichtbar, nachdem versucht wurde, einen Schlüssel auszutauschen. Wenn die Verschlüsselung mit dem ausgetauschten Schlüssel erfolgreich ist, hat diese Eigenschaft den Wert **true**. Andernfalls hat die Eigenschaft den Wert **false**. Wenn der Wert „false“ ist, versucht die Instanz am nächsten Tag erneut, zu verschlüsseln.

Schlüsseltext mit Schlüsselaustausch erneut schlüsseln

Ressourcenaustausch unterstützt das erneute Schlüsseln von Geheimtext in der Zielinstanz, der mit Schlüsseln aus der Quelle verschlüsselt wurde. Die Aktivität „Erneuter Schlüssel“ wird im Lebenszyklus des Schlüssels nachverfolgt.

Übersicht

Administratoren, die KMF für die Verschlüsselung auf Spaltenebene verwenden, können Key Exchange verwenden, um kryptografische Schlüssel zwischen Produktionsinstanzen beim Klonen von Daten neu zu schlüsseln. Ein aktiver Schlüssel muss zuerst auf der Zielinstanz für die erneute Schlüsselerstellung verfügbar sein, da für eine erneute Schlüsselerstellung ein aktiver Schlüssel erforderlich ist. Ein Verschlüsselungsauftrag wird automatisch erstellt und vom System ausgeführt, um den Quellschlüssel zu rotieren und neu zu schlüsseln und den Geheimtext erneut zu verschlüsseln.

Verwenden Sie Key Exchange für Folgendes:

- Legen Sie einen Ablaufzeitrahmen für die erneute Schlüsselerstellung fest.

  Wenn die Anforderung abgelaufen ist, wird die Anforderung abgelehnt, und der Schlüssel wird gelöscht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Automatisieren Sie die erneute Schlüsselung von Geheimtext, der mit Schlüsseln aus Quellinstanzen verschlüsselt wurde.

  Ein neuer geklonter Krypto-Schlüssel wird verwendet, um den Geheimtext in der Zielinstanz erneut zu verschlüsseln.

- Der Zweck „Rekey“ wird während des Klonvorgangs eingerichtet und als Teil des Klons automatisiert.
- Die Aktivität „ **Rekey** “ wird auf der Registerkarte „Modulschlüssel“ des kryptografischen Moduls nachverfolgt. Greifen Sie auf den Schlüssellebenszyklusstatus und die Schlüsselversion für die Schlüsselaktivität zu. Weitere Informationen finden Sie unter Schlüssel rotieren.

Konfigurieren Sie einen Key Exchange, und aktivieren Sie das Kontrollkästchen **Rekeying nach Schlüsselimport** aktivieren, um zu aktivieren. Details siehe Konfigurieren Sie den Schlüsselaustausch.

Vorstellung des wiederkehrenden Schlüsselaustauschs

Verwenden Sie diese Tour, um einen wiederkehrenden Schlüsselaustausch in Ihrer Instanz mit und Ressourcenaustauscheinzurichten.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Dieses Beispiel zeigt, wie eine Zielinstanz Schlüssel von einer Hostinstanz anfordert.

- Bevor Sie dieses Verfahren ausführen können, müssen Sie eine Instanz klonen. Weitere Informationen finden Sie unter Systemklon .
- **Automatischer Schlüsselaustausch**: Die Basissystemeigenschaft `glide_encryption.auto_key_exchange.enabled` ist standardmäßig „ **true** “, was bedeutet, dass beim Klonen einer Instanz automatisch aktiviert wird. Die Eigenschaft wird in die Zielinstanz geklont.
- Deaktivieren Sie die automatische, indem Sie die Eigenschaft auf **false**setzen.

Prozedur

1. Erstellen Sie in der Quellinstanz ein Krypto-Modul, oder greifen Sie mit column_level_encryption auf ein vorhandenes Krypto-Modul zu, und richten Sie die verschlüsselten Feldkonfigurationen für die Geheimtextverschlüsselung für Key Exchangeein.
   Weitere Informationen finden Sie unter und.

   a. Stellen Sie sicher, dass im Krypto-Modul Schlüssel generiert wurden.

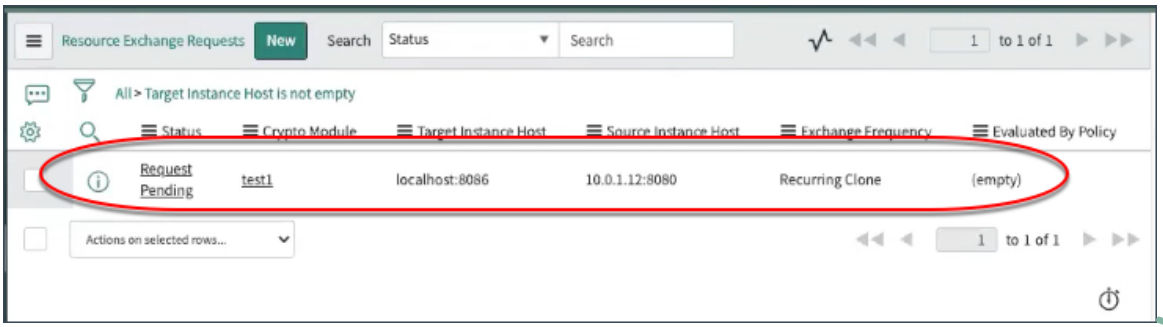
   Hinweis:
   Ihre Instanz erstellt automatisch eine Modulzugriffsrichtlinie, wenn die Klonanforderung ausgeführt wird.

2. Navigieren Sie in der geklonten Instanz zu **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen** > **Neu**.

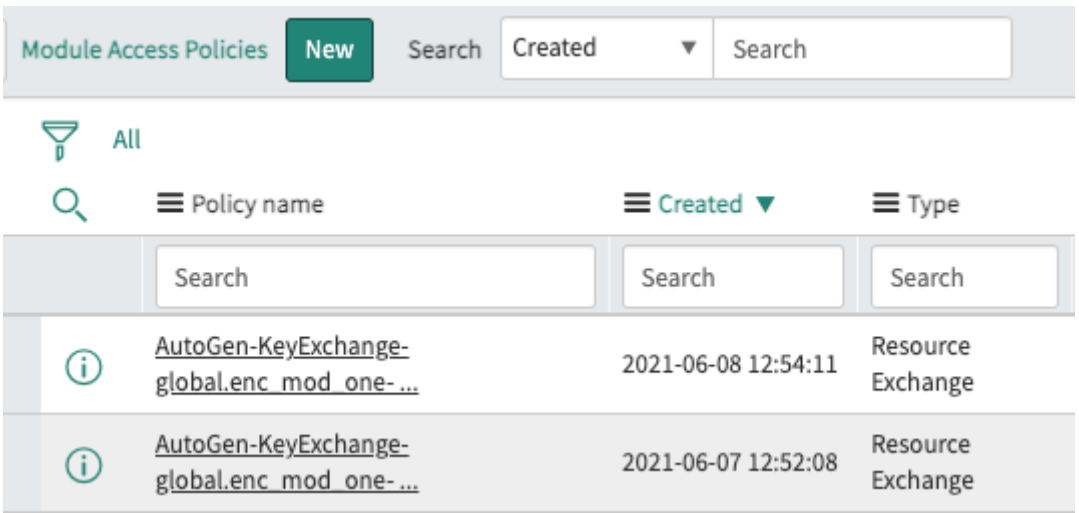
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

3. Füllen Sie das Formular aus, und wählen Sie **Wiederkehrender Klon** als Austauschhäufigkeit aus.
4. Navigieren Sie in der Zielinstanz des Klons zu **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen**.
   Die Anforderung von der Hostinstanz wird in der Tabelle angezeigt.

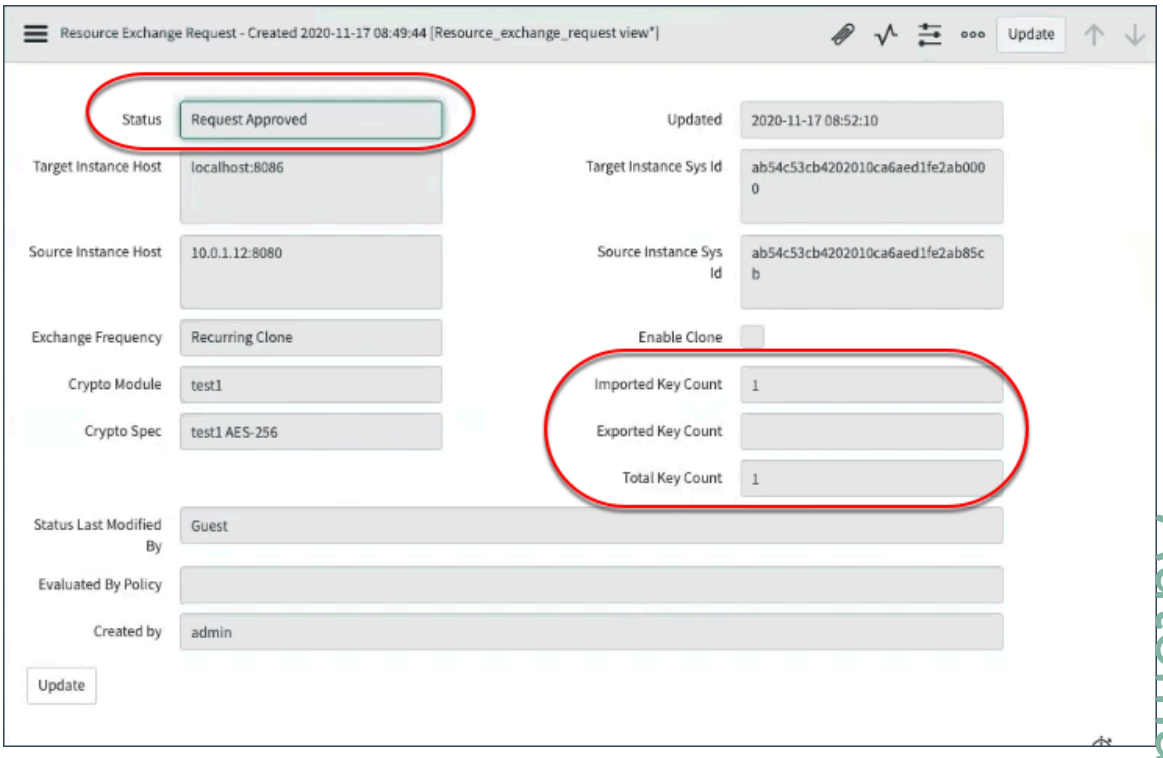


Wichtig:
Sowohl für einmalige als auch für wiederkehrende Klonanforderungen erstellt Ihre Instanz automatisch eine Modulzugriffsrichtlinie. Sie müssen eine Richtlinie nicht manuell konfigurieren. Zum Zeitpunkt des Klonens wird diese Richtlinie in der Quellinstanz aufgerufen, um die Anforderung automatisch zu genehmigen und Schlüssel an das neu geklonte Ziel zu senden.

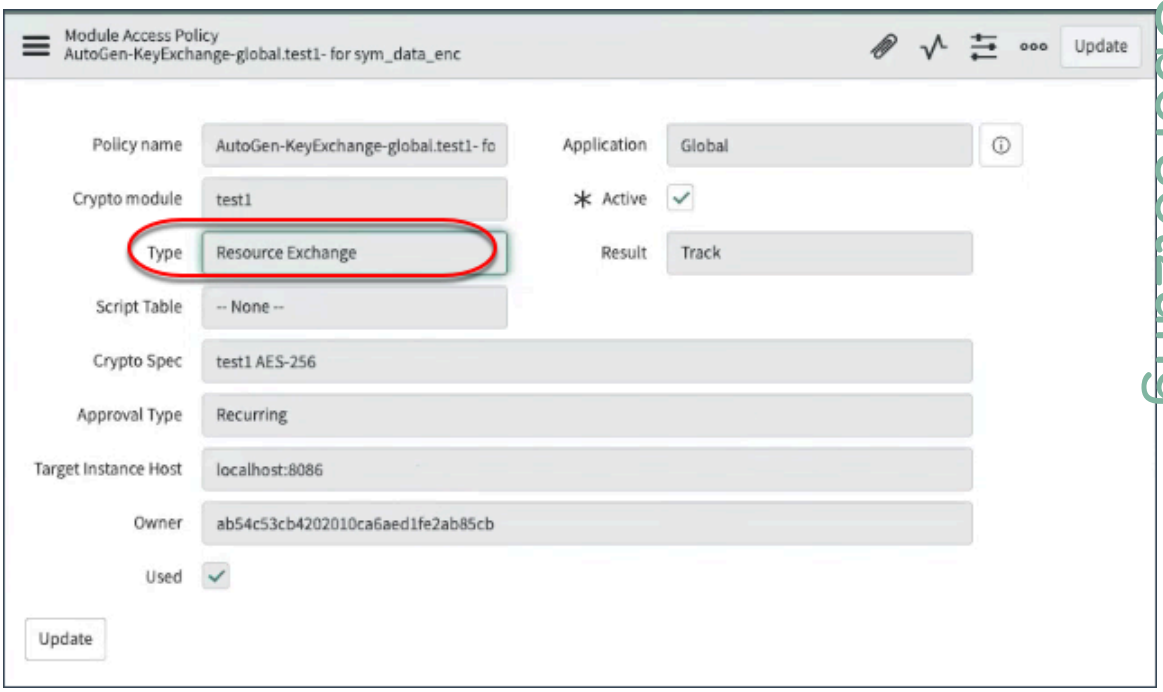


Im Formular „Anforderungen“ wird der Status auf „ **Anforderung genehmigt** “ aktualisiert, und das Feld Anzahl **importierter Schlüssel** wird im Datensatz angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Kehren Sie zur Hostinstanz zurück.
6. Zeigen Sie den Anforderungsdatensatz an, um die Anzahl der exportierten Schlüssel anzuzeigen.
7. Zeigen Sie den Datensatz der Modulzugriffsrichtlinie an, um zu sehen, dass der **Typ**Ressourcenaustauschist.



Hinweis:
Ressourcenaustausch unterstützt auch das erneute Schlüsseln von Geheimtext in der Zielinstanz. Weitere Informationen finden Sie unter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Nachdem versucht wurde, einen Schlüssel auszutauschen, aktualisiert Ihre Nicht-Produktionsinstanz die Systemeigenschaft `protected.script.values.kmf.rekeyed`. Diese Eigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] sichtbar. Wenn die Verschlüsselung mit dem ausgetauschten Schlüssel erfolgreich ist, hat diese Eigenschaft den Wert **true**. Andernfalls hat die Eigenschaft den Wert **false**. Wenn der Wert „false“ ist, versucht Ihre Instanz am nächsten Tag erneut, zu verschlüsseln.

Verschlüsselung auf Spaltenebene

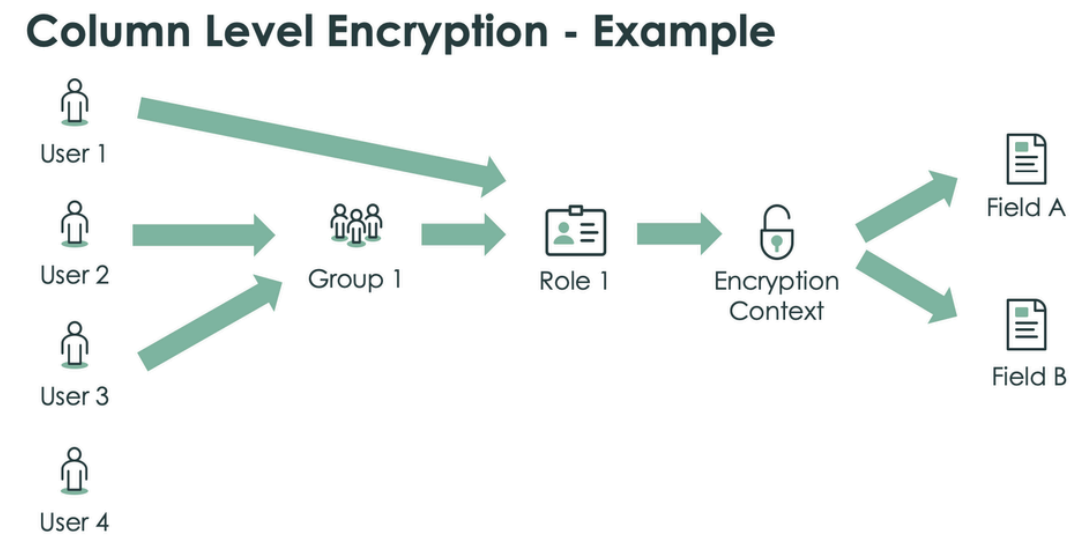
Column Level Encryption (CLE), ehemals Encryption Support, erlaubt und verweigert den Zugriff auf verschlüsselte Daten basierend auf der Benutzerrolle. Die Verschlüsselung auf Spaltenebene wird in um eine grundlegende Schlüsselverwaltung mit Verschlüsselungsmodulen erweitert, die kostenlos ist.

Über Verschlüsselung auf Spaltenebene

Hinweis:
Zuvor konfigurierte Verschlüsselungskontexte werden automatisch in Verschlüsselungsmodule konvertiert. Column Level Encryption (CLE) ist eine kostenlose Sicherheitsverbesserung der Verschlüsselungsunterstützung. Weitere Informationen zu den Verschlüsselungsoptionen finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

Die Implementierung der Verschlüsselung auf Spaltenebene beginnt mit der Definition eines oder mehrerer Verschlüsselungsmodule in Ihren Instanzen von Now Platform. Dieser Prozess umfasst die Auswahl eines Verschlüsselungsalgorithmus und die Bereitstellung eines entsprechenden geheimen Schlüssels. Der Zugriff auf Daten, die später mit der Funktion verschlüsselt werden, ist rollenbasiert, wobei Module Rollen zugeordnet sind. Benutzer ohne die richtige Rolle sehen das Feld überhaupt nicht. Abbildung 1 zeigt, wie die rollenbasierte Verschlüsselung funktioniert.

Abbildung 1 – Beispiel für rollenbasierte Verschlüsselung



Hier sind die Ergebnisse der Beziehungen in Abbildung 1:

- Benutzer 1 ist Mitglied von Rolle 1, die Zugriff auf das Verschlüsselungsmodul 1 bietet. Benutzer 1 kann den Inhalt von Feld A und Feld B sehen.
- Benutzer 2 und Benutzer 3 sind Mitglieder von Gruppe 1. Gruppe 1 ist Mitglied von Rolle 1, die jedem in Gruppe 1 den Zugriff auf Verschlüsselungsmodul 1 ermöglicht und Benutzer 2 und Benutzer 3 den Inhalt von Feld A und Feld B sehen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Benutzer 4 ist kein Mitglied einer Gruppe oder Rolle und hat keinen Zugriff auf Verschlüsselungsmodul 1. Benutzer 4 hat nicht nur keinen Zugriff auf Feld A oder Feld B, sondern Benutzer 4 sieht diese Felder nicht einmal in einem Formular. In einer Listenansicht wären die Werte leer.

Sie können auch eine wesentlich komplexere rollenbasierte Verschlüsselung implementieren.

Der rollenbasierte Zugriff muss auch entsprechend implementiert werden, damit dieses Feld für Benutzer zugänglich ist, denen das Verschlüsselungsmodul über eine Rolle zugewiesen ist.

Alle Verschlüsselungsschlüssel des Kunden, die bei der Verschlüsselung auf Spaltenebene verwendet werden, werden in derselben eindeutigen Instanzdatenbank gespeichert, in der die von ihnen verschlüsselten Daten gespeichert werden. Als weitere Sicherheitsmaßnahme werden sie mit einem für diese Instanz eindeutigen sekundären Schlüssel erneut verschlüsselt, wodurch der direkte Zugriff auf den Verschlüsselungsschlüssel für jedes Verschlüsselungsmodul durch einen Instanzadministrator oder ServiceNowverringert wird.

Verschlüsselte Daten auf Spaltenebene können nicht gefiltert werden.

Verschlüsselung auf Spaltenebene:

- Der Zugriff auf verschlüsselte Daten wird durch die Benutzerrolle bestimmt.
- Sie können die Stärke des Verschlüsselungsalgorithmus auswählen: AES-128 oder AES-256.
- Sie können Zeichenfolgentext, Datums- und Datums-/Uhrzeitfelder, Anhänge und URLs verschlüsseln.
- Verschlüsselungsmodule bieten eine Verschlüsselung mit Gleichstellungserhaltung.

Verschlüsselung auf Spaltenebene Enterprise unterstützt die folgenden zusätzlichen Funktionen:

- Vom Kunden bereitgestellte Schlüssel.
- Der Schlüsselzugriff ermöglicht Benutzersitzungen mit Zugriff auf das Modul, und der Schlüssel kann auf andere Back-End- oder Systembenutzerprozesse zugreifen.
- Skript, Ressourcenaustauschund App-Zugriff
- Erweiterte Unterstützung für Anhänge.
- Der Zugriff über die Anwendungsprogrammierschnittstelle (API) ist verfügbar.
- Die Reihenfolge erhaltende Verschlüsselung oder standardmäßige, nicht deterministische Verschlüsselung wird nicht unterstützt.

Standard- und Enterprise-Editionen

Die Verschlüsselung auf Spaltenebene ist in der Standard- und Unternehmensversion verfügbar. Column Level Encryption Enterprise ist ein kostenpflichtiges Plugin, das zusätzliche Funktionen sowie eine größere Anzahl von Modulen und Modulzugriffsrichtlinien bietet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen der Verschlüsselung auf Spaltenebene nach Version

Verschlüsselung auf Spaltenebene	Column Level Encryption Enterprise
• Der Zugriff auf verschlüsselte Daten wird durch die Benutzerrolle bestimmt • Unterstützung für bis zu 5 Module und Modulzugriffsrichtlinien (MAP). • Verschlüsselungsalgorithmen AES-128 und AES-256 • Verschlüsselung für Zeichenfolgentext, Datums- und Datums-/Uhrzeitfelder, Anhänge und URLs. • Verschlüsselungsmodule bieten eine Verschlüsselung mit Gleichstellungserhaltung. • Aktualisierte APIs `getDisplayValue()` und `setDisplayValue()`, die Klartextwerte zurückgeben und verschlüsselte Daten für verschlüsselte Felder einfügen können	Zusätzlich zu den links aufgeführten Funktionen unterstützt Column Level Encryption Enterprise die folgenden zusätzlichen Funktionen. • Unterstützung für mehr als 5 Module und Modulzugriffsrichtlinien (MAP). • Verschlüsselung für zusätzliche Feldtypen wie Journal, HTML und übersetzte Felder. • Konfigurierbare automatische Schlüsselrotation. • Vom Kunden bereitgestellte Schlüssel. Verwalten Sie den gesamten Schlüssellebenszyklus Ihrer Datenverschlüsselungsschlüssel. Optional können Sie in Ihrer Umgebung generierte Datenverschlüsselungsschlüssel sicher austauschen. • Flüchtige kryptografische Schlüssel • Aktualisierte APIs `getValue()` und `setValue()`.

Weitere Informationen zur Enterprise-Version dieses Produkts finden Sie unter Column Level Encryption Enterprise

Verschlüsselungsmethoden

Zu den Feldern, die die Verschlüsselung auf Spaltenebene verwenden, gehören:

- Neue oder vorhandene Felder für verschlüsselten Text.
- Zeichenfolge, Datum, Datum/Uhrzeit oder URL-Felder, die in den verschlüsselten Feldkonfigurationsdatensätzen enthalten sind.

Die Tabelle „Verschlüsselte Feldkonfigurationen“ [*sys_platform_encryption_configuration*] enthält einen Datensatz für jedes Feld, das mit Verschlüsselung auf Spaltenebene verschlüsselt ist. Mit dieser Tabelle kann ein Sicherheitsadministrator alle Felder in der Instanz überwachen, die Verschlüsselung auf Spaltenebene verwendet.

Hinweis:
Beim Upgrade werden für alle vorhandenen verschlüsselten Textfelder Datensätze für die Konfiguration verschlüsselter Felder erstellt. Wenn ein neues verschlüsseltes Textfeld hinzugefügt wird, wird standardmäßig ein Datensatz für die verschlüsselte Feldkonfiguration erstellt.

Verschlüsselte Feldkonfigurationen können Felder mit einer der folgenden Methoden verschlüsseln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode	Beschreibung
Einzelnes Verschlüsselungsmodul	Das Feld wird mit der Verschlüsselungsmethode verschlüsselt, die im Verschlüsselungsmodulfeld definiert ist. Benutzer, die nicht über den verschlüsselten Modulzugriff verfügen, können keine Feldwerte anzeigen oder aktualisieren.
Mehrere Verschlüsselungsmodule	Das Feld wird mit dem Verschlüsselungsmodul des ersten Benutzers verschlüsselt, der Daten in dieses Feld eingibt. Wenn der Benutzer über zwei oder mehr Verschlüsselungsmodule verfügt, wird das in der Verschlüsselungsmodulauswahl definierte Modul verwendet. Da das Verschlüsselungsmodul pro Datensatz festgelegt wird, können Felder in einer Liste unterschiedliche Verschlüsselungsmodule haben. Innerhalb eines einzelnen Datensatzes kann das Feld jedoch nur von einem Modul verschlüsselt werden. Wenn ein Feld für verschlüsselten Text erstellt wird, wird eine verschlüsselte Feldkonfiguration mit der Methode für mehrere Verschlüsselungsmodule erstellt. Verschlüsselte Textfelder und Felder, die mit der Methode mit mehreren Verschlüsselungsmodulen verschlüsselt sind, verhalten sich gleich. **Hinweis:** Massenverschlüsselung ist nicht verfügbar, wenn die Methode mit mehreren Verschlüsselungsmodulen verwendet wird.

Zugriff auf verschlüsselte Daten

Ein Verschlüsselungsmodul bestimmt den Zugriff auf verschlüsselte Daten. Security_admin-Benutzer können einem Benutzer eine Zugriffsrichtlinie für ein Verschlüsselungsmodul erteilen, indem sie dem Benutzer eine zugeordnete Rolle zuweisen.

Um die Zuweisung von Rollen zu überwachen, können der Kunde oder professionelle Services Sicherheitsmaßnahmen einrichten. Beispielsweise kann eine E-Mail an einen festgelegten Verschlüsselungsmanager gesendet werden, wenn einem Benutzer eine einem Verschlüsselungsmodul zugeordnete Rolle gewährt wird.

Hinweis:
Durch Identitätswechsel wird das für einen Benutzer verfügbare Verschlüsselungsmodul nicht geändert. Selbst während Sie die Identität von annehmen, stehen Ihnen ursprünglich nur die Verschlüsselungsmodule zur Verfügung. Diese Funktionalität wird in Vancouvereingeführt.

Zugriffsebene	Datenzugriff auf ein Feld mit der Methode eines einzelnen Verschlüsselungsmoduls	Datenzugriff auf ein Feld mithilfe der Methode mit mehreren Verschlüsselungsmodulen
Benutzer ohne Verschlüsselungsmodule	Das Formular blendet das verschlüsselte Feld aus. In der Listenansicht wird das Feld leer angezeigt und kann nicht bearbeitet werden, auch wenn die Daten im Feld entschlüsselt sind.	Das Formular blendet das verschlüsselte Feld aus. In der Listenansicht wird das Feld leer angezeigt und kann nicht bearbeitet werden, auch wenn die Daten im Feld entschlüsselt sind.
Benutzer mit einem Verschlüsselungsmodul	Um das Feld zu verwenden, muss der Benutzer Zugriff auf die Verschlüsselungsmodule haben, die in der Konfiguration des verschlüsselten Felds definiert sind. Wenn der Benutzer keinen	Der Benutzer verwendet automatisch seine Verschlüsselungsmodule mit dem verschlüsselten Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsebene	Datenzugriff auf ein Feld mit der Methode eines einzelnen Verschlüsselungsmoduls	Datenzugriff auf ein Feld mithilfe der Methode mit mehreren Verschlüsselungsmodulen
	Zugriff auf die Verschlüsselungsmodule hat, wird das Feld im Formular ausgeblendet. In der Listenansicht wird das Feld leer angezeigt und kann nicht bearbeitet werden. • Wenn das Feld keine Daten enthält: ○ Wenn der Benutzer Zugriff auf das Verschlüsselungsmodul hat, zeigt das Formular das Feld an (vorausgesetzt, die UI-Richtlinie verhindert dies nicht). ○ Benutzer mit Zugriff auf das Verschlüsselungsmodul können das leere Feld anzeigen und aktualisieren. ○ In das Feld eingegebene Daten werden mit dem Verschlüsselungsmodul verschlüsselt, das in der verschlüsselten Feldkonfiguration definiert ist. • Wenn sich Daten im Feld befinden: Wenn der Benutzer Zugriff auf das Verschlüsselungsmodul hat, kann der Benutzer Daten im Feld anzeigen und bearbeiten.	• Wenn das Feld keine Daten enthält: ○ Das Formular zeigt das Feld (vorausgesetzt, dies wird nicht durch eine UI-Richtlinie verhindert). ○ Benutzer mit einem beliebigen Verschlüsselungsmodul können das leere Feld anzeigen und aktualisieren. ○ Wenn Sie Daten in das Feld eingeben, verwendet das Feld das aktuell ausgewählte Verschlüsselungsmodul zum Verschlüsseln der Daten. • Wenn sich Daten im Feld befinden: Wenn der Benutzer Zugriff auf das Verschlüsselungsmodul hat, das zum Verschlüsseln des Felds verwendet wird, kann der Benutzer das Feld anzeigen und bearbeiten.
Benutzer mit zwei oder mehr Verschlüsselungsmodulen	Um das Feld zu verwenden, muss der Benutzer Zugriff auf das Verschlüsselungsmodul haben, das in der Konfiguration des verschlüsselten Felds definiert ist. Wenn der Benutzer keinen Zugriff auf das Verschlüsselungsmodul hat, wird das Feld im Formular ausgeblendet. In der Listenansicht wird das Feld leer angezeigt und kann nicht bearbeitet werden. • Wenn das Feld keine Daten enthält: ○ Wenn der Benutzer Zugriff auf das Verschlüsselungsmodul hat, zeigt das Formular das Feld an (vorausgesetzt, die UI-Richtlinie verhindert dies nicht). ○ Benutzer mit Zugriff auf das Verschlüsselungsmodul können das leere Feld anzeigen und aktualisieren.	Der Benutzer kann ein Verschlüsselungsmodul aus der Verschlüsselungsmodulauswahl in der Willkommensleiste auswählen. • Wenn das Feld keine Daten enthält: ○ Das Formular zeigt das Feld (vorausgesetzt, die UI-Richtlinie verhindert dies nicht). Benutzer mit einem beliebigen Verschlüsselungsmodul können das leere Feld anzeigen und aktualisieren. ○ Wenn Sie Daten in das Feld eingeben, verwendet das Feld das aktuell ausgewählte Verschlüsselungsmodul zum Verschlüsseln der Daten. ○ Das Feld verwendet immer das ursprüngliche Verschlüsselungsmodul,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsebene	Datenzugriff auf ein Feld mit der Methode eines einzelnen Verschlüsselungsmoduls	Datenzugriff auf ein Feld mithilfe der Methode mit mehreren Verschlüsselungsmodulen
	○ In das Feld eingegebene Daten werden mit dem Verschlüsselungsmodul verschlüsselt, das in der verschlüsselten Feldkonfiguration definiert ist. • Wenn sich Daten im Feld befinden: ○ Wenn der Benutzer Zugriff auf das Verschlüsselungsmodul hat, kann er das Feld anzeigen und bearbeiten. ○ Das Feld verwendet immer das ursprüngliche Verschlüsselungsmodul, um Änderungen am Feld zu verschlüsseln. Dieses Verhalten verhindert, dass Benutzer mit zwei oder mehr Verschlüsselungsmodulen das Verschlüsselungsmodul eines Felds ändern.	um Änderungen am Feld zu verschlüsseln. Dieses Verhalten verhindert, dass Benutzer mit zwei oder mehr Verschlüsselungsmodulen das Verschlüsselungsmodul eines Felds ändern. • Wenn sich Daten im Feld befinden: ○ Wenn der Benutzer Zugriff auf das Verschlüsselungsmodul hat, das zum Verschlüsseln des Felds verwendet wird, kann der Benutzer das Feld anzeigen und bearbeiten. ○ Das Feld verwendet das ursprüngliche Verschlüsselungsmodul, um Änderungen am Feld zu verschlüsseln. Dieses Verhalten verhindert, dass Benutzer mit mehreren Verschlüsselungsmodulen das Verschlüsselungsmodul eines Felds ändern.

Unterstützte Konfigurationsinformationen

- Die folgenden Feldtypen können verschlüsselt werden:
  - Anlagen
  - Datum
  - Datum/Uhrzeit
  - Zeichenfolgentext
  - URL

Hinweis:
In Enterprise sind weitere Feldtypen verfügbar. Details siehe Column Level Encryption Enterprise.

- Da Module an Rollen und Rollen an Benutzer gebunden sind, haben Sie keinen Zugriff auf Schlüssel aus Nicht-Benutzersitzungen. Alles, was als Systembenutzer oder als geplante Aufgabe ausgeführt wird und keine Benutzersitzung hat, kann nicht auf den Schlüssel zugreifen, um Daten zu verschlüsseln oder zu entschlüsseln.
- Sie können auf den „Wert“ oder den „Anzeigewert“ zugreifen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie „Wert“ auswählen, wird der Geheimtext zurückgegeben.
- Wenn Sie „Anzeigewert“ auswählen, wird Klartext zurückgegeben, sofern Sie über die richtige Rolle verfügen.

Viele Skripts in den Anwendungsebenen sind so geskriptet, dass sie diesen Unterschied ignorieren und den Wert verwenden. Wenn Sie die Skripts nicht ändern, um den Anzeigewert zu verwenden, werden die Daten nicht verschlüsselt oder entschlüsselt.

Anhangsverschlüsselung

Standardmäßige Anhangverschlüsselung

Bei Kunden, die die Verschlüsselung auf Spaltenebene verwenden, werden Anhänge in Tabellen mit dem aktiven EFC-Typ (Encrypted Field Configuration) `Attachment`standardmäßig verschlüsselt.

Diese durch die EFC-Konfiguration definierte Standardverschlüsselung bedeutet, dass Administratoren nicht manuell deklarieren müssen, dass ein Anhang beim Hochladen für diese Tabellen verschlüsselt werden soll.

Deaktivieren der Standardverschlüsselung

Wenn Sie nicht möchten, dass Anhänge basierend auf der EFC-Konfiguration standardmäßig verschlüsselt werden, können Sie diese Option deaktivieren, indem Sie sich an den Support wenden.

Um diese Funktion zu deaktivieren, erstellen Sie einen Support-Fall beim Support, und fügen Sie diese Anweisung in einen Kommentar zum Falldatensatz ein:

„Ich [Name des Kunden] verstehe, dass ich die empfohlene Best Practice für Sicherheit für Anhänge verlange und dass [das Unternehmen des Kunden] zusätzliche Risiken im Zusammenhang mit der Konfiguration und Verwendung unverschlüsselter Anhänge in der Anwendung übernimmt.“

Verschlüsselte Felder filtern und durchsuchen

Wenn ein verschlüsseltes Textfeld oder ein Feld mit einer verschlüsselten Feldkonfiguration als linker Operand in einem Filter ausgewählt wird, sind die folgenden Operatoren verfügbar:

- **ist**
- **ist nicht**
- **ist leer**
- **ist nicht leer**

Verwenden Sie für Datumsfelder die Datumsauswahl, um das Datum festzulegen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie für Felder vom Typ Datum/Uhrzeit die Datums- und Zeitauswahl, um das Datum und die Uhrzeit festzulegen:

Wenn ein Benutzer mit einem Verschlüsselungsmodul nach Gleichheit filtert oder nach einem Wert in einer Liste sucht:

- Es werden nur Werte zurückgegeben, die mit einem für den Benutzer verfügbaren Verschlüsselungsmodul verschlüsselt sind.
- Die Operatoren „ **ist leer"** und „ **ist nicht leer** " geben alle übereinstimmenden Datensätze zurück. Felder, die mit einem Verschlüsselungsmodul verschlüsselt sind, das dem aktuellen Benutzer nicht zur Verfügung steht, erscheinen leer.

Wenn ein Benutzer keine Verschlüsselungsmodule hat, werden keine Datensätze zurückgegeben.

Die Optionen **Übereinstimmungen anzeigen** und **Herausfiltern** werden in Listen unterstützt. Nur genaue Übereinstimmungen werden zurückgegeben oder herausgefiltert.

Hinweis:
Das Hinzufügen von verschlüsselten Feldern in Bedingungsfiltern wird in Skripts wie UI-Richtlinien und Business-Regeln unterstützt.

Daten aus verschlüsselten Feldern werden exportiert

Beim Exportieren verschlüsselter Felder in einer Liste oder einem Formular in ein Dateiformat werden im exportierten Dokument nur Felder angezeigt, die mit einem Verschlüsselungsmodul verschlüsselt wurden. Das verwendete Verschlüsselungsmodul muss für den aktuellen Benutzer verfügbar sein.

Um den Export verschlüsselter Daten aus einer Listenansicht zu deaktivieren, fügen Sie die Systemeigenschaft `glide.encryption.export_encrypted_data.allowed` hinzu, und legen Sie den Wert auf **false**fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselung für Systemtabellen

Die Verschlüsselung auf Spaltenebene unterstützt derzeit nicht die Verschlüsselung von Feldern und Anhängen von Systemtabellen (Tabellen, die mit **sys_**beginnen).

Verhindern Sie, dass Benutzer unverschlüsselte Dateien anhängen

Ändern Sie die Eigenschaft com.glide.encryption.enable_attachment_key_ui, um zu verhindern, dass Benutzer mit Zugriff auf einen Verschlüsselungsmodulschlüssel unverschlüsselte Anhänge anhängen.

Vorbereitungen

Erforderliche Rolle: security_admin

Führen Sie diese Schritte aus, müssen Sie auf die Rolle „security_admin“ hochstufen. Anweisungen finden Sie unter Auf eine privilegierte Rolle erhöhen

Standardmäßig können Benutzer, die Zugriff auf einen Verschlüsselungsmodulschlüssel haben, unverschlüsselte Anhänge hochladen. Verwenden Sie die Systemeigenschaft `com.glide.encryption.enable_attachment_key_ui`, um dieses Verhalten zu ändern.

Beim Anfügen sehen Ihre Benutzer eine UI-Auswahl für Datensätze, die eine verschlüsselte Feldkonfiguration mit mehreren Modulen aufweisen. Wenn diese Eigenschaft auf „false“ festgelegt ist, sehen Benutzer keine Option mehr, einen Anhang nicht zu verschlüsseln.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen und öffnen Sie in der Liste der Systemeigenschaften die Systemeigenschaft.
3. Legen Sie den **Wert** der Eigenschaft auf `false` fest.

Guided Tour zur Verschlüsselung auf Spaltenebene

Die Tour gibt einen kurzen Überblick über das CLE-Setup (Column Level Encryption), das zum Verschlüsseln von Tabellenfeldern oder Anhängen erforderlich ist. Schritte zum Erstellen von Feldverschlüsselungsmodulen, Modulzugriffsrichtlinien und verschlüsselten Feldkonfigurationen werden ebenfalls behandelt. Die Tour enthält Links zu einer detaillierten Dokumentation und zum ServiceNow University-Kurs „Verschlüsselung auf Spaltenebene – Übersicht“.

Vorbereitungen

Erforderliche Rolle: sn_kmf.crypto_manager oder security_admin

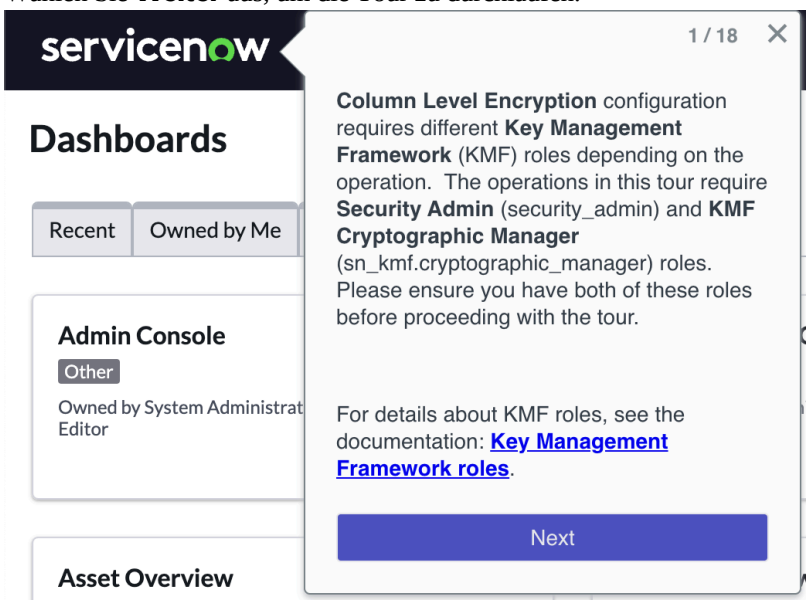
Hinweis:
Die Guided Tour ist noch nicht verfügbar, wenn Next Experience aktiviert ist.

Prozedur

1. Navigieren Sie in Ihrer Instanz zur UI-Seite **$pa_dashboards_overview.do**.
   Beispiel: `http://yourcompany.servicenow.com/nav_to.do?uri=%2F$pa_dashboards_overview.do`
   Ersetzen Sie`yourcompany` durch den Namen Ihrer Instanz.
2. Öffnen Sie das Symbol „Hilfe anzeigen“ (**Zeigt** das Symbol zum Umschalten der in der oberen linken Ecke an.
3. Wählen Sie am unteren Rand der Seitenleiste **Tour** starten aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Weiter** aus, um die Tour zu durchlaufen.



Column Level Encryption Enterprise

Verschlüsselung auf Spaltenebene Enterprise (CLE) verwendet Key Management Framework (KMF), damit Sie die Verschlüsselung und Entschlüsselung von Feldern und Anhängen in Ihrer Instanz vollständig anpassen und verwalten können. Für die Verwendung von Verschlüsselung auf Spaltenebene Enterpriseist ein -Abonnement erforderlich.

> **Wichtig:**
> Dieses Thema behandelt die Unternehmensversion von Column Level Encryption. Weitere Informationen zur Standardversion von CLE oder zu den Unterschieden zwischen den beiden Versionen finden Sie unter Verschlüsselung auf Spaltenebene.

Verschlüsselung auf Spaltenebene Enterprise basiert auf CLE (Column Level Encryption) und verwendet Key Management Framework und dessen vollständige Unterstützung für Schlüsselverwaltungsfunktionen. Verschlüsselung auf Spaltenebene Enterprise bietet Schlüsselschutz und Schlüssellebenszyklusverwaltung für die Feldverschlüsselung auf Anwendungsebene. Alle Schlüssel werden durch eine Key-Wrapping-Hierarchie geschützt, die letztendlich in FIPS 140-2-L3 Hardware Security Modules (HSM) verwurzelt ist.

Verschlüsselung auf Spaltenebene Enterprise gibt Ihnen die Möglichkeit zu verwalten, wie unterstützte Felder gemäß NIST 800-57- Praktiken verschlüsselt und entschlüsselt werden. Außerdem wird die aktuellste Version der Verschlüsselung auf Feldebene verwendet, einschließlich der Integration für ordnungsgemäßen Schlüsselschutz und ordnungsgemäße Verwaltung.

Insbesondere verwendet Verschlüsselung auf Spaltenebene Enterprise die Verschlüsselungsmodule KMF, wodurch Sie mehr Kontrolle über die serverseitige Verschlüsselung haben. KMF stellt mithilfe der Schlüsselhierarchie und der Umschlagverschlüsselung einen ordnungsgemäßen Schutz des Datenverschlüsselungsschlüssels sicher. Ihre Instanz verschlüsselt Daten durch kryptografische Module, die Sie konfigurieren. Sie können eine Zugriffsrichtlinie für jedes Modul erstellen, dann kryptografische Spezifikationen und Zugriffsrichtlinien konfigurieren und die Steuerung der Lebenszyklusverwaltung für Schlüssel steuern.

Verschlüsselung auf Spaltenebene Enterprise unterstützt Modulzugriffsrichtlinien basierend auf:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Umfang
- Rolle
- Skript
- Ressourcenaustausch
- Systemanwender

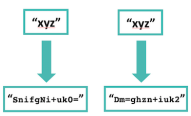
Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

Hinweis:
Weitere Informationen zu den unterstützten Funktionen von Verschlüsselung auf Spaltenebene und zum Aktualisieren und Abonnieren der Berechtigung [Verschlüsselung auf Spaltenebene Enterprise finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

Verschlüsselungsbegriffe

Begriff	Beschreibung
Schlüsselverwaltung	Unterstützung für Schlüsselverwaltung Von grundlegender Bedeutung für Verschlüsselung auf Spaltenebene Enterprise ist das Key Management Framework (KMF). Erhalten Sie die folgenden Fähigkeiten: • Schlüssel-Lebenszyklusverwaltung. • Schlüsselrotation. Details siehe Schlüssel rotieren. • Schlüsselschutz und Schlüsselgenerierung mit FIPS 140-2-L3 Hardware Security Modules (HSMs). • Trennung von Rollen und Aufgaben. • Die sichere Übertragung von Datenverschlüsselungsschlüsseln zwischen Instanzen, z. B. Produktions- und Nicht-Produktionsinstanzen. • Vom Kunden bereitgestellte Schlüssel (CSK) mit Schlüsselumschließung. • Nicht deterministische Verschlüsselung. • Massenverschlüsselung/-entschlüsselung. • Audit des Schlüsselzugriffs/-nutzung. Details siehe Key Management Framework verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Begriff	Beschreibung
Vom Kunden bereitgestellter Schlüssel 	Unterstützung für vom Kunden bereitgestellte Schlüssel Einer der größten Vorteile von Verschlüsselung auf Spaltenebene Enterprise besteht darin, dass Sie Ihre eigenen Schlüssel für die Verschlüsselung verwenden können. Administratoren haben die Möglichkeit, die von ServiceNow bereitgestellten Schlüssel oder Ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auf dem Now Platform®zu verwenden. Sie können auch den Schlüssellebenszyklus verwalten und entscheiden, wann die Schlüssel widerrufen, rotiert und deaktiviert werden sollen. Nachdem Sie vom Kunden bereitgestellte Schlüssel aktiviert und ein kryptografisches Modul erstellt haben, laden Sie ein Token und einen öffentlichen flüchtigen Schlüssel herunter. Sie verwenden das Token und den öffentlichen Schlüssel, um Ihren Schlüssel zu umschließen, und laden ihn dann in die Instanz hoch. Informationen zur Verwendung von vom Kunden bereitgestellten Schlüsseln finden Sie unter Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen und Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
Verschlüsselung auf Spaltenebene 	Unterstützung für Feldverschlüsselung und Anhangverschlüsselung Sowohl die Feldverschlüsselung als auch die Anhangverschlüsselung verwenden kryptografische Module und Zugriffsrichtlinien über verschlüsselte Feldkonfigurationen. Das Formular „Verschlüsselte Feldkonfiguration“ wird verwendet, um einen Verschlüsselungstyp für die *Spalten-* oder *Anhangverschlüsselung* auszuwählen. Weitere Informationen und unterstützte Feldtypen finden Sie unter Legen Sie verschlüsselte Feldkonfigurationen fest.
Nicht deterministische Verschlüsselung 	Unterstützung für nicht deterministische Verschlüsselung Verschlüsselung auf Spaltenebene Enterprise unterstützt die *nicht deterministische* Verschlüsselung für mehr Sicherheit. Wenn das System dieselben Daten mehr als einmal verschlüsselt, sind die Geheimtexte jedes Mal unterschiedlich. Nicht deterministische Verschlüsselung ist mit AES-Verschlüsselung mit Cipher Block Chaining (CBC) verfügbar. Sie können diese Funktion über die Option „Gleichstellungserhaltung“ in der Phase „Algorithmusdefinition“ der kryptografischen Spezifikation aktivieren. Erstellen Sie eine kryptografische Spezifikation für ein Krypto-Modul, definieren Sie einen Algorithmus für die Verschlüsselung, und generieren Sie den Schlüssel. Unter Erstellen Sie ein kryptografisches Modul erfahren Sie, wie Sie die für Verschlüsselungsvorgänge verwendeten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Begriff	Beschreibung
	Mechanismen definieren und wie Sie die nicht deterministische Verschlüsselung aktivieren.
Ressourcenaustausch	Ressourcenaustausch Verschlüsselung auf Spaltenebene Enterprise verschlüsselt Instanz zu Instanz auf sichere Weise mithilfe der kryptografischen APIs von KMF, um Vertraulichkeit, Integrität, Authentifizierung und Nicht-Zurückweisung zu gewährleisten. Ressourcenaustausch ist eine Funktion von KMF, mit der Sie Ressourcen zwischen Instanzen auf sichere Weise austauschen können. Details siehe Key Management Framework Ressourcenaustausch.

Hinweis:
Wenn Sie Verschlüsselung auf Spaltenebene Enterprisenicht aktivieren, können Sie CLE weiterhin verwenden. Module für die Verschlüsselung auf Spaltenebene erlauben und verweigern den Zugriff auf verschlüsselte Daten basierend auf der Benutzerrolle. Weitere Informationen finden Sie unter Verschlüsselung auf Spaltenebene.

Verschlüsselung auf Spaltenebene Enterprise unterstützt On-Premise-Kunden. Domänentrennung wird nicht unterstützt.

Unterstützung für zusätzliche Module und Modulzugriffsrichtlinien

Die Standardversion von Verschlüsselung auf Spaltenebene ist auf fünf Module und Modulzugriffsrichtlinien (MAP) beschränkt. Verschlüsselung auf Spaltenebene Enterprise unterstützt eine größere Anzahl von Modulen und MAPs.

Unterstützte Feldinformationen

Die folgenden Feldtypen können verschlüsselt werden:

- Anlagen
- Datum
- Datum/Uhrzeit
- E-Mail
- HTML
- Journal
- Journaleingabe
- Journalliste
- Telefon
- Zeichenfolgentext
- Übersetztes Feld
- Übersetzte HTML
- Übersetzter Text
- URL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anhangsverschlüsselung

Standardmäßige Anhangverschlüsselung

Bei Kunden, die die Verschlüsselung auf Spaltenebene verwenden, werden Anhänge in Tabellen mit dem aktiven EFC-Typ (Encrypted Field Configuration) `Attachment`standardmäßig verschlüsselt.

Diese durch die EFC-Konfiguration definierte Standardverschlüsselung bedeutet, dass Administratoren nicht manuell deklarieren müssen, dass ein Anhang beim Hochladen für diese Tabellen verschlüsselt werden soll.

Deaktivieren der Standardverschlüsselung

Wenn Sie nicht möchten, dass Anhänge basierend auf der EFC-Konfiguration standardmäßig verschlüsselt werden, können Sie diese Option deaktivieren, indem Sie sich an den ServiceNow -Support wenden.

Um diese Funktion zu deaktivieren, erstellen Sie einen Supportfall mit ServiceNow -Support, und fügen Sie diese Anweisung in einen Kommentar zum Falldatensatz ein:

„Ich [Name des Kunden] verstehe, dass ich ServiceNow bitte, eine empfohlene Best Practice für Sicherheit für Anhänge zu deaktivieren, und dass [Kundenunternehmen] zusätzliche Risiken im Zusammenhang mit der Konfiguration und Verwendung unverschlüsselter Anhänge in der Anwendung ServiceNow] übernimmt. “

API-Unterstützung

Verschlüsselung auf Spaltenebene Enterprise aktualisiert die APIs setDisplayValue() und setValue(), sodass sie verschlüsselte Daten für verschlüsselte Felder einfügen können. Außerdem können getDisplayValue() und getValue() Klartextwerte zurückgeben.

Das folgende Skript veranschaulicht diese API-Änderungen, wenn die Kurzbeschreibung des Incidents verschlüsselt wird:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Wenn Sie getValue() verwenden, um verschlüsselten Text abzurufen, gibt Ihr Skript den Geheimtext nicht mehr zurück. Ihr Skript gibt den Nur-Text zurück, vorausgesetzt, der Benutzer hat Zugriff auf das kryptografische Modul. Wenn der Benutzer keinen Zugriff auf das kryptografische Modul hat, gibt getValue() den Geheimtext zurück.

Aktivieren Sie Column Level Encryption Enterprise

Mit dem Abonnement von Verschlüsselung auf Spaltenebene Enterprisekann ein Administrator das Plugin „com.glide.now.platform.encryption“ aktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager kann die Aktivierung des Plugins für die Produktions- und Nicht-Produktionsinstanzen Ihrer Organisation veranlassen, in der Regel innerhalb weniger Tage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Durch die Aktivierung des Plugins Verschlüsselung auf Spaltenebene Enterprise (com.glide.now.platform.encryption) werden die folgenden Änderungen an Ihrer Instanz vorgenommen:

- Das Plugin „Encryption Support“ (com.glide.encryption) wird ebenfalls aktiviert.

  Hinweis:
  Das Plugin Key Management Framework (com.glide.kmf.global) ist standardmäßig bereits aktiv.

- Die Eigenschaft glide_encryption.set_value_support_cle.disabled ist auf **false**festgelegt, wodurch die Funktion SetValue aktiviert wird. Die SetValue-Unterstützung ermöglicht es den APIs setDisplayValue() und setValue(), verschlüsselte Daten zu unterstützen. Außerdem können getDisplayValue() und getValue() Klartextwerte zurückgeben.
- Zwei geplante Aufgaben sind aktiviert:
  - **autoKeyMigration**: Migriert Verschlüsselungskontextschlüssel zu kryptografischen Modulschlüsseln von Key Management Framework (KMF).
  - **autoDataMigration**: Migriert Daten, die Sie bereits verschlüsselt haben, zur Verwendung des kryptografischen Modulschlüssels KMF.

  Administratoren können ändern, wann diese regelmäßigen Aufgaben ausgeführt werden, und sie jederzeit anhalten oder neu starten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin *„Platform Encryption – com.glide.now.platform.encryption“*.
   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

   Hinweis:
   Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Migration zu Column Level Encryption Enterprise

Regelmäßige Aufgaben migrieren Ihre Schlüssel und verschlüsselten Daten vom Verschlüsselungssupport zu Verschlüsselung auf Spaltenebene Enterprise.

Sie können die geplanten Aufgaben überprüfen, indem Sie zu navigieren **Systemsicherheit** > **Strenge Sicherheitseinstellungen** > **Security-Aufträge**:

- **autoKeyMigration**: Migriert Verschlüsselungskontextschlüssel zu kryptografischen Modulschlüsseln von Key Management Framework (KMF).
- **autoDataMigration**: Migriert Daten, die Sie bereits verschlüsselt haben, zur Verwendung des kryptografischen Modulschlüssels KMF.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können ändern, wann diese regelmäßigen Aufgaben ausgeführt werden, und sie jederzeit anhalten oder neu starten.

Stellen Sie sicher, dass die verschlüsselten Feldkonfigurationen Ihre neu migrierten Modulschlüssel verwenden, indem Sie zu navigieren **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**. Suchen Sie nach den folgenden Elementen:

- Das Feld **Methode** ist **Einzelmodul**.
- Das Feld **Krypto-Modul** wird mit dem Namen des Kryptografiemoduls ausgefüllt, das das System automatisch erstellt. Sie können dieses Modul und die Modulzugriffsrichtlinie überprüfen, die beide aktiv und veröffentlicht sind.

Column Level Encryption Enterprise- und Systemklone

Wenn Verschlüsselung auf Spaltenebene Enterprise in Ihrer Instanz installiert ist, wird als Teil des Klonvorgangs automatisch ein neuer Verschlüsselungsschlüssel für das Feldverschlüsselungsmodul in der Zielklon-Instanz generiert. Diese Schlüssel werden für alle Module generiert, auf die der Benutzer Zugriff hat und die noch keinen Schlüssel haben.

Aus diesem Grund können in Feldverschlüsselungsmodulen in der Zielkloninstanz zwei Modulverschlüsselungsschlüssel vorhanden sein:

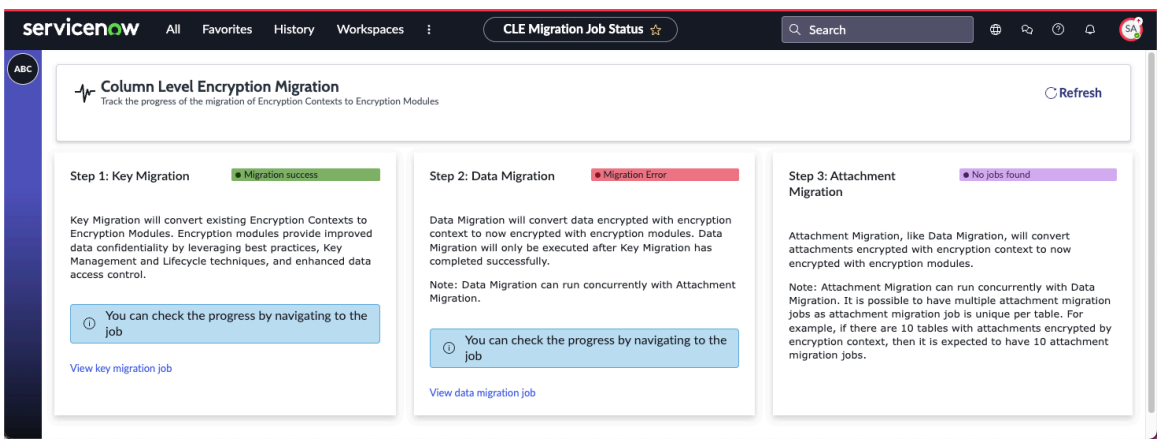
- Ein aktiver Modulverschlüsselungsschlüssel. Dies ist der neue Schlüssel, der nach dem Klonen generiert wird, solange der Benutzer auf das Modul zugreifen kann und keine vorherigen Schlüssel hat.
- Ein deaktivierter Verschlüsselungsmodulschlüssel (aus der automatisierten Schlüsselaustauschübertragung).

  Der aktive Modulverschlüsselungsschlüssel wird verwendet, um eingefügte Daten nach Bedarf in der Zielklon-Instanz zu verschlüsseln. Das deaktivierte Modul wird verwendet, um vorhandene Daten zu entschlüsseln, die als Teil des Systemklons geklont wurden.

  Um einen einzigen Schlüssel zum Entschlüsseln und Verschlüsseln aller Daten zu verwenden, können Sie einen Modul-Rekeying-Auftrag ausführen. Weitere Informationen zu Neuschlüsselungsaufträgen für Module finden Sie unter Massenverschlüsselungs-, entschlüsselungs- und Neuschlüsselungsaufträge planen.

Migrationsstatusseite der Verschlüsselung auf Spaltenebene

Verwenden Sie die Migrationsstatusseite, um die Migration von Verschlüsselungskontexten zu Verschlüsselungsmodulen nachzuverfolgen.



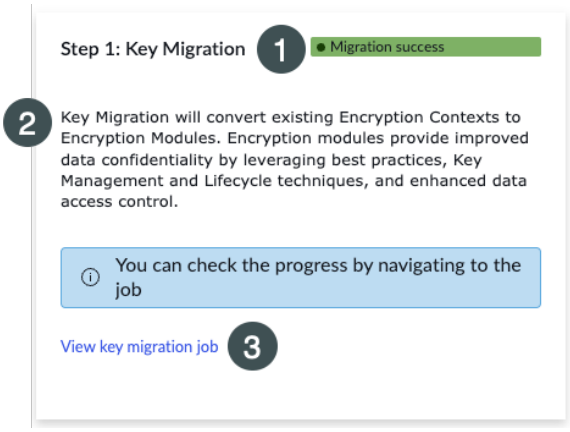
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Seite Verschlüsselung auf Spaltenebene Migration wird der Status der Schritte angezeigt, die an der Migration von Verschlüsselungskontexten zu Verschlüsselungsmodulen beteiligt sind. Jeder der drei Abschnitte zeigt den Status eines bestimmten Schritts im Prozess an.

Seitenabschnittskarten

Die Seite enthält drei Karten, die die Schritte des Migrationsfortschritts darstellen. Diese Karten werden angezeigt:

- (1) Der Status des aktuellen Schritts. Dieser Status zeigt an, ob der Schritt erfolgreich abgeschlossen wurde oder ob keine Aufträge zu verarbeiten sind.
- (2) Eine Beschreibung des aufgelisteten Schritts.
- (3) Ein Link zum entsprechenden Verschlüsselungsauftragsdatensatz [sys_mass_encryption_job].



Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene

Erstellen Sie ein Verschlüsselungsmodul auf Spaltenebene, um die für kryptografische Vorgänge verwendeten Mechanismen zu definieren.

Vorbereitungen

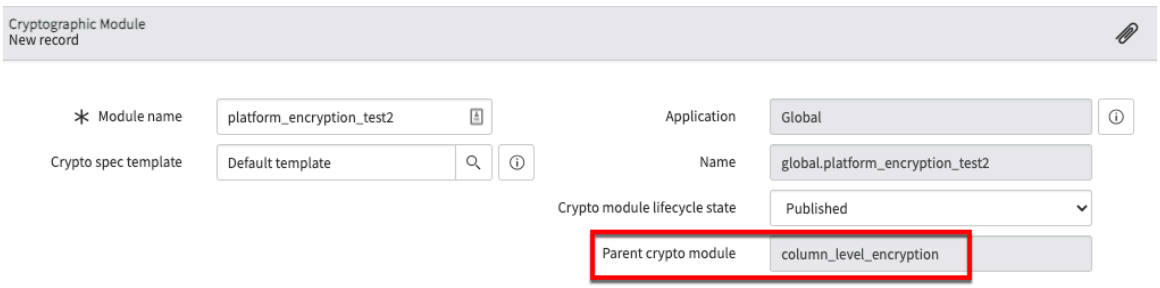
Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf_admin, security_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt Optionen, die mit Column Level Encryption (CLE) mit dem Basissystem verfügbar sind, und zusätzliche Konfigurationsoptionen, die mit der Funktionalität Verschlüsselung auf Spaltenebene Enterprise (CLE_Ent) verfügbar werden. Verschlüsselung auf Spaltenebene Enterprise ist mit einem kostenpflichtigen Abonnement verfügbar. Unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung finden Sie Informationen zu unterstützten Funktionen und Optionen, die mit jedem Angebot verfügbar sind. Weitere Informationen zum Abrufen von [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselungsmodule** > **Neu**.



2. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Kryptografisches Modul“

Feld	Beschreibung
Modulname	Alphanumerische Zeichenfolge, auf die beim Ausführen von Skripts verwiesen werden soll.
Krypto-Spezifikationsvorlage	Standardvorlage, die zum Erstellen des kryptografischen Moduls verwendet wird, das Zuordnungen vieler Kryptografiezwecke zu Kryptografiespezifikationen und empfohlenen Algorithmen enthält.
Anwendung	Der ausgewählte Anwendungsbereich.
Name	Der Name des Verschlüsselungsmoduls wird dem Namen des Anwendungsbereichs vorangestellt, um Konflikte mit anderen bereichsbezogenen Anwendungen bei der Modulerstellung zu vermeiden. Wenn Sie beispielsweise ein Modul mit dem Namen my_crypto_module im globalen Anwendungsbereich erstellt haben, wird der Name als global.my_crypto_module gespeichert.
Lebenszyklusstatus kryptografisches Modul	Der Begriff *Lebenszyklus* bezieht sich auf die Erstellung, Verwendung und Deaktivierung eines kryptografischen Moduls. Legen Sie während der Konfiguration anfänglich **Entwurf** fest. Wenn Sie das -Modul verwenden, setzen Sie auf **Veröffentlicht**. Die Vorlage Standard wird automatisch auf **Veröffentlicht**gesetzt.
Übergeordnetes kryptografisches Modul	Das übergeordnete Element wird automatisch als **column_level_encryption ausgefüllt**.

3. Klicken Sie auf **Absenden**.

Nach der erfolgreichen Übermittlung wird Ihr kryptografisches Modul in der Tabelle „Kryptografische Module“ aufgeführt.

⚠ Warnung:

Für Benutzer des Supports für veraltete Verschlüsselung:

Wenn Sie die Nicht-Enterprise-Version von Column Level Encryption verwenden, sind Sie auf fünf Module beschränkt. Wenn Sie dieses Limit überschritten haben, erhalten Sie die folgende Warnung:

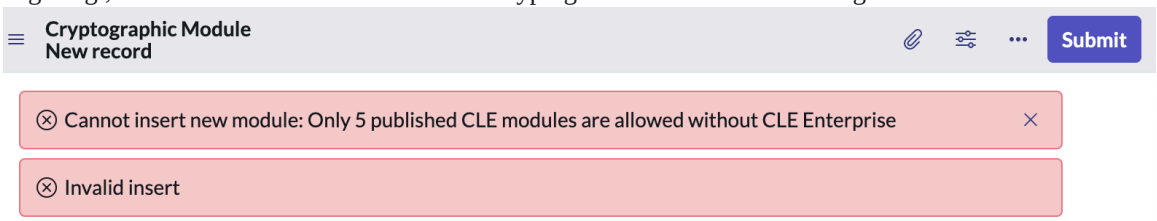
Diese Einfügung überschreitet die Anzahl der veröffentlichten Module, die für die Verschlüsselung auf Spaltenebene zulässig sind, mit dem Abonnementprodukt. Für zusätzliche Module ist das Enterprise-Abonnement für Verschlüsselung auf Spaltenebene erforderlich. Wenden Sie sich an Ihr Account-Team.

Eine kryptografische Standardspezifikation wird erstellt, wobei der Kryptografiezweck auf Symmetrische Datenverschlüsselung/-entschlüsselung und der Algorithmus auf AES 256 CBC festgelegt ist. Wählen Sie den Algorithmus für Updates aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Um die Konfigurationsoptionen zu öffnen, klicken Sie auf das neu erstellte kryptografische Modul.

Hinweis:
Vor dem Upgrade auf Verschlüsselung auf Spaltenebene Enterprisesind maximal fünf Verschlüsselungsmodule auf Spaltenebene zulässig. Eine Fehlermeldung wird angezeigt, und Sie können keine zusätzlichen kryptografischen Module hinzufügen.



Nächste Maßnahme
Erstellen Sie eine kryptografische Spezifikation für die Verschlüsselung auf Spaltenebene.

Verwendung mehrerer Verschlüsselungsmodule

Mehrere Verschlüsselungsmodule ermöglichen die Verschlüsselung von Daten mit mehr als einem Verschlüsselungsmodul. Wenn jedes Modul über eine eigene Zugriffsrichtlinie verfügt, die beispielsweise auf einer Rolle basiert, können Benutzer mit unterschiedlichen Rollen Daten in derselben Tabelle verschlüsseln, sie können jedoch weiterhin daran gehindert werden, die verschlüsselten Daten der anderen Benutzer anzuzeigen.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nur die Verschlüsselung in Spalten unterstützt mehrere Module. Die Anhangverschlüsselung funktioniert nicht. Massenverschlüsselung ist nicht verfügbar, wenn die Methode mit mehreren Verschlüsselungsmodulen verwendet wird.

Sie können ein Feld nicht mit mehreren Verschlüsselungsmodulen ändern, um ein einzelnes Verschlüsselungsmodul zu verwenden.

Das Feld wird vom Verschlüsselungsmodul des ersten Benutzers verschlüsselt, der Daten eingibt. Da das Verschlüsselungsmodul pro Datensatz festgelegt wird, können Felder in einer Liste unterschiedliche Verschlüsselungsmodule haben. Innerhalb eines einzelnen Datensatzes kann das Feld nur von einem Modul verschlüsselt werden.

Prozedur

1. Erstellen Sie mehrere kryptografische Module und jeweils eine Zugriffsrichtlinie.

   Stellen Sie sicher, dass Sie den verschiedenen kryptografischen Modulen über die Zugriffsrichtlinien unterschiedliche Rollen gewähren.

2. Navigieren zu **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**.

   Weitere Informationen zu verschlüsselten Feldkonfigurationen finden Sie unter Legen Sie verschlüsselte Feldkonfigurationen fest.

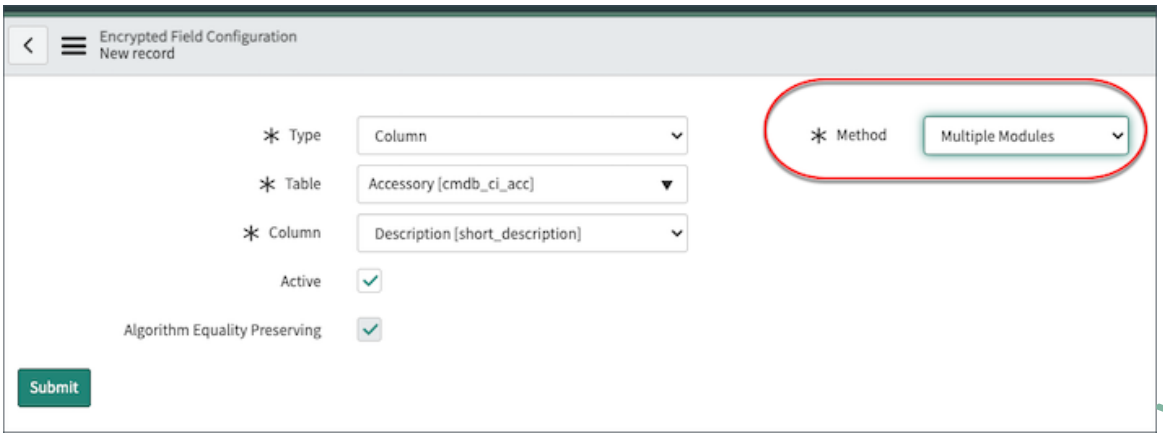
3. Wählen Sie im Feld **Typ** die Option **Spalte**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anhangverschlüsselung unterstützt nicht mehrere Module.

4. Wählen Sie **Mehrere Module** im Feld **Methode** aus.



5. Wählen Sie die **Tabelle** und die **Spalte** in der Tabelle aus, die Sie verschlüsseln möchten.
6. Klicken Sie auf **Absenden**.

Ergebnisse

Neu erstellte Daten für das angegebene Feld werden mit dem Schlüssel des entsprechenden Moduls verschlüsselt. Wenn ein Benutzer mit der in der Zugriffsrichtlinie von Modul A angegebenen Rolle in die angegebene Tabelle schreibt, werden die Daten mit dem Schlüssel von Modul A verschlüsselt. Nur Benutzer mit derselben Rolle können die Daten lesen.

Example:

So verschlüsseln Sie die Spalte „Kurzbeschreibung“ in der Incident-Tabelle. Sie würden Folgendes tun:

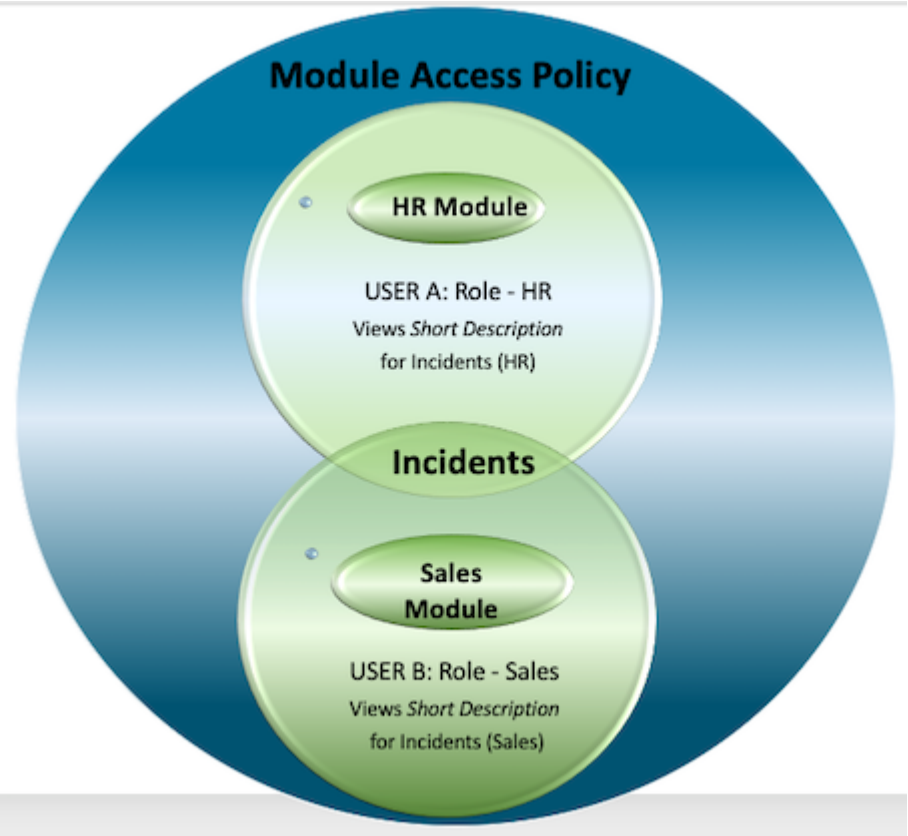
1. Erstellen Sie zwei kryptografische Module A und B.
2. Erstellen Sie für jedes Modul eine Modulzugriffsrichtlinie.

   Gewähren Sie für Modul A Benutzern mit einer HR-Rolle Zugriff. Gewähren Sie für Modul B Benutzern mit der Rolle „Vertrieb“ Zugriff.
3. Erstellen Sie einen Datensatz für die verschlüsselte Feldkonfiguration, indem Sie die Spalte Kurzbeschreibung in der Incident-Tabelle angeben, und stellen Sie sicher, dass Sie **Mehrere Module** im Feld **Methode** auswählen.
4. Lassen Sie zwei Benutzer, einen mit der HR-Rolle (Benutzer A) und einen mit der Vertriebsrolle (Benutzer B), einen Incident mit einer Kurzbeschreibung erstellen und dann beide Benutzer die Liste der Incidents anzeigen lassen.

   Die Kurzbeschreibung für den vom Benutzer mit der HR-Rolle erstellten Incident wird mit dem Schlüssel für Modul A verschlüsselt. Ebenso wird die Kurzbeschreibung für den vom Benutzer mit der Vertriebsrolle erstellten Incident mit dem Schlüssel für Modul B verschlüsselt.

   Obwohl alle Benutzer mit den HR- und Vertriebsrollen Zugriff auf Incidents haben, kann nur ein Benutzer mit der HR-Rolle die Kurzbeschreibung für die von Benutzer A mit der HR-Rolle erstellten Incidents entschlüsseln und anzeigen. Ebenso können nur Benutzer mit der Rolle „Vertrieb“ die Kurzbeschreibungen für die Incidents entschlüsseln und anzeigen, die von Benutzer B mit der Rolle „Vertrieb“ erstellt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erstellen Sie eine kryptografische Spezifikation für die Verschlüsselung auf Spaltenebene

Nachdem Sie ein kryptografisches Modul erstellt haben, greifen Sie auf die entsprechende kryptografische Spezifikation zu, um den Algorithmus zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf_admin und security_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt Optionen, die mit Column Level Encryption (CLE) mit dem Basissystem verfügbar sind, und zusätzliche Konfigurationsoptionen, die mit der Funktionalität Verschlüsselung auf Spaltenebene Enterprise (CLE_Ent) verfügbar werden. Die Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist mit einem kostenpflichtigen Abonnement verfügbar. Unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung finden Sie Informationen zu unterstützten Funktionen und Optionen, die mit jedem Angebot verfügbar sind. Weitere Informationen zum Abrufen von [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Eine kryptografische Spezifikation wird vom System erstellt, wenn Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene erstellen.

.

Prozedur

1. Navigieren zu **Systemsicherheit** > **Feldverschlüsselungsmodule** > **Alle**.
2. Wählen Sie das kryptografische Modul aus, um die Konfigurationsoptionen zu öffnen.
   Informationen zum kryptografischen Modul werden oben auf dem Bildschirm angezeigt. Eine Kryptospezifikation für symmetrische Datenverschlüsselung/-entschlüsselung wird automatisch mit einem AES 256 CBC-Algorithmus erstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie die Krypto-Spezifikation aus der Tabelle aus, um die Algorithmusdefinition zu öffnen. Informationen Verschlüsselung auf Spaltenebene Enterprise zu finden Sie unter Konfigurieren Sie erweiterte Algorithmen für Column Level Encryption Enterprise.
4. Klicken Sie auf **Weiter**, um auf den Schlüssellebenszyklus zuzugreifen.

Nächste Maßnahme

Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Weitere Informationen zum Abschließen der Lebenszyklusdefinition für den Schlüssel finden Sie unter Konfigurieren Sie wichtige Lebenszyklusstatus.
- Klicken Sie auf **Weiter**, um einen kryptografischen Schlüssel zu erstellen. Details zu diesem Vorgang finden Sie unter Generieren Sie einen kryptografischen Schlüssel ServiceNow ..

Konfigurieren Sie erweiterte Algorithmen für Column Level Encryption Enterprise

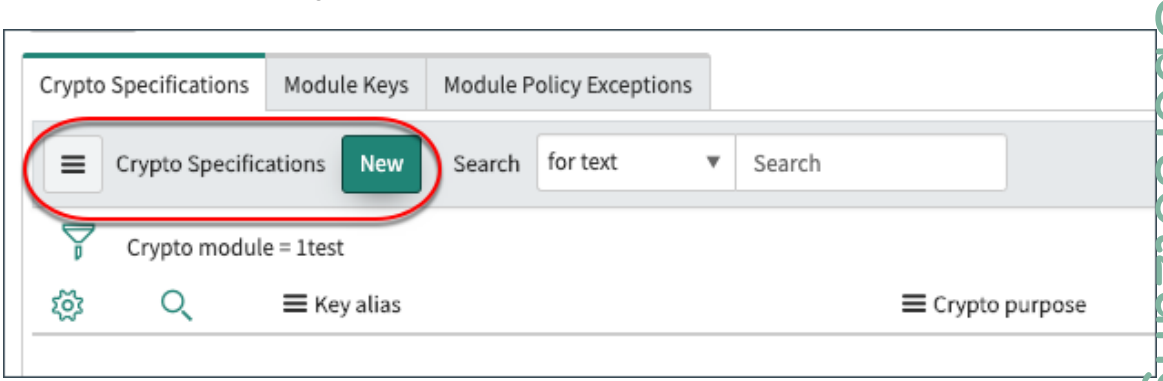
Erstellen Sie eine kryptografische Spezifikation, um den Algorithmus für ein kryptografisches Modul zu definieren. Passen Sie die Verschlüsselungsspezifikationen mit erweiterten Optionen an, die für Verschlüsselung auf Spaltenebene Enterpriseverfügbar sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Klicken Sie auf der Registerkarte **Krypto-Spezifikationen (#)** auf **Neu**.



2. Füllen Sie die Felder des Formulars aus.

Formular „Algorithmusdefinition“.

Feld	Beschreibung
Crypto-Modul	Name des ausgewählten kryptografischen Moduls ausgefüllt.
Kryptografischer Zweck	Der Wert ist **Symmetrische Datenverschlüsselung/-entschlüsselung** für Verschlüsselung auf Spaltenebene Enterprise.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

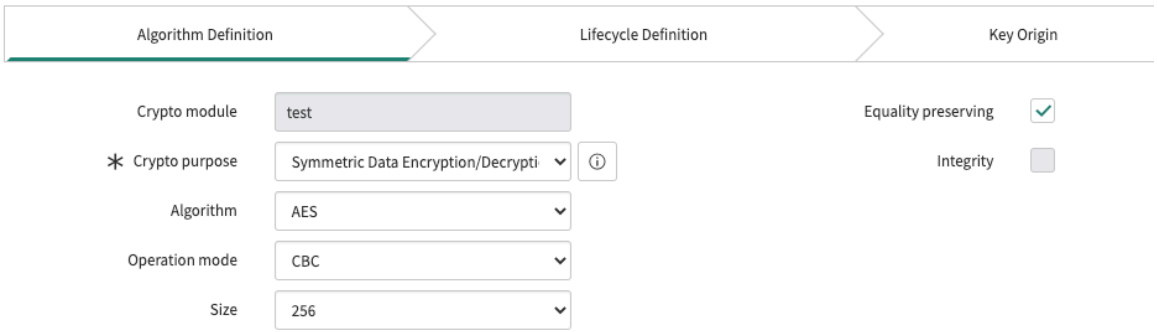
Feld	Beschreibung
Algorithmus	Der Wert ist **AES** für Verschlüsselung auf Spaltenebene Enterprise.
Betriebsmodus	Der Wert ist **CBC** für Verschlüsselung auf Spaltenebene Enterprise.
Größe	Mögliche Werte sind **256** und **128**. **Hinweis:** Eine Größe von 256 Bit ist für die Verschlüsselung am sichersten und wird für die symmetrische Datenverschlüsselung/ -entschlüsselung für Verschlüsselung auf Spaltenebene Enterpriseverwendet.
Gleichstellungserhaltung	Option zum Aktivieren der deterministischer Verschlüsselung. **Hinweis:** Wenn Sie diese Option auswählen, sollte der verschlüsselte Wert eines Felds derselbe sein, wenn der Feldwert gleich bleibt. Option zum Aktivieren der **symmetrischen Datenverschlüsselung/-entschlüsselung** mit **AES** im **CBC-Modus (Cipher Block Chaining)**.
Integrität	Option zur Bereitstellung von Integrität im GCM-Vorgang; gilt nicht für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise.

3. Klicken Sie auf **Absenden**.

Das folgende Beispiel zeigt die AES-CBC-256-Verschlüsselung. Wenn Verschlüsselung auf Spaltenebene Enterprise aktiv ist und das übergeordnete Modul column_level_encryption ist, gilt nur die symmetrische Datenverschlüsselung/-entschlüsselung AES CBC-256

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

als Verschlüsselungszweck. Details siehe Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.



Nächste Maßnahme
Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Weitere Informationen zum Abschließen der Lebenszyklusdefinition für den Schlüssel finden Sie unter Konfigurieren Sie wichtige Lebenszyklusstatus.
- Klicken Sie auf **Weiter**, um einen kryptografischen Schlüssel zu erstellen. Informationen zur Schlüsselgenerierung finden Sie unter einer der folgenden Aufgaben:
  - Generieren Sie einen kryptografischen Schlüssel ServiceNow ..
  - Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
  - Importieren Sie das Schlüsselpaar zum Packen/Entpacken.

Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel

Wenn das Plugin Verschlüsselung auf Spaltenebene Enterprise aktiviert ist, können Sie Systemeigenschaften verwenden, um die Tastenauffüllung, die Größe des flüchtigen Schlüsselpaars und einen Schlüsselgültigkeitszeitraum Ihrer vom Kunden bereitgestellten Schlüssel zu definieren.

Verschlüsselung auf Spaltenebene Enterprise Mit Key Management können Sie den gesamten Schlüssellebenszyklus Ihrer Datenverschlüsselungsschlüssel verwalten. Optional können Sie in Ihrer Umgebung generierte Datenverschlüsselungsschlüssel sicher austauschen.

Hinweis:
Die Eigenschaften in diesem Thema gelten nur für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise. Die Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist nur verfügbar, wenn das Plugin `„com.glide.now.platform.encryption“` aktiv ist. Weitere Informationen zum Abrufen von [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Nachdem der Datenverschlüsselungsschlüssel in die Instanz importiert wurde, schützt ein sicherer Schlüssel zum Umschließen neue Modulschlüssel in der Instanz. Der Wrapping-Schlüssel ist ein Instanzschlüssel-Verschlüsselungsschlüssel (IKEK), der von einem Hardware-Sicherheitsmodul (HSM) in SafeNet KeySecure generiert wird. Weitere Informationen zu Schlüsseltypen finden Sie unter Schlüssel auf Instanzebene im Key Management Framework.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Ihren eigenen Schlüssel angeben, müssen Sie ihn mit dem öffentlichen RSA-Schlüssel umschließen. Drei Eigenschaften definieren die Größe, den Füllalgorithmus und den Gültigkeitszeitraum des RSA-Schlüsselpaars mit Wrapping:

- `glide.kmf.ephemeral_key.key_padding` steuert das Tastenauffüllungsschema für den flüchtigen Schlüssel. Das Standardschema ist OAEP SHA256, aber SHA1 wird auch unterstützt.
- `glide.kmf.ephemeral_key.key_size` steuert die Schlüsselgröße des flüchtigen Schlüsselpaars. Der Standardwert ist 4096 Bit, aber 2048 Bit werden auch unterstützt.
- `glide.kmf.ephemeral_key.key_validity_period` definiert den Zeitraum, für den das flüchtige Schlüsselpaar gültig ist. Der Standardwert beträgt zwei Stunden.

Fahren Sie mit Umschließen Sie Ihren vom Kunden bereitgestellten Schlüsselfort.

Umschließen Sie Ihren vom Kunden bereitgestellten Schlüssel

Wenn Sie vom Kunden bereitgestellte Schlüssel verwenden, umschließen Sie den symmetrischen Schlüssel, der für die Verschlüsselung verwendet werden soll, mit dem heruntergeladenen öffentlichen Schlüssel.

Vorbereitungen

Hinweis:
Dieses Verfahren beschreibt Optionen, die mit dem KMF Basissystem verfügbar sind, und Optionen, die mit der Funktionalität Verschlüsselung auf Spaltenebene Enterprise verwendet werden sollen. Die Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist nur verfügbar, wenn das Plugin `„com.glide.now.platform.encryption“` aktiv ist. Weitere Informationen zum Abrufen von [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Einige der Schritte in diesem Dokument erfordern die Verwendung eines kryptografischen Tools, das auf Ihrem lokalen Gerät installiert ist. In den Beispielen in dieser Aufgabe wird das OpenSSL-Tool verwendet. Weitere Informationen zu diesem Tool finden Sie unter https://www.openssl.org . Wenn Sie andere kryptografische Tools wie LibreSSL oder GnuTLS verwenden, finden Sie in der Dokumentation für diese Produkte ähnliche Schritte.

- Ändern Sie optionale Eigenschaften, die die Größe, den Füllalgorithmus und den Gültigkeitszeitraum des Schlüssels steuern.
- Sie benötigen Ihren symmetrischen Schlüssel (.BIN) für die Verschlüsselung.
- Sie benötigen ein kryptografisches Tool, um Ihren Schlüssel zu umbrechen. In diesem Beispiel wird OpenSSL 1.1 verwendet.

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Key Management Framework** > **Kryptografische Module** > **Alle**.
2. Wählen Sie das kryptografische Modul, das Sie für den vom Kunden bereitgestellten Schlüssel erstellt haben, aus der zugehörigen Liste „Krypto-Spezifikationen“ aus.
3. Sie werden zum Schritt „ **Schlüsselerstellung** “ weitergeleitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn Sie den Schlüssel zum Packen noch nicht heruntergeladen haben, klicken Sie auf den Link, um *token_publickey* herunterzuladen<id> ZIP -Datei, und speichern Sie sie am selben Speicherort wie Ihren Schlüssel.

   Hinweis:
   Benennen Sie den heruntergeladenen *token_publickey* nicht um<id> Datei.

5. Entpacken Sie die Datei in Ihr lokales Netzwerk.
   Die ZIP-Datei enthält zwei Dateien, ein Importtoken und ein öffentliches PEM-Zertifikat. Umschließen Sie Ihren symmetrischen Schlüssel mit dem öffentlichen Schlüssel, um ihn zu verschlüsseln.
6. Kopieren Sie den Namen der Datei *token_publickey* in die Zwischenablage.
7. Verwenden Sie in einer Befehlszeile den kopierten Dateinamen *token_publickey*, um den Ordner der entpackten Dateien als Platzhalter für den umschlossenen Schlüssel zu öffnen.
8. Bearbeiten Sie dieses Skript, indem Sie die Beispiele durch die Namen Ihrer Krypto-Dateien ersetzen.

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
-in <keyname.bin>
-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt
 rsa_oaep_md:sha<128 or 256> "
```

   Überprüfen Sie die Schlüssel-Wrapping-Befehle in der folgenden Tabelle auf weitere Informationen.

Schlüssel-Wrapping-Befehle

Richtungen	Befehl	Beispiel
Öffnen Sie das Dateiverzeichnis, in das Sie das Wrapping-Token heruntergeladen haben.	`cd`	`cd token_publickey123456789`
Fügen Sie den Namen des publickey.PEM- Zertifikats ein.	`openssl pkeyutl -encrypt -pubin -inkey`	`publickey_586798643ffff.PEM`
Fügen Sie den Namen Ihres Schlüssels hier ein.	`-in`	`mykey.bin`
Geben Sie den Befehl <-out> ein, und geben Sie an, ob der Schlüssel 128 Bit oder 256 Bit ist.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	N/V

9. Führen Sie den Befehl aus.
   Eine Systemmeldung zeigt token_publickey_ an.<keynumber> . Der Schlüssel wird generiert und dem Verzeichnis eine *wrap_key_material* -Datei hinzugefügt.
10. Laden Sie den umschlossenen Schlüssel hoch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Kehren Sie zu Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch zurück, um Ihren umschlossenen Schlüssel hochzuladen.

Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch

Sie können Ihren eigenen vom Kunden bereitgestellten Schlüssel anstelle der vom System generierten Schlüssel von ServiceNow® verwenden.

Vorbereitungen

Erforderliche Rolle: security_admin, sn_kmf.cryptographic_manager

Wenn Sie keine eigenen Schlüssel angeben, müssen Sie dieses Verfahren nicht ausführen. Um ein kryptografisches Modul mit den Schlüsseln ServiceNow® zu erstellen, wechseln Sie zu Erstellen Sie ein kryptografisches Modul oder Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene.

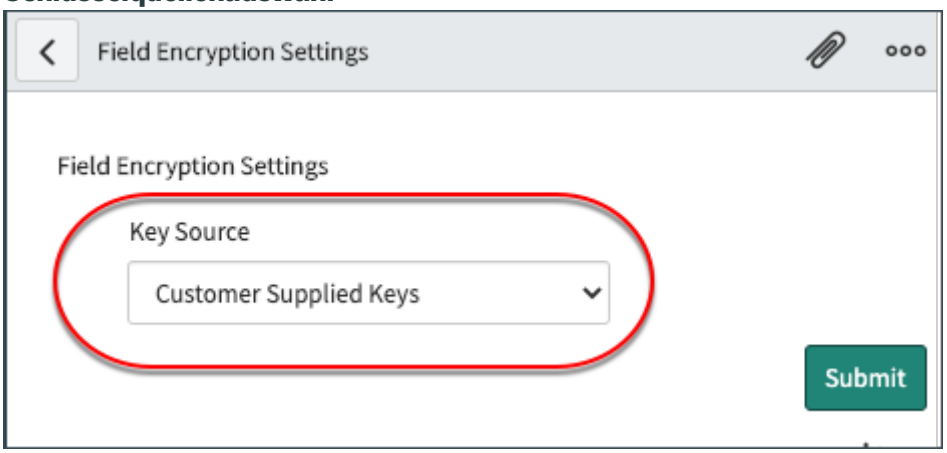
Hinweis:
Dieses Verfahren gilt nur für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise. Weitere Informationen finden Sie unter Aktivieren Sie Column Level Encryption Enterprise.

Wichtig:
Sie können einen vom Kunden bereitgestellten Schlüssel nicht widerrufen.

Prozedur

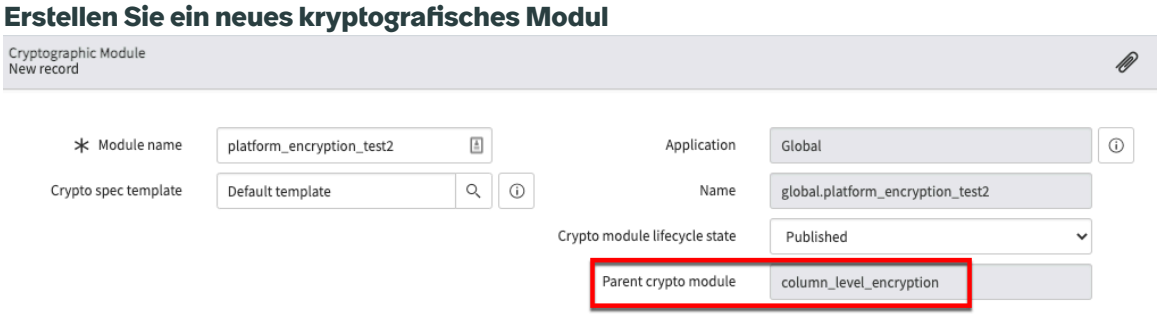
1. Navigieren zu **Alle** > **Systemsicherheit** > **Einstellungen für Feldverschlüsselung** und stellen Sie sicher, dass **Vom Kunden bereitgestellte Schlüssel** ausgewählt ist.

Schlüsselquellenauswahl



2. Wählen Sie **Absenden**.
3. Zurück zu **Systemsicherheit** > **Feldverschlüsselungsmodule** > > **Neu erstellen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie das Formular „Kryptografisches Modul“ wie folgt aus:

Felder des kryptografischen Moduls

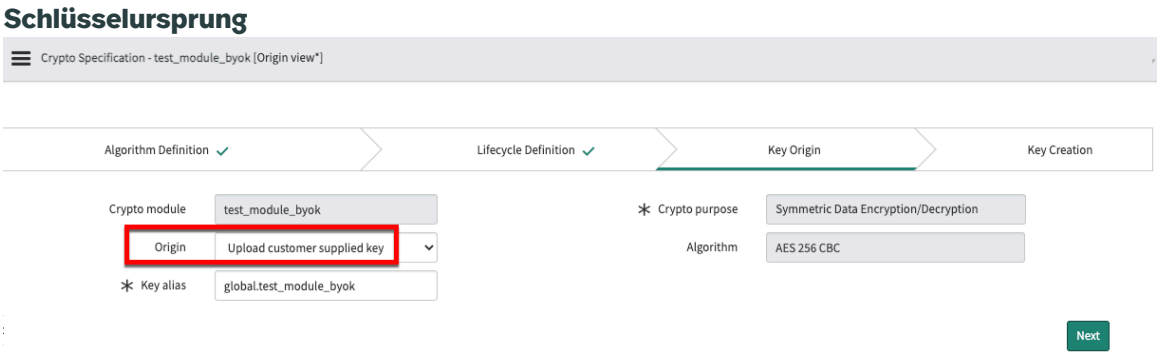
Feld	Beschreibung
Modulname	Geben Sie einen Namen für das Modul ein.
Krypto-Spezifikationsvorlage	Die kryptografische Standardvorlage ist ausgewählt.
Name	Wird basierend auf dem Modulnamen automatisch ausgefüllt und dem Namen wird der Bereich vorangestellt, um sicherzustellen, welche Anwendung angewendet wird. In diesem Fall wird der globale Bereich angewendet.
Lebenszyklusstatus kryptografisches Modul	Auswahlvorgang **Veröffentlicht** , um das Krypto-Modul zu aktivieren.
Übergeordnetes kryptografisches Modul	Das übergeordnete Modul **column_level_encryption** wird automatisch ausgewählt, wenn vom Kunden bereitgestellte Schlüssel und Verschlüsselungsmodule verwendet werden.

5. Wählen Sie **Absenden**.

6. Wählen Sie das neu erstellte kryptografische Modul aus der Tabelle aus.
Wählen Sie in der zugehörigen Liste **„Krypto-Spezifikationen** “ den automatisch generierten Schlüsselalias mit dem AES 256 CDB-Algorithmus aus.

Das System füllt den kryptografischen Zweck und den Algorithmus für CLE automatisch aus und springt zur Phase „ **Schlüsselursprung“**.

7. Beachten Sie, dass der vom **Upload-Kunden bereitgestellte Schlüssel** der **Ursprung** ist und der **Schlüsselalias** bereits ausgefüllt ist.



Automatische Übersetzung

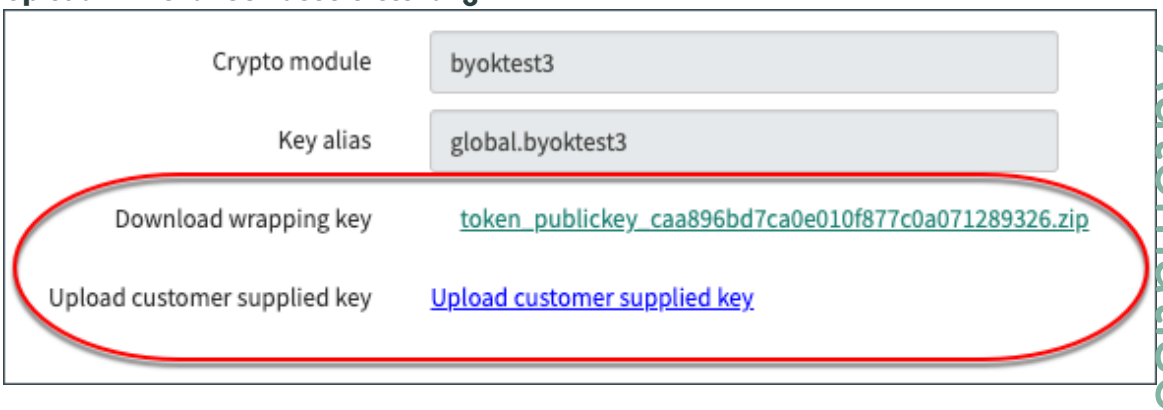
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie **Weiter** aus, um zur Phase **„Schlüsselerstellung“** zu wechseln.

   Es gibt zwei Links:

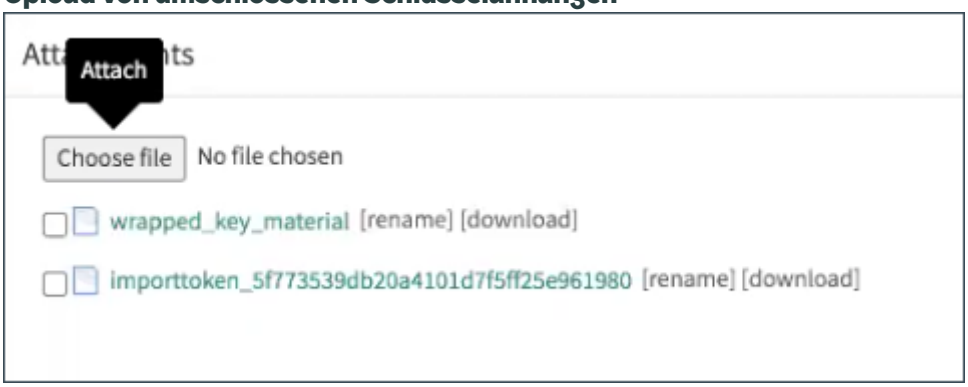
   - Schlüssel mit**Schlüssel** herunterladen lädt den Schlüssel in einer ZIP-Datei herunter, die ein Importtoken und ein Zertifikat für den öffentlichen Schlüssel (.PEM -Datei) enthält. Verwenden Sie das Importtoken, um das erfolgreiche Key Wrapping gemäß der Sicherheitsspezifikation für die Instanz zu überprüfen. Verwenden Sie die PEM -Datei des Zertifikats des öffentlichen Schlüssels, um den vom Kunden bereitgestellten Schlüssel sicher zu verpacken, bevor Sie ihn zusammen mit dem Token hochladen.
   - **Vom Kunden bereitgestellten Schlüssel hochladen** öffnet den Dateibrowser, um das Token und den verschlüsselten Schlüssel auszuwählen, den Sie umschlossen haben.

   Upload-Links für Schlüsselerstellung

9. Wählen Sie **Schlüssel zum Umschlüsseln herunterladen** aus, um das Token zu speichern.
   Speichern Sie das Token an demselben Zielspeicherort, an dem der Schlüssel in Ihrem System gespeichert ist. Benennen Sie das heruntergeladene Token nicht um.
10. Führen Sie den Befehl BYOK auf einem Terminal aus, um den Schlüssel zu umbrechen.
    Weitere Informationen finden Sie unter Umschließen Sie Ihren vom Kunden bereitgestellten Schlüssel.
11. Wählen Sie **„Vom Kunden bereitgestellten Schlüssel hochladen“ aus**.
12. Wählen Sie **Durchsuchen** aus, um die beiden Dateien auszuwählen, den umschlossenen Schlüssel und die Token-Datei.
    Im Fenster „Anhänge“ werden die beiden Dateien angezeigt.

    Upload von umschlossenen Schlüsselanhängen

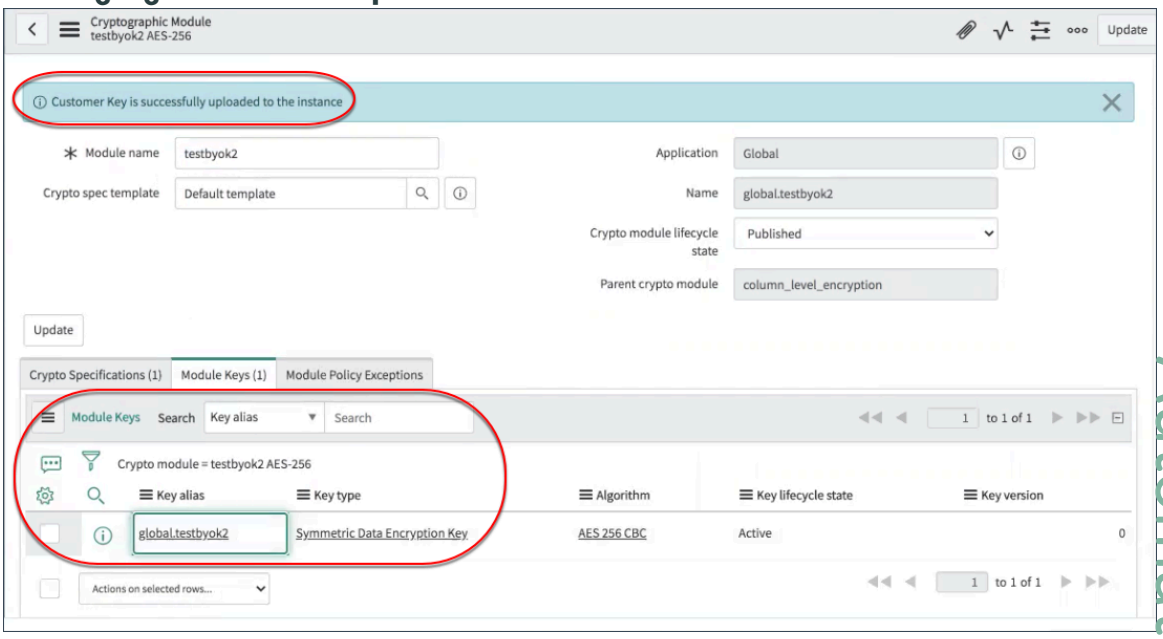
    Wählen Sie eine Datei aus, die entfernt werden soll, und laden Sie sie bei Bedarf erneut hoch.
13. Wählen Sie **OK**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie kehren zum Bildschirm „Kryptografisches Modul“ zurück. Bei einem erfolgreichen Upload des Kundenschlüssels wird eine Bestätigungsmeldung angezeigt. Der Schlüssel wird auch in der zugehörigen Liste „Modulschlüssel“ aufgeführt.

Bestätigung des Schlüssel-Uploads



Nächste Maßnahme

Nachdem Sie die Konfiguration Ihres kryptografischen Moduls mit dem vom Kunden bereitgestellten Schlüssel abgeschlossen haben, fahren Sie mit fort Erstellen Sie eine Modulzugriffsrichtlinie

Verschlüsseln von Feldern und Anhängen

Nachdem Sie Ihre kryptografischen Module erstellt haben, erstellen Sie verschlüsselte Feldkonfigurationen und geben an, ob ein Feld in einer Tabelle oder Anhänge verschlüsselt werden soll.

So verschlüsseln Sie Felder

Hinweis:
Verschlüsselte Felder werden nicht vom Design geprüft. Dieses Verhalten ist nicht konfigurierbar.

1. Geben Sie die Schlüsselquelle an: vom System generierte Schlüssel oder vom Kunden bereitgestellte Schlüssel (bringen Sie Ihren eigenen Schlüssel mit) in **Systemsicherheit** > **Einstellungen für Feldverschlüsselung**.
2. Nachdem Sie die Schlüsselquelle angegeben haben, erstellen Sie ein neues kryptografisches Modul, oder verwenden Sie ein vorhandenes kryptografisches Modul. Beginnen Sie mit Erstellen Sie ein kryptografisches Modul für Anweisungen.

Hinweis:
Wenn Sie vom Kunden bereitgestellte Schlüssel verwenden, befolgen Sie die Anweisungen in Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene und Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie eine verschlüsselte Feldkonfiguration, in der Sie die Tabelle angeben, für die die Verschlüsselung ausgeführt wird, und entweder die Spalte in der Tabelle oder die zu verschlüsselnden Anhänge in der Tabelle. Informationen zu den ersten Schritten finden Sie unter Legen Sie verschlüsselte Feldkonfigurationen fest.

Hinweis:
Unter Column Level Encryption Enterprise-Beispiele wird veranschaulicht, wie Felder und Anhänge mit vom Kunden bereitgestellten Schlüsseln verschlüsselt werden.

Legen Sie verschlüsselte Feldkonfigurationen fest

Konfigurieren Sie, welche Tabellenspalten oder Anhänge das System mit einem vorkonfigurierten Verschlüsselungsmodul verschlüsselt.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager und security_admin, oder Rolle zum Sicherheitsadministrator erhöhen.

Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie sicher, dass Sie sich im richtigen Anwendungsbereich befinden, damit Sie die Tabellen in diesem Bereich sehen können.

Nur Benutzer mit Zugriff auf das kryptografische Modul, das Sie in dieser verschlüsselten Feldkonfiguration angeben, können die Daten in der verschlüsselten Tabellenspalte lesen oder auf den Anhang zugreifen.

- Wenn ein Benutzer Schreibzugriff, aber keinen Lesezugriff hat, wird das Feld im Bearbeitungsmodus angezeigt, und die eingegebenen Daten werden als Sternchen angezeigt.
- Wenn ein Benutzer Lesezugriff, aber keinen Schreibzugriff hat, zeigt das Feld den schreibgeschützten Modus für entschlüsselte Daten an.
- Wenn ein Benutzer allen Zugriff hat, sind Lese-/Schreibfunktionen für das verschlüsselte Feld verfügbar.

Siehe Erstellen Sie ein kryptografisches Modul oder Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene, um zu beginnen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen** > **Neu**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus.

Feld	Beschreibung
Typ	**Spalte** zum Verschlüsseln einer Tabellenspalte oder Anhang zum Verschlüsseln aller **Anhänge** einer Tabelle. Typen der verschlüsselten Daten: ○ Zeichenfolgentext ○ Anlagen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Datum, Datum/Uhrzeit: **Hinweis:** Sie können Verschlüsselungsfeld-Konfigurationen zum Verschlüsseln der vorhandenen Datums- und Datums-/Uhrzeitfelder erstellen. Sie können eine neue Verschlüsselungskonfiguration nur einer übergeordneten Tabelle hinzufügen. Sie können eine neue Verschlüsselungskonfiguration nicht einer untergeordneten Tabelle hinzufügen. ○ URL ○ Verschlüsselung auf Spaltenebene Enterprise unterstützt auch die folgenden Feldtypen: ▪ HTML ▪ Journal ▪ Übersetzt
Tabelle	Tabelle, deren Felder oder Anhänge verschlüsselt werden sollen.
Spalte	Spalte (Feld), die verschlüsselt werden soll, wenn Sie „ **Spalte** “ als Typ ausgewählt haben.
Aktiv	Wählen Sie diese Option aus, um die Konfiguration als aktiv zu markieren. Deaktivieren, wenn die Konfiguration noch nicht verwendet wird.
Crypto-Modul	Das kryptografische Modul, für das die verschlüsselte Feldkonfiguration gilt.
Methode	Wählen Sie **Einzelnes Modul** aus, um die Feldkonfiguration für ein Modul festzulegen. Wählen Sie **Mehrere Module** für rollenbasierten Zugriff aus, der sich über mehr als ein kryptografisches Modul erstreckt. **Einzelnes Modul** Verwenden Sie diese Option, um alle Anhänge mit einem einzelnen Modul zu verschlüsseln. Ihre Benutzer benötigen Zugriff auf dieses Modul, andernfalls können sie keine Anhänge hochladen. **Mehrere Module** Verwenden Sie diese Option, damit Benutzer beim Hochladen von Anhängen ein Modul auswählen können. Benutzer mit Zugriff auf mindestens ein Modul können ein Modul für die Verschlüsselung auswählen. Benutzer ohne Modulzugriff können unverschlüsselte Anhänge hochladen.
Algorithmus Encrypted Preserving [schreibgeschützt]	Gibt an, ob das von Ihnen ausgewählte Krypto-Modul bereits für die Unterstützung nicht deterministischer Verschlüsselung konfiguriert ist. Dies bedeutet, dass die Verschlüsselung jedes Mal anders ist, wenn dieselben Daten mehr als einmal verschlüsselt werden.

4. Klicken Sie auf **Absenden**.

Skriptzugriff für kryptografische Module

Skripts können ausgeführt werden, um für kryptografische Zwecke auf eine kryptografische Modulrichtlinie zuzugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Key Management Frameworkkönnen Richtlinien auf Skripts basieren. Wenn eine Zugriffsrichtlinie für den Skriptzugriff ausgelöst wird, kann das Back-End-Skript die Modulrichtlinienaktionen aus dem Skript ausführen.

Kryptografische Module können einen oder mehrere Verschlüsselungszwecke unterstützen, z. B. asymmetrische Datenentschlüsselung und symmetrische Datenentschlüsselung. Jeder kryptografische Zweck erfordert die Generierung eines Verschlüsselungsschlüssels und einen definierten kryptografischen Zweck.

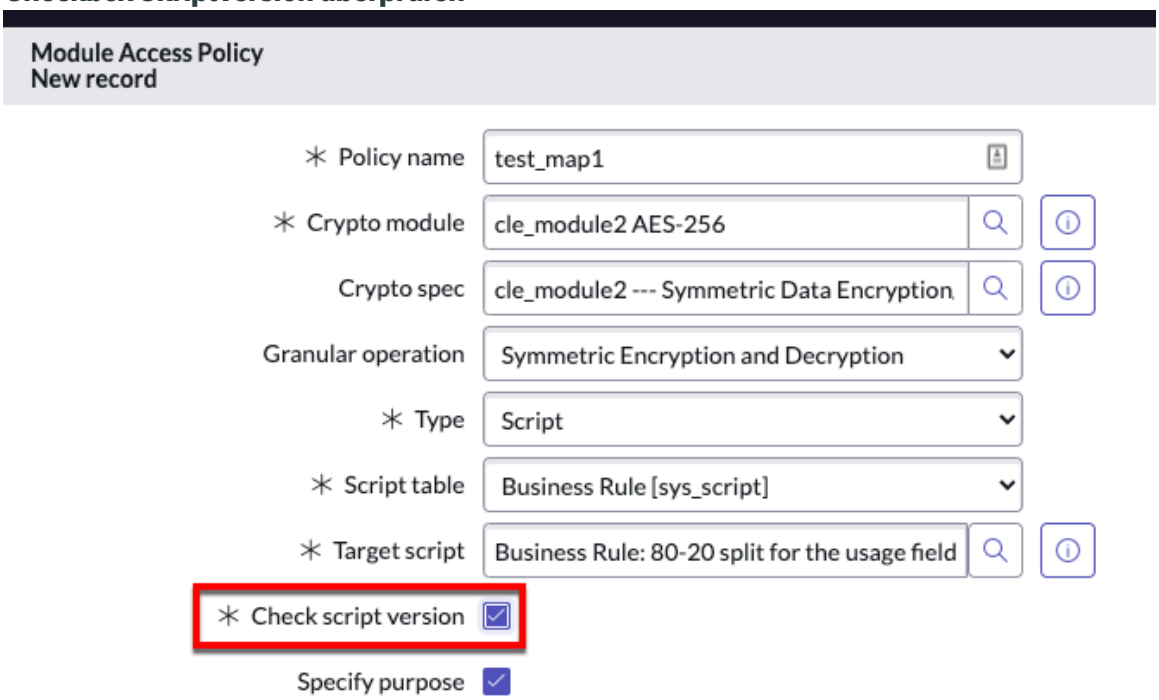
Berücksichtigen Sie Folgendes, wenn Sie eine Verschlüsselungsskriptanforderung ausführen:

- Der referenzierte kryptografische Zweck muss im kryptografischen Modul definiert werden.
- Für das kryptografische Modul muss ein aktiver generierter Schlüssel vorhanden sein.
- Der Typ der Modulzugriffsrichtlinie muss auf **Skript**festgelegt werden.

Skriptversion überprüfen

Beim Erstellen einer Modulzugriffsrichtlinie, die auf den Skripttyp festgelegt ist, ist eine Option zum Validieren der Integrität der Skriptversion verfügbar, auf die zugegriffen wird. Nur die zugewiesene Version des Skripts erhält Zugriff auf die Verschlüsselungsmodule. Wenn die **Checkbox Skriptversion** überprüfen in der Modulzugriffsrichtlinie aktiviert ist, führt das System jedes Mal, wenn das Skript ausgeführt wird, einen Versionsvergleich durch. Wenn das Skript geändert wurde, wird der Benutzer benachrichtigt.

Checkbox Skriptversion überprüfen



Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten

Führen Sie ein Skript aus, um die kryptografische Modulrichtlinie für einen kryptografischen Zweck auszuführen. Spezifischer Lese- (Entschlüsseln/Entpacken) oder Schreibzugriff (Verschlüsseln, Umbrechen) kann basierend auf der Granularität des Modulzugriffsrichtlinienvorgangs definiert werden.

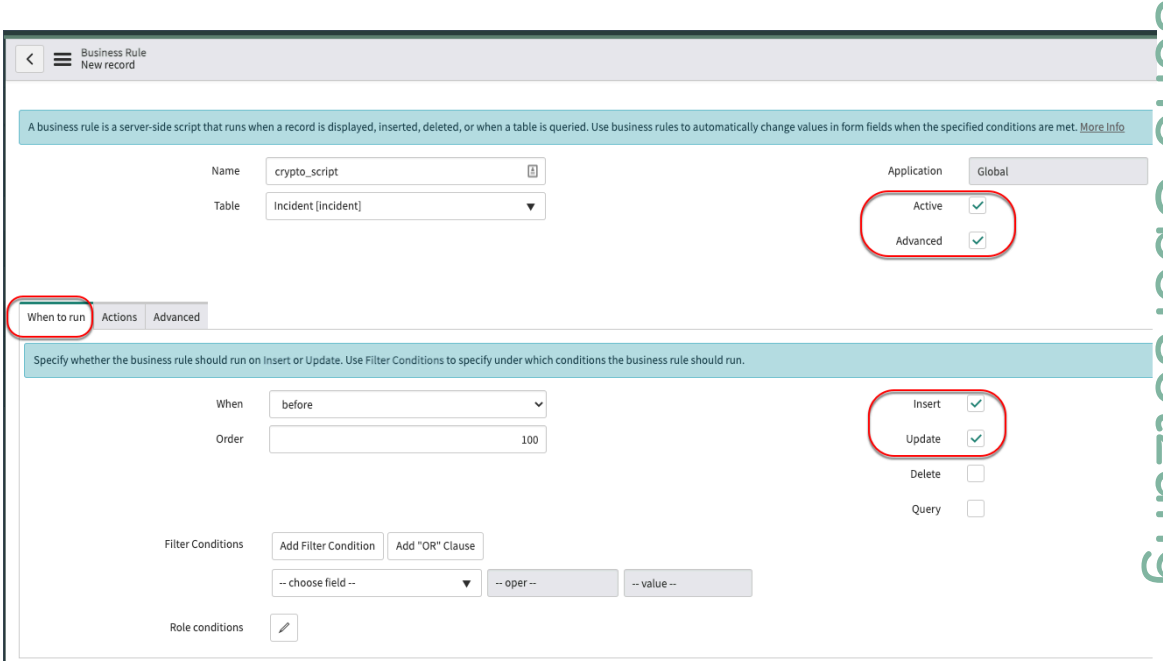
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird
Anwendungsbeispiele sind Business Rules und Skripteinbindungen. Dieses Verfahren verwendet ein Skript für Business Rules.

Prozedur
1. Erstellen Sie ein kryptografisches Modul mit dem symmetrischen Datenverschlüsselungs-/-entschlüsselungsalgorithmus.
   Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul. Der spezifische Zugriff auf die Daten oder den Anhang wird mit einer Modulzugriffsrichtlinie mit den folgenden Eigenschaften gesteuert:
   - Symmetrische Verschlüsselung: Das Skript kann Daten verschlüsseln, aber nicht entschlüsseln.
   - Symmetrische Entschlüsselung: Das Skript kann hochgeladene verschlüsselte Daten oder Anhänge entschlüsseln, aber keine Daten oder Anhänge verschlüsseln.
   - Symmetrische Verschlüsselung und Entschlüsselung: Das Skript kann Daten oder Anhänge sowohl verschlüsseln als auch entschlüsseln.
2. Navigieren zu **Systemdefinition** > **Business-Regeln**.
3. Klicken Sie auf **Neu**.



4. Füllen Sie das Formular auf der Registerkarte Zeitpunkt **für Ausführung aus,** und geben Sie das Skript auf der Registerkarte **Erweitert** ein:

Business Rule-Felder

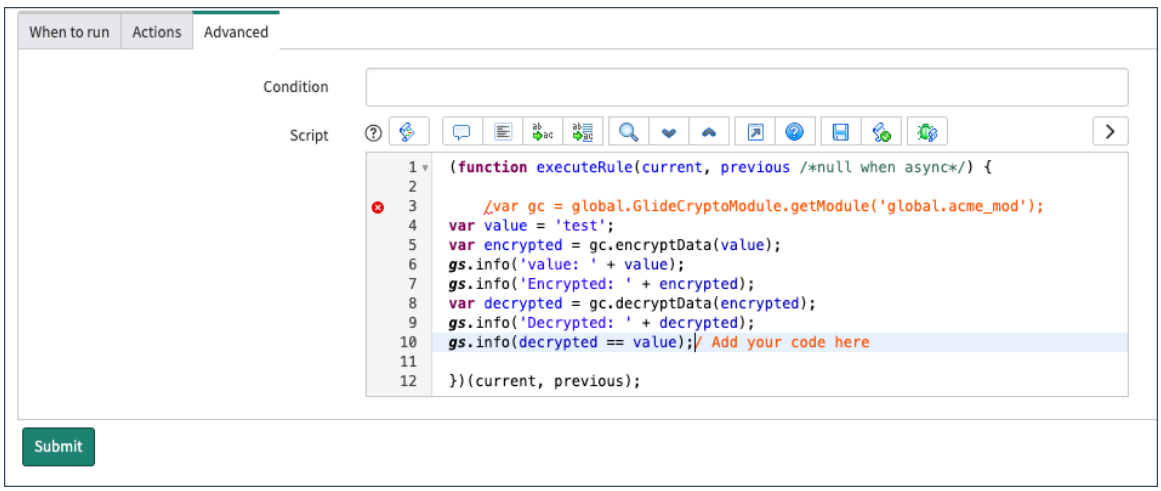
Feld	Beschreibung
Name	Geben Sie einen Namen für die Business Rule ein.
Tabelle	Wählen Sie **Incident [incident]**aus der Dropdown-Liste aus.
Anwendung	**Global** ist standardmäßig ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Markieren Sie die Regel als **Aktiv**.
Erweitert	Aktivieren Sie die Checkbox, um erweiterte Optionen anzuzeigen.
Registerkarte „Ausführungszeitpunkt“	Aktivieren Sie auf der Registerkarte Zeitpunkt **für Ausführung** die Felder **Einfügen** und **Aktualisieren**.

Registerkarte „Erweitert“	Fügen Sie auf der Registerkarte **Erweitert** den folgenden Skripttext in Zeile 3 ein:
	`//`
	`var gc =`
	` global.GlideCryptoModule.getModule('global.acme_mod');`
	`var value = 'test';`
	`var encrypted = gc.encryptData(value);`
	`gs.info('value: ' + value);`
	`gs.info('Encrypted: ' + encrypted);`
	`var decrypted = gc.decryptData(encrypted);`
	`gs.info('Decrypted: ' + decrypted);`
	`gs.info(decrypted == value);`
	Hinweis:
	Weitere Informationen finden Sie in der Abbildung „Business Rules Advanced-Registerkarte“.



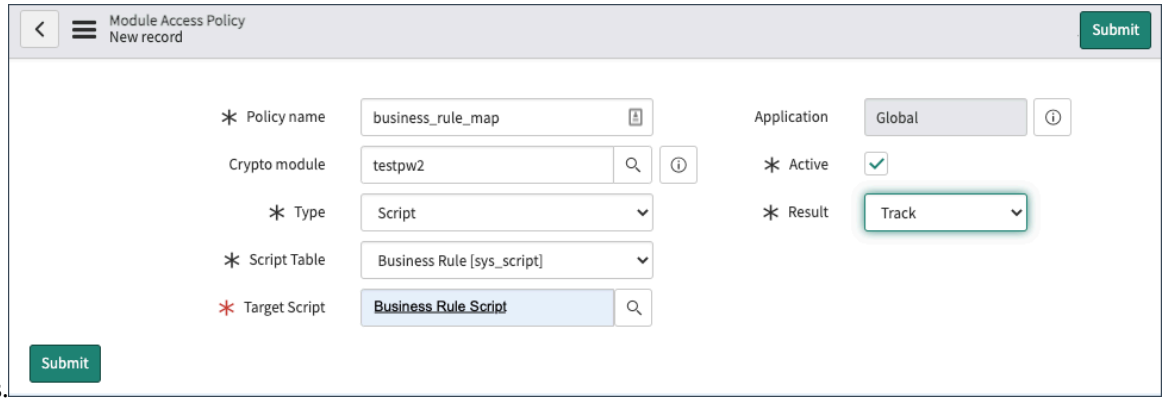
5. Klicken Sie auf **Absenden**.
6. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**.

Hinweis:
Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Füllen Sie das Formular aus.



Felder „Modulzugriffsrichtlinien“.

9. Klicken Sie auf **Absenden**.
Die Modulzugriffsrichtlinie für das Skript ist jetzt im System verfügbar.

Abgelehnte Nutzungsanforderungen für kryptografische Module anzeigen

Zeigen Sie kryptografische Module an, die Verschlüsselungsanforderungen von Skripts aufgrund nicht unterstützter Verschlüsselungsmechanismen abgelehnt haben.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

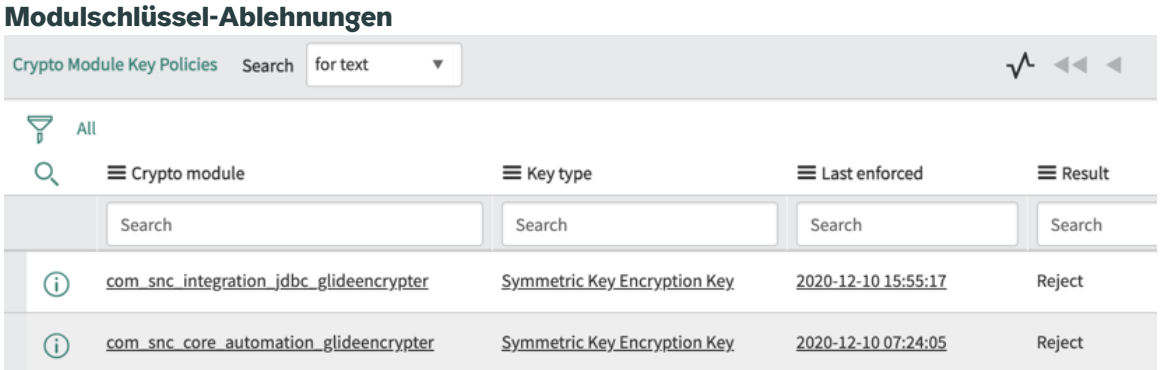
Kryptografische Module können einen oder mehrere Verschlüsselungszwecke unterstützen, z. B. asymmetrische Datenentschlüsselung und symmetrische Datenentschlüsselung. Auf verschlüsselte Daten kann nur basierend auf der Modulzugriffsrichtlinie zugegriffen werden. Wenn ein Skript versucht, ein kryptografisches Modul für einen Zweck zu verwenden, der nicht im Modul definiert ist, kann das Skript nicht auf die verschlüsselten Daten zugreifen.

Im folgenden Beispiel wurde einem kryptografischen Zweck ein kryptografischer Zweck zugewiesen, aber es wurde nie ein Schlüssel dafür generiert.

Prozedur

Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulschlüssel-Richtlinien** > **Modulschlüssel-Ablehnungen**.

Eine Liste der kryptografischen Module, die Anforderungen abgelehnt haben, wird zusammen mit dem im entsprechenden Skript verwendeten Verschlüsselungsschlüssel angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn ein anderes Skript versucht, dasselbe kryptografische Modul mit demselben Schlüsseltyp zu verwenden, wird der Wert für **Zuletzt erzwungen** aktualisiert. Eine weitere Zeile wird nicht generiert.

In diesem Beispiel hat das erste Modul am 2020-02-10_15:55:17 eine Anforderung abgelehnt, da der Schlüssel von Modul1 gefährdet ist. Am 2020-02-10_07:24:05 hat das zweite Modul eine Anforderung abgelehnt, da der Schlüssel des zweiten Moduls angehalten wurde.

Um Skripts die Berechtigung zur Verwendung des Verschlüsselungsmoduls bei der nächsten Ausführung zu erteilen, erstellen Sie eine Modulzugriffsrichtlinie für die Skriptverschlüsselung. Weitere Informationen finden Sie unter Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten.

Planen Sie Massenverschlüsselungs-, entschlüsselungs- und rekeying-Aufträge

Planen Sie Verschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge zu einem Zeitpunkt, der für Ihre Instanz am besten geeignet ist.

Vorbereitungen
Verschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge können zeit- und ressourcenintensiv sein. Planen Sie sie daher außerhalb der Spitzenzeiten ein. Stellen Sie außerdem sicher, dass der Benutzer, der die Aufgabe plant, über den entsprechenden Zugriff für jede Aufgabe verfügt.

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird
Massenverschlüsselung und -entschlüsselung ist auch im Formular „Verschlüsselte Feldkonfigurationen“ verfügbar. Siehe Massenverschlüsselung oder -entschlüsselung ausführen für Anweisungen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Strenge Sicherheitseinstellungen** > **Security-Aufträge**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Planungsformular aus.

Feld	Beschreibung
Name	Name des Verschlüsselungs-, Entschlüsselungs- oder Neuschlüsselungsauftrags.
Typ	Auftragstyp: ○ **Key Migration Context to Module (Schlüsselmigrationskontext zu Modul):** Massenmigration von Verschlüsselungskontextschlüsseln zu Verschlüsselungsmodulen, einschließlich der Erstellung von Datensätzen für Modulzugriffsrichtlinien für Zugriffssteuerungen für die Verschlüsselungsmodule ○ Datenmigrationskontext**zu Modul**: Migriert Daten, die durch Verschlüsselungskontexte verschlüsselt sind, in Verschlüsselungsmodule ○ Massenentschlüsselung von**Anhängen**: Entschlüsselt alle verschlüsselten Anhänge in Datensätzen für eine einzelne Tabelle, die Sie im Feld **Tabelle** definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Massenverschlüsselungsanhang**: Verschlüsselt alle Anhänge in Datensätzen für eine einzelne Tabelle, die Sie im Feld **Tabelle** definieren. ○ **Massenverschlüsselungsmodul**: Verschlüsselt alle bereits vorhandenen Werte in der definierten Spalte/dem definierten Feld, das in der Feldverschlüsselungskonfiguration verwendet wird ○ **Massenentschlüsselungsmodul**: Entschlüsselt alle bereits vorhandenen Werte in der definierten Spalte/dem definierten Feld, das in der Feldverschlüsselungskonfiguration mit Einzelmodul verwendet wird. ○ Massenentschlüsselung mit mehreren Modulen:**Entschlüsselt**alle bereits vorhandenen Werte in der definierten Spalte/dem definierten Feld, das in der Feldverschlüsselungskonfiguration mit mehreren Modulen verwendet wird. ○ **Modul-Neuschlüsselung**: Verschlüsselt alle bereits vorhandenen Werte in der definierten Spalte/dem definierten Feld, das in der Feldverschlüsselungskonfiguration verwendet wird, mit dem aktuell aktiven Schlüssel für das Modul erneut. ○ **Anhangskontext zu Modul**migrieren: Verschlüsselt alle bereits vorhandenen Anhänge in der Tabelle, die in der Feldverschlüsselungskonfiguration definiert ist. Jeder Anhang, der zuvor mit einem Kontext verschlüsselt wurde, wird mit dem Modul erneut verschlüsselt.
Status	Der Anfangsstatus des Auftrags ist „Neu“. Nachdem die Aufgabe wie geplant ausgeführt wurde, wird der Status entsprechend aktualisiert.
Zeitfensterstart	Startzeit für die Aufgabe im 24-Stunden-Format.
Zeitfensterende	Endzeit für die Aufgabe im 24-Stunden-Format.
Tabelle	Tabelle, die verschlüsselt oder entschlüsselt werden soll.
Feld	Feld, das verschlüsselt oder entschlüsselt werden soll.
Zusammenfassung	Auftragsstatusinformationen, wenn der Auftrag ausgeführt wird, abgeschlossen ist oder Fehler aufweist.

Hinweis:
Aufgrund des System-Overheads sollten Sie Massenverschlüsselungs-, entschlüsselungs- und rekeying-Aufträge so planen, dass sie außerhalb der Spitzenzeiten ausgeführt werden. Now Platform führt die Aufgabe zwischen dem **Start des Zeitfensters** und dem **Ende**des Zeitfensters aus. Wenn die Aufgabe in einem Verarbeitungsfenster nicht abgeschlossen ist, wird sie während des nächsten angegebenen Verarbeitungsfensters fortgesetzt, bis die gesamte Verarbeitung abgeschlossen ist.

4. Klicken Sie auf **Absenden**.
5. Nachdem Sie eine Aufgabe geplant haben, können Sie Folgendes tun.
   - **Klicken** Sie auf Auftrag abbrechen, um einen laufenden Auftrag abzubrechen.
   - Klicken Sie auf **Starten**, um eine Aufgabe sofort zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf **Aktualisieren**, um alle Änderungen zu speichern, die Sie am Aufgabenzeitplan vorgenommen haben.
- Klicken Sie auf **Löschen**, um die geplante Aufgabe zu löschen.

Massenverschlüsselung oder -entschlüsselung ausführen

Sie können die Massenverschlüsselung für Verschlüsselungskonfigurationen sowie eine Massenentschlüsselung ausführen, um zuvor verschlüsselte Werte zu entschlüsseln.

Vorbereitungen
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch regelmäßige Aufgaben für die Massenverschlüsselung und -entschlüsselung erstellen. Siehe Planen Sie Massenverschlüsselungs-, entschlüsselungs- und rekeying-Aufträge für Anweisungen.

Massenverschlüsselung und -entschlüsselung sind nur verfügbar, wenn eine verschlüsselte Feldkonfiguration das einzelne kryptografische Modul verwendet. Massenentschlüsselung ist sowohl für die Einzel- als auch für Mehrfachverschlüsselungsmethode verfügbar,.

Hinweis:
Massenverschlüsselung und -entschlüsselung sollten Sie nur außerhalb der Spitzenzeiten ausführen, da die Vorgänge ressourcen- und zeitintensiv sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**.
2. Öffnen Sie die verschlüsselte Feldkonfiguration für das Feld, das Sie massenverschlüsseln oder entschlüsseln möchten.
3. Wählen Sie unter Zugehörige Links eine verfügbare Option aus.
   - **Planen Sie den Massenentschlüsselungsauftrag**
   - **Planen Sie den Massenverschlüsselungsauftrag**
4. Bestätigen Sie Ihre Auswahl im Dialogfeld.

Ergebnisse
Wenn eine Massenverschlüsselung ausgeführt wird, werden alle Werte mit dem Verschlüsselungsmodul verschlüsselt, das im Datensatz der verschlüsselten Feldkonfiguration definiert ist. Wenn Sie eine Massenentschlüsselung ausführen, werden nur Felder entschlüsselt, die mit einem Verschlüsselungsmodul verschlüsselt sind, auf das Sie Zugriff haben.

Column Level Encryption Enterprise-Beispiele

Diese Beispiele führen Sie durch die Verschlüsselung von Feldern und Anhängen mit vom Kunden bereitgestellten Schlüssel.

Walkthrough zur Feldverschlüsselung

Diese Tour zeigt, wie Sie ein Feld in Ihrer Instanz mit Verschlüsselung auf Spaltenebene Enterprise mit Key Management Framework (KMF) verschlüsseln. Außerdem wird gezeigt, wie Sie Ihren eigenen Schlüssel verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis:
Dieses Verfahren gilt nur für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise. Weitere Informationen zum Abrufen von [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Erforderliche Rolle: admin oder security_admin

Hinweis:
security_admin ist eine privilegierte Rolle. Weitere Informationen zur Verwendung von privilegierten Rollen finden Sie unter Zu einer privilegierten Rolle erweitern

Warum und wann dieser Vorgang ausgeführt wird

Diese Tour beginnt mit einer Instanz, in der Sie bereits Ihren persönlichen kryptografischen Schlüssel erstellt und hochgeladen haben. Sie können den Schlüssel ServiceNow verwenden, in diesem Beispiel wird jedoch ein vom Kunden bereitgestellter Schlüssel verwendet.

Nachdem der Schlüssel in einem kryptografischen Modul gespeichert wurde, können Sie mit der Konfiguration von Feldern in Ihrer Instanz beginnen, z. B. Gehalt oder Sozialversicherungsnummern, auf die bestimmte Benutzer nur eingeschränkten Zugriff haben. Geben Sie in der verschlüsselten Feldkonfiguration an, welche autorisierten Mitarbeiter auf vertrauliche Daten zugreifen können.

Diese Aufgabe veranschaulicht zwei Szenarien. Ein Beispiel ist das Verschlüsseln des Felds **Kurzbeschreibung** in einem Incident für Benutzer, die nicht berechtigt sind, die vertraulichen Daten anzuzeigen.

Anhänge können auch verschlüsselt und nur für Benutzer sichtbar sein, denen Zugriff gewährt wird, oder für alle Benutzer sichtbar sein, die nicht auf die Anzeige der Daten beschränkt sind. Informationen zum Verschlüsseln eines Anhangs finden Sie unter Vorstellung der Anhangverschlüsselung.

Prozedur

1. Stellen Sie sicher, dass Verschlüsselung auf Spaltenebene Enterprise aktiviert ist.
2. Erstellen Sie ein kryptografisches Modul für column_level_encryption.
   Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene Erstellen Sie ein kryptografisches Modul.
3. Navigieren zu **Systemsicherheit** > **Verschlüsselungsfeld-Konfigurationen**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder des Formulars aus.

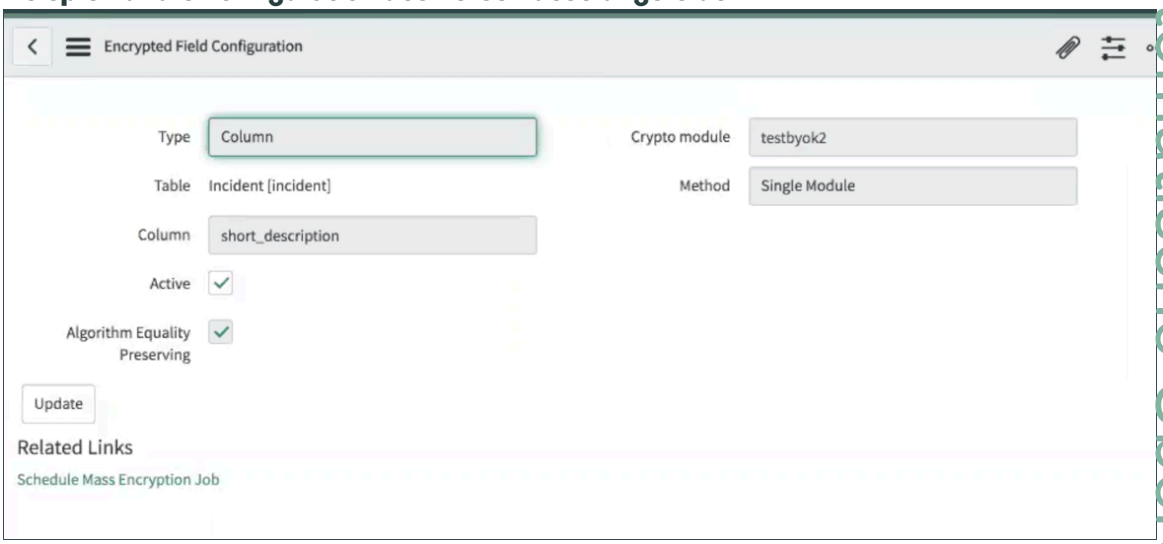
Verschlüsseltes Feldkonfigurationsformular

Feld	Beschreibung
Typ	**Spalte** ist erforderlich, um Ihren persönlichen Schlüssel zu verwenden.
Tabelle	Tabelle, in der die vertraulichen Informationen gespeichert werden Wählen Sie für dieses Beispiel **Incident [incident]**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Spalte	Spalte oder bestimmte Informationen, die das zu verschlüsselnde vertrauliche Datum darstellen. Wählen Sie für dieses Beispiel **short_description aus**.
Aktiv	Option zum Markieren von **Aktiv**, um die Feldkonfiguration zu verwenden.
Algorithmus-Gleichstellungserhaltung	Die Option ist automatisch ausgewählt.
Crypto-Modul	Modul, das Sie zur Verwendung mit dem persönlichen Schlüssel erstellt haben.
Methode	Die Option **Einzelnes Modul** wird verwendet, um die Richtlinien für ein Modul anzuwenden. **Mehrere Module** werden verwendet, um die Richtlinien auf mehrere Module anzuwenden.

Beispiel für die Konfiguration des Verschlüsselungsfelds



6. Klicken Sie auf **Absenden**.

Richten Sie eine Modulzugriffsrichtlinie ein, um Zugriff auf das kryptografische Modul zuzuweisen. Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > > **Neu erstellen** > **.**
8. Füllen Sie die Felder des Formulars aus.

Formular „Modulzugriffsrichtlinie“

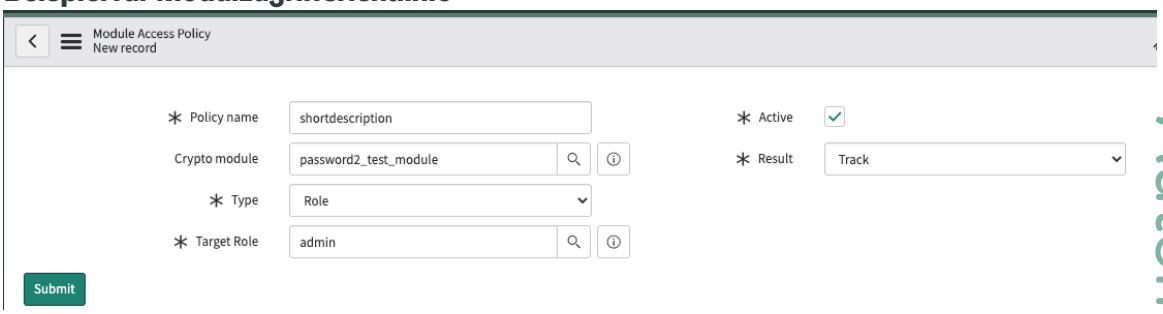
Feld	Beschreibung
Richtlinienname	Name für die Richtlinie, z. B. Kurzbeschreibung.
Crypto-Modul	Krypto-Modul, das Sie zum Verschlüsseln Ihres Schlüssels erstellt haben.
Typ	Typ der Zugriffsbezeichnung für die Krypto-Richtlinie. Verwenden Sie **Rolle**, um nur den Benutzern Zugriff auf das verschlüsselte Feld zu gewähren, denen die Rolle zugewiesen ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

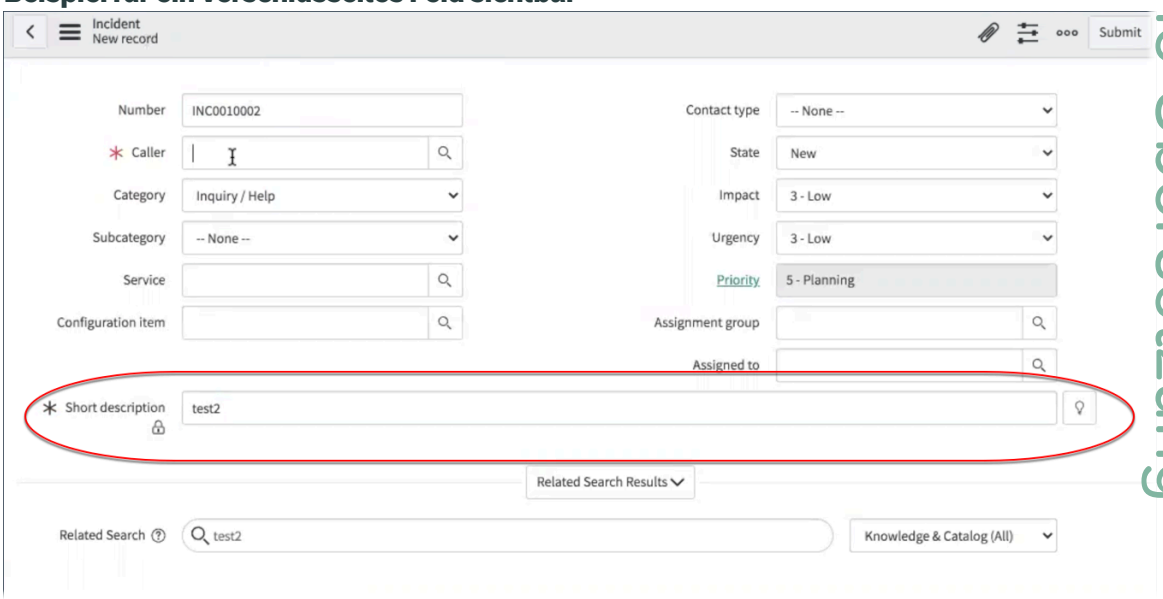
Feld	Beschreibung
Zielrolle	Die Rolle, die Zugriff auf das verschlüsselte Feld hat. **Wählen**Sie für dieses Beispiel Administrator aus.
Aktiv	Option zum Aktivieren der Modulzugriffsrichtlinie.
Ergebnis	Die **Option**Nachverfolgen ermöglicht den Zugriff auf das Feld für die ausgewählte Rolle. (Um den Zugriff auf dieses Feld für die ausgewählte Rolle einzuschränken, wählen Sie **Ablehnen** oder**Striktes Ablehnen**aus.)

Beispiel für Modulzugriffsrichtlinie



9. Klicken Sie auf **Absenden**.
10. Navigieren Sie als Benutzer mit der Rolle sn_kmf.admin zu **Incident** > **Neu**.

Beispiel für ein verschlüsseltes Feld sichtbar



Sie können jetzt das Feld Kurzbeschreibung basierend auf der Konfiguration der Modulzugriffsrichtlinie anzeigen.

Hinweis:
Der Rolle sn_kmf.admin wurde Benutzerzugriff auf das verschlüsselte Feld Kurzbeschreibung gewährt, indem die **Modulzugriffsrichtlinie**auf Nachverfolgen festgelegt wurde. Beachten Sie das Schlosssymbol ( ) unter dem Feldnamen, das angibt, dass das Feld ein verschlüsseltes Feld ist.

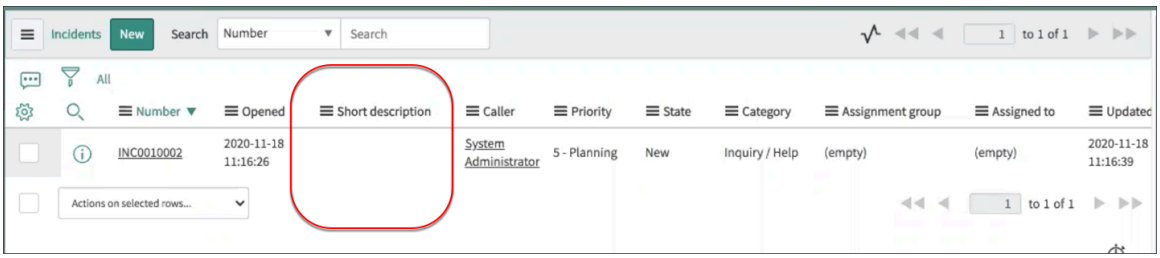
Sie können jetzt als Endbenutzer auf das **Incidents** -Modul zugreifen, um die verschlüsselte Feldkonfiguration zu testen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

11. Melden Sie sich als Benutzer an, der im konfigurierten Feld von der Anzeige der verschlüsselten Daten ausgeschlossen werden soll.

Verschlüsselte Daten auf Feldebene



Wenn Sie auf die Incident-Nummer zugreifen, sind die Daten in der Kurzbeschreibung nicht sichtbar.

Ergebnisse

Sie haben Ihren symmetrischen Schlüssel erfolgreich verwendet, um den Zugriff auf ein bestimmtes Feld mit Verschlüsselung auf Spaltenebene Enterprisezu steuern.

Vorstellung der Anhangverschlüsselung

Diese Tour zeigt, wie Sie einen Anhang in Ihrer Instanz mit Verschlüsselung auf Spaltenebene Enterprise mit dem Key Management Framework (KMF) verschlüsseln. Außerdem wird gezeigt, wie Sie Ihren eigenen Schlüssel verwenden.

Vorbereitungen

Hinweis:
Dieses Verfahren gilt nur für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise. Weitere Informationen zum Abrufen von [Aktivieren Sie Column Level Encryption Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Erforderliche Rolle: kmf kryptografischer Manager

Warum und wann dieser Vorgang ausgeführt wird

Diese Tour beginnt mit einer Instanz, in der Sie Ihren vom Kunden bereitgestellten kryptografischen Schlüssel bereits erstellt und hochgeladen haben. Sie können den Schlüssel ServiceNow® verwenden, in diesem Beispiel wird jedoch ein vom Kunden bereitgestellter Schlüssel verwendet.

Laden Sie vertrauliche Anhänge in Ihre Instanz hoch, und beschränken Sie den Zugriff für bestimmte Benutzer. Verwenden Sie die verschlüsselte Feldkonfiguration, um anzugeben, welche autorisierten Mitarbeiter auf vertrauliche Daten zugreifen können.

Wir zeigen Ihnen, wie Sie Anhänge so verschlüsseln, dass sie nur für Benutzer sichtbar sind, denen Zugriff gewährt wird, oder für alle Benutzer sichtbar sind, die nicht auf die Anzeige der Daten beschränkt sind. In diesem Beispiel beschränken wir den Zugriff einer bestimmten Rolle auf einen Anhang im **Incidents** -Modul.

Hinweis:
Obwohl Sie mehrere Module mit Spaltenverschlüsselung verwenden können, müssen bei der Anhangverschlüsselung einzelne Module verwendet werden.

Prozedur

1. Stellen Sie sicher, dass Verschlüsselung auf Spaltenebene Enterprise aktiviert ist.
2. Erstellen Sie ein kryptografisches Modul.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

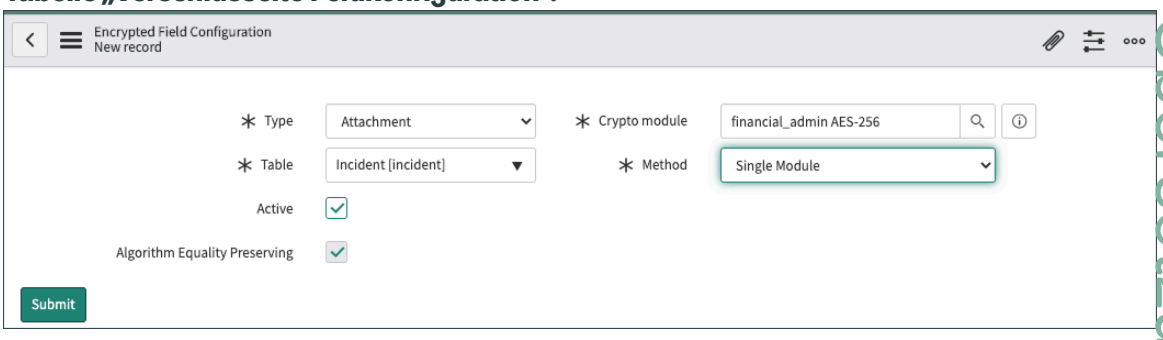
Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene.

3. Navigieren zu **Systemsicherheit** > **Verschlüsselungsfeld-Konfigurationen**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie das Formular aus:

Verschlüsselte Feldkonfigurationsfelder

Feld	Beschreibung
Typ	Wählen Sie **Anhang** aus, um Ihren persönlichen Schlüssel zum Verschlüsseln eines Anhangs aus der ausgewählten **Tabelle** zu verwenden. Wählen Sie für dieses Beispiel **Incident**aus.
Tabelle	Wählen Sie die Tabelle aus, um auf die vertraulichen Informationen zuzugreifen. Wählen Sie für dieses Beispiel **Incident [incident]**aus.
Aktiv	Markieren **Sie Aktiv**, um die Feldkonfiguration verwenden zu können.
Algorithmus-Gleichstellungserhaltung	Wenn Sie die Verschlüsselung auf Spaltenebene auswählen, wird dieses Feld basierend auf der ausgewählten Tabelle angezeigt.
Crypto-Modul	Wählen Sie das von Ihnen erstellte Modul zur Verwendung mit dem persönlichen Schlüssel aus.
Methode	Die Option **Einzelnes Modul** wird verwendet, um die Richtlinien für ein Modul anzuwenden. **Mehrere Module** werden verwendet, um die Richtlinien auf mehrere Module anzuwenden.

Tabelle „Verschlüsselte Feldkonfiguration“.



6. Klicken Sie auf **Absenden**.

Richten Sie eine Modulzugriffsrichtlinie ein, um Zugriff auf das kryptografische Modul zuzuweisen. Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**.
8. Klicken Sie auf **Neu**.
9. Füllen Sie das Formular aus:

Felder der Modulzugriffsrichtlinie

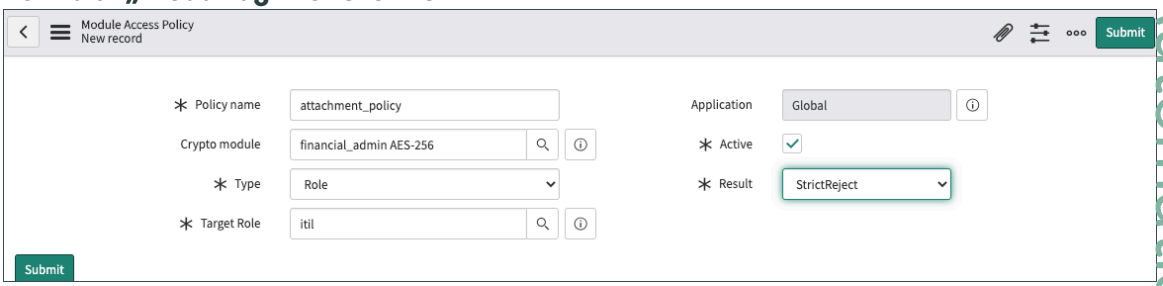
Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein, z. B. „Anhangrichtlinie“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

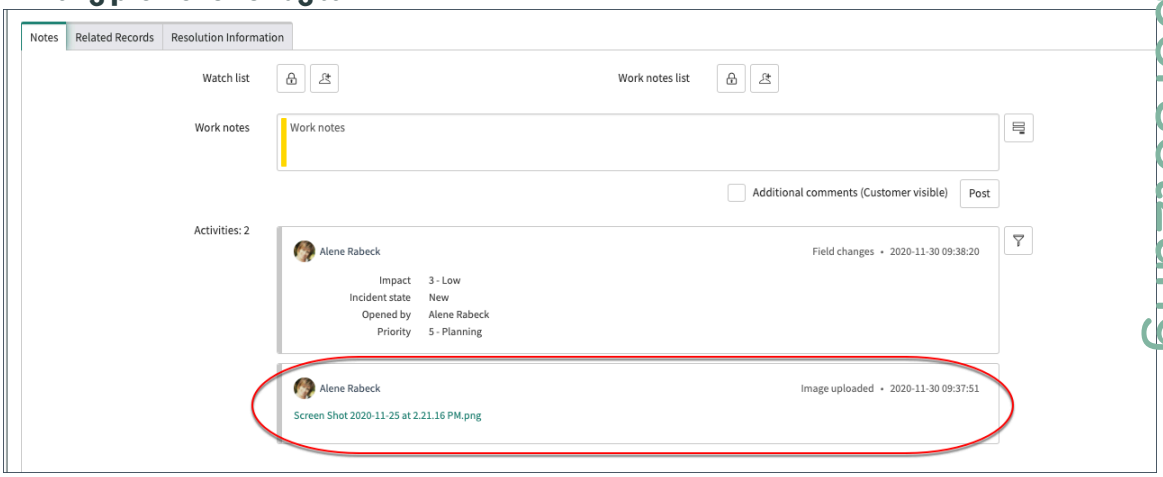
Feld	Beschreibung
Crypto-Modul	Wählen Sie das Krypto-Modul aus, das Sie erstellt haben, um Ihren Schlüssel zu verschlüsseln.
Typ	Wählen Sie **Rolle** aus, um den Zugriff auf das verschlüsselte Feld für Benutzer mit der zugewiesenen Rolle zu beschränken.
Zielrolle	Wählen Sie die Rolle aus, die keinen Zugriff auf das verschlüsselte Feld hat. Wählen Sie für dieses Beispiel **itil aus**.
Aktiv	Aktivieren Sie diese Checkbox, um die Modulzugriffsrichtlinie verwenden zu können.
Ergebnis	Wählen Sie **Striktes Ablehnen** aus, um den Zugriff auf den Anhang von der ausgewählten Rolle aus zu steuern. (Um Zugriff für die ausgewählte Rolle zu gewähren, wählen Sie **Nachverfolgen**.)

Formular „Modulzugriffsrichtlinie“



10. Klicken Sie auf **Absenden**.
11. Navigieren Sie als Administrator oder als Person, die den Incident erstellt hat, zu **Incidents**, und fügen Sie in der zugehörigen Liste „ **Notizen** “ einen Anhang zu **Aktivitäten** hinzu.

Anhang pro Rolle verfügbar



12. Melden Sie sich als Benutzer an, der den Zugriff auf den verschlüsselten Anhang eingeschränkt hat.
13. Öffnen Sie den Incident, und scrollen Sie zum Abschnitt **Aktivitäten:.**

> **Hinweis:**
> Der Link zum Öffnen des Anhangs ist für Benutzer mit der eingeschränkten Rolle nicht zugänglich.

14. Sie haben jetzt erfolgreich Ihren vom Kunden bereitgestellten Schlüssel verwendet, um den Zugriff auf einen bestimmten Anhang mithilfe der Verschlüsselung auf Spaltenebene zu steuern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Infrastruktursicherheit

Verwenden Sie Infrastruktur-Sicherheitstools, um Zertifikate zu erstellen, hochzuladen und zu verwalten, die Ihre Instanz zum Verschlüsseln des Datenverkehrs vom Client zum Server verwendet.

Das Plugin „Infrastructure Security“ bietet die Tools, mit denen Sie TLS-Verschlüsselungen und -Zertifikate (Transport Layer Security) verwalten können. Ihre Instanz verwendet TLS, um den Datenverkehr vom Client zu Ihrem Server zu verschlüsseln.

Wählen Sie die in Ihrer Instanz verwendeten Verschlüsselungen aus

Auf der **TLS-Seite**können Administratoren konfigurieren, welche Rechenzentrums-Verschlüsselungen in ihrer Instanz verwendet werden sollen, und die Reihenfolge auswählen, in der die Verschlüsselungen getestet werden.

Eigene Zertifikate generieren und hochladen

Verwenden Sie die Sicherheitstools der Infrastruktur, um eigene Zertifikatsignaturanforderungen zu generieren, die von der Zertifizierungsstelle Ihrer Wahl signiert werden können. Anschließend können Sie die Tools von verwenden, um das signierte Zertifikat in das Lastenausgleichsmodul Ihrer Instanz hochzuladen.

Überwachen Sie den Status Ihrer Verschlüsselungen und Zertifikate

Verwenden Sie die Seiten **TLS-Einstellungen** und **SYOC-Einstellungen**, um den Status der Änderungen anzuzeigen, die Sie an Ihren Verschlüsselungen und Zertifikaten vorgenommen haben.

Installieren Sie das Plugin „Infrastructure Security“.

Installieren Sie das Plugin ServiceNow „ Infrastructure Security Settings“ (com.glide.infrastructure_security), um mit der Verwendung dieser Funktionen zu beginnen. Weitere Informationen zur Aktivierung von Plugins finden Sie unter Plugins aktivieren .

Aktivieren Sie nach der Installation des Plugins die SYOC-Funktionalität (Sign Your Own Security), indem Sie die Systemeigenschaft `sn_infra_sec.syoc.enabled` auf `true`setzen.

Hinweis:
Wenn die Eigenschaft `sn_infra_sec.syoc.enabled` in Ihrer Instanz nicht verfügbar ist, müssen Sie sie erstellen. Details zu diesem Vorgang finden Sie unter Add a system property .

Generieren Sie eine Zertifikatsignaturanforderung

Verwenden Sie die Seite „Zertifikatsignatur generieren (CSR)“, um eine Zertifikatsignaturanforderung zu erstellen, um vom Kunden signierte Zertifikate für das Lastenausgleichsmodul Ihrer Instanz zu unterstützen.

Vorbereitungen

Erforderliche Rolle: admin

Weitere Informationen zur Verwendung von benutzerdefinierten URLs mit ServiceNowfinden Sie unter Legen Sie eine benutzerdefinierte URL als Instanz-URL fest.

Prozedur

1. Navigieren zu **Alle** > **Sicherheitseinstellungen der Infrastruktur** > **CSR generieren**.
2. Fügen Sie Ihrer Anforderung eine oder mehrere Domänen hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie unter der Überschrift **Domänen** auf die Schaltfläche **Hinzufügen**.

b. Geben Sie im Popup-Fenster die Domäne ein, und wählen Sie **OK**.

c. Wiederholen Sie diese Schritte nach Bedarf, um weitere Domänen hinzuzufügen.

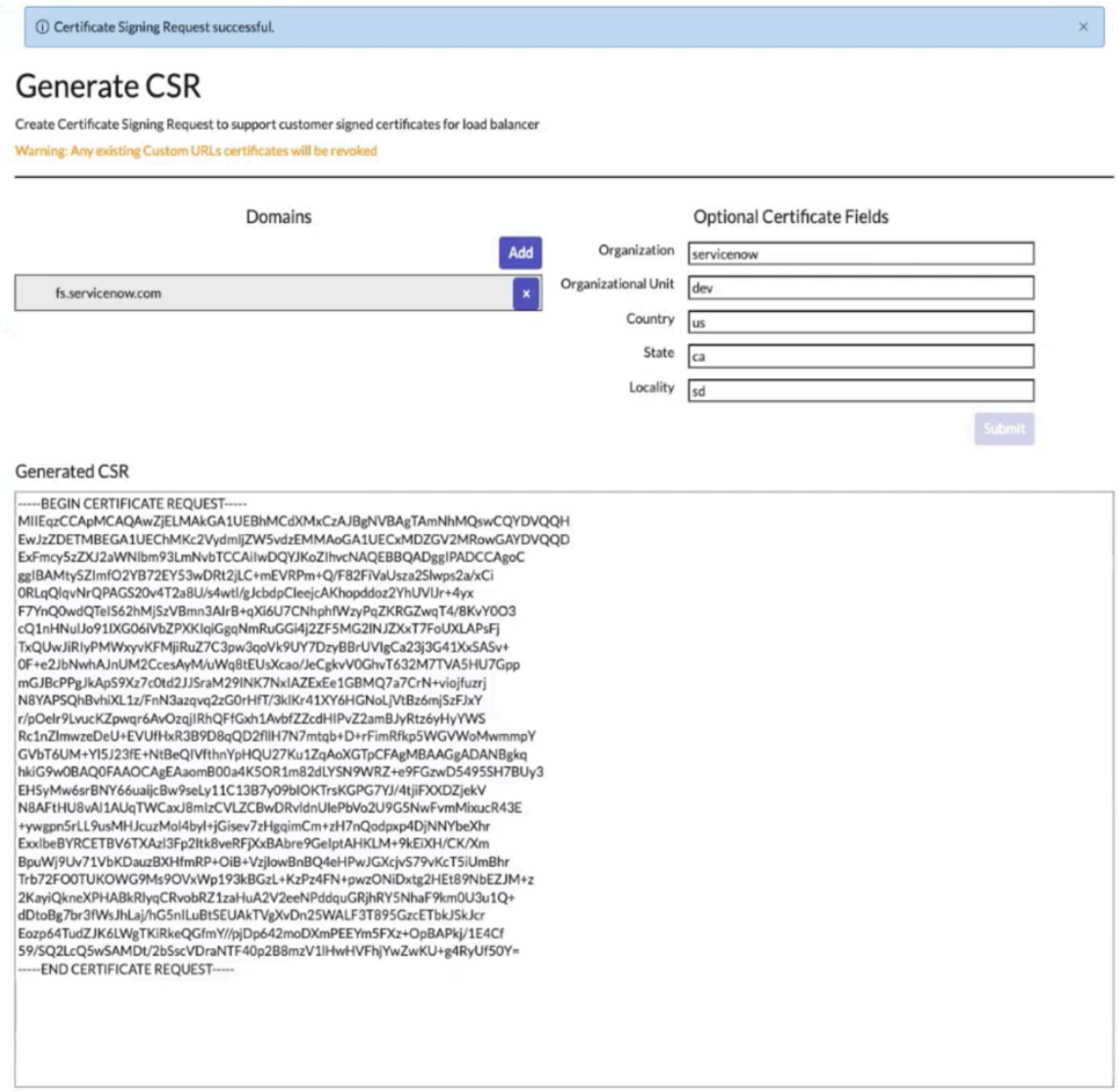
> **Hinweis:**
> Domänen können entfernt werden, indem Sie links neben jedem Domäneneintrag auf die Schaltfläche X klicken.

3. Geben Sie alle Informationen, die in Ihre Anforderung aufgenommen werden sollen, in das **Feld Optionale Zertifikatsfelder**ein.
4. Wählen Sie **Absenden**.

> **Warnung:**
> Sie können keine Anforderung senden, während eine andere Anforderung generiert wird. Wenn dieses Problem auftritt, wird der Fehler „Ressource in Konflikt“ angezeigt. Brechen Sie zur Verarbeitung die aktuelle Anforderung ab, oder warten Sie, bis die aktuelle Anforderung verarbeitet ist, bevor Sie eine weitere Anforderung senden.

Nachdem Sie **Absenden**ausgewählt haben, generiert Ihre Instanz die Zertifikatsignaturanforderung. Die Anforderung wird im Feld **Generierte CSR** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Kopieren Sie den Inhalt des Felds **Generierte CSR**.

Nächste Maßnahme

Signieren Sie die Zertifikatanforderung mit der Zertifizierungsstelle Ihrer Wahl. Dieser Prozess wird von der Zertifizierungsstelle definiert, die Sie auswählen. Informationen zu diesem Vorgang finden Sie in der Dokumentation der Behörde. Wenn Sie ein signiertes Zertifikat haben, laden Sie es mit den Schritten in Ein Zertifikat wird in eine Instanz hochgeladenin Ihre Instanz hoch.

Password2-Verschlüsselung mit dem Key Management Framework (KMF)

Unterstützt von Key Management Frameworkverwenden Sie den Password2 Feldtyp (zweifach verschlüsselt), um benutzerdefinierte Felder mit Aufgabentrennung, Schlüsselschutz und Lebenszyklusverwaltung zu verschlüsseln und zu entschlüsseln. Es funktioniert gemäß den NIST 800-57-Richtlinien und bietet FIPS 140-2-L3-Schutz.

Password2 ist ein Textfeld, in dem Passwörter mit bidirektionaler Verschlüsselung gespeichert werden. Bei der bidirektionalen Verschlüsselung werden Passwörter als sicherer verschlüsselter Wert gespeichert, der innerhalb der Instanz entschlüsselt werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp:
Ab dem Release Vancouver können Administratoren die 3DES-Verschlüsselung für Passwort2-Felder durch den neueren Advanced Encryption Standard (AES) ersetzen. Details finden Sie unter GlideEncrypter-Nutzung von 3DES für Passwort2-Felder veraltet.

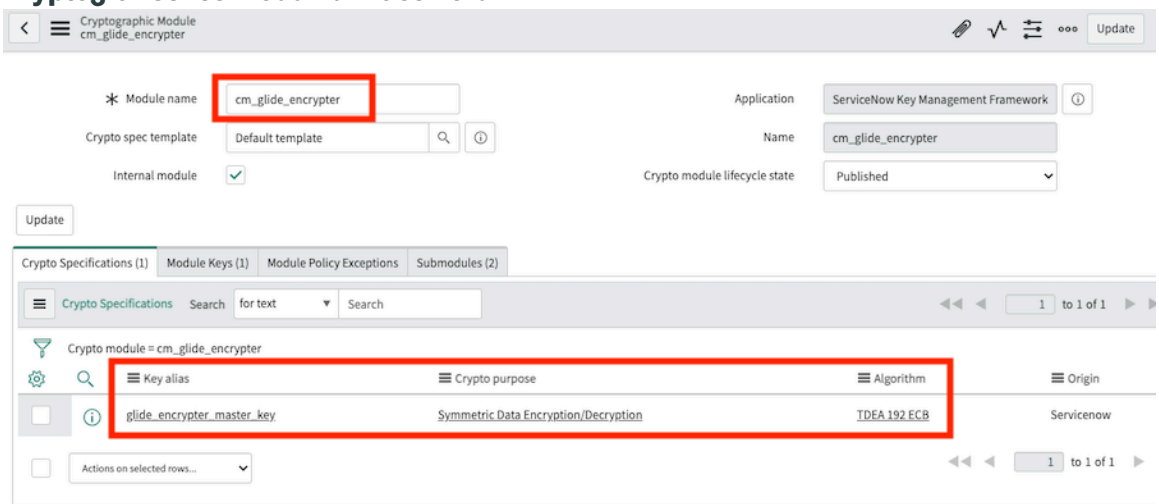
Aktivierung

Password2 -Funktionalität ist standardmäßig aktiviert. Sie wird durch die Eigenschaft `glide.kmf.encrypter.enabled` gesteuert, die für alle neuen Instanzen und Upgrades auf „ **true** “ festgelegt wird. Sie müssen [] nicht aktivieren, um Password2Verschlüsselung auf Spaltenebene Enterprise zu verwenden.

Funktionsweise von Password2

Key Management Framework stellt das übergeordnete kryptografische **Basissystemmodul cm_glide_encrypter bereit**. Dieses Modul stellt eine kryptografische Spezifikation und einen Schlüssel bereit, mit dem ältere Password2 -Felder entschlüsseln kann.

Kryptografisches Modul für Password2



Dieses cm_glide_encrypter-Modul kann Submodule mit jeweils einem eigenen Modulschlüssel und einer eigenen Spezifikation haben. Wenn ein Submodul mit demselben Anwendungsbereich wie die Anwendung vorhanden ist, in der sich das Feld Password2 befindet, verwendet das System das Submodul. Beispiel: Wenn eine Tabelle in der Anwendung ServiceNow® Kundenservice ein Submodul aufweist und Sie Informationen in ein Feld Password2 in einer Tabelle im Anwendungsbereich Kundenservice] schreiben, ruft der kryptografische Prozess das Submodul Kundenservice auf. Der Prozess verwendet auch den Schlüssel dieses Submoduls für die Verschlüsselung und Entschlüsselung mit einem eindeutigen AES 256 GCM-Verschlüsselungsschlüssel. Ein Submodul pro Anwendungsbereich ist zulässig. Übergeordnete Module werden nicht immer für den globalen Bereich verwendet. Im Allgemeinen verwenden neue Felder instance_level_glide_encrypter.

Hinweis:
Sie können keine eigenen Submodule in Washington DCerstellen. Submodule werden in verschiedenen Anwendungs-Plugins auf der Now Platformbereitgestellt. Sie können Schlüssel für Submodule rotieren, aber nicht für das übergeordnete cm_glide_encrypter-Modul.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung und On-Premise-Kunden

KMF Password2 unterstützt keine Domänentrennung. Sie können Password2 mit lokalen Instanzen verwenden.

Veraltete Password2 und aktuelle Password2

In Washington DCwurde das vorhandene Feld Password2 aktualisiert.

Die aktuelle Implementierung von Password2:

- Verwendet Key Management Framework gemäß NIST 800-57 Key Wrapping-Richtlinien und bietet FIPS 140-2-L3- Schutz für die gesamte Schlüsselhierarchie.
- Enthält Funktionen zum Erstellen dedizierter und eindeutiger KMF Password2 -Submodule für bestimmte Anwendungen, die eine Steuerung durch den Anwendungsbereich ermöglichen. Jedes Submodul verfügt über einen eigenen eindeutigen AES 256 GCM-Verschlüsselungsschlüssel.

Passwort2-Felder in Skripts

Wenn Sie mit einem Skript auf Felder von Password2 zugreifen, führen Sie das Skript im selben Bereich wie der Tabellenbereich aus. Verwenden Sie setDisplayValue(), um Password2 Werte zu verschlüsseln, und getDecryptedValue(), um den Wert zu entschlüsseln und zu lesen.

Hinweis:
Verwenden Sie die GlideEncrypter()- API nicht für Felder Password2.

Dieses Beispielskript zeigt, wie my@Password in der Spalte password2 der Tabelle „table_xyz“ verschlüsselt wird.

```
var  gr =  new GlideRecord('table_xyz');
gr.setDisplayValue('pwd2column_name', 'my@Password');
gr.insert();
```

Wichtig:
Sie können die setValue()- API nicht für das Feld Password2 verwenden.

Dieses Beispielskript zeigt, wie Sie dasselbe Feld entschlüsseln, um den Wert abzurufen:

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

Wichtig:
Die API getDecryptedValue() ist nicht bereichsbezogen. Sie ist global verfügbar.

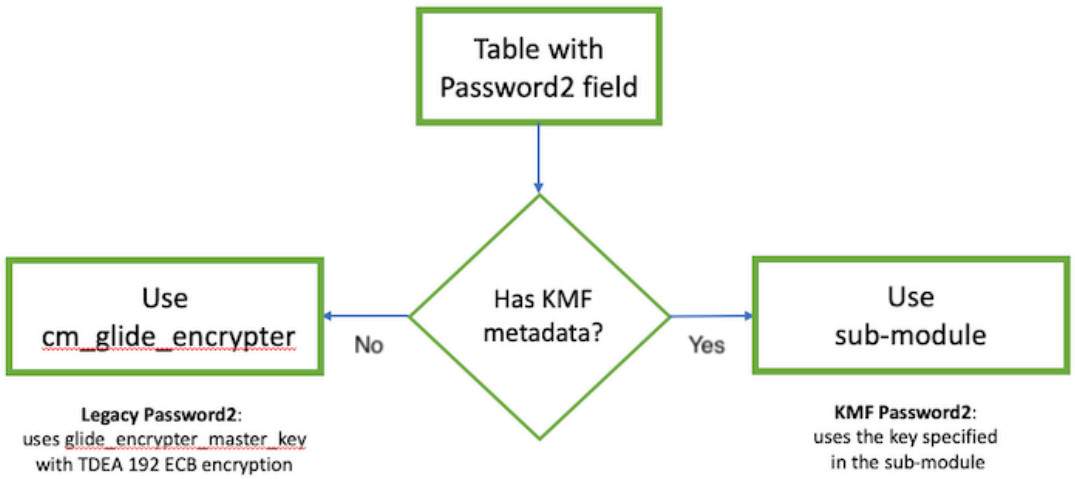
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn Sie Daten in einem Feld Password2 verschlüsseln, bestimmt das System den Anwendungsbereich, in dem sich das Feld Password2 befindet.
2. Das System sucht dann nach einem Submodul des übergeordneten **cm_glide_encrypter** -Moduls mit demselben Bereich wie die Anwendung, wenn die Eigenschaft auf *true*festgelegt ist.

Hinweis:
Wenn ein Submodul mit demselben Bereich vorhanden ist, verwendet es die Submodulspezifikation und den Schlüssel, um die Verschlüsselung durchzuführen.

In dieser Abbildung wird erläutert, wie Ihre Instanz Daten in Feldern von Password2 entschlüsselt:

Password2-Entschlüsselungs-Flow



KMF Password2 -Migrationsauftrag

Für Kunden, die ein Upgrade von früheren Releases durchführen, wird ein Migrationsauftrag bereitgestellt. Daten, die mit einer veralteten Password2 -Verschlüsselung verschlüsselt sind, werden mit dem Schlüssel in einem KMF Password2 -Submodulschlüssel erneut verschlüsselt. Die erneute Verschlüsselung gilt nur für Tabellen mit Feldern Password2 in Anwendungsbereichen, für die auch Submodule für diesen Bereich erstellt wurden. Zum Beispiel wird ein Legacy-Feld Password2 in der Anwendung **XYZ_example** (mit Anwendungsbereich **XYZ_example**) nur dann erneut verschlüsselt, wenn ein Submodul für den Anwendungsbereich **XYZ_example** unter dem übergeordneten Modul cm_glide_encrypter vorhanden ist.

Die Verschlüsselungsschlüssel KMF Password2 im -Submodul sind in der Schlüsselhierarchie KMF geschützt (Umschlag verschlüsselt).

Cloud-Verschlüsselung mit Schlüsselverwaltung

ServiceNow® Cloud-Verschlüsselung bietet verschlüsselten Speicher für die Datenbank mithilfe von Blockverschlüsselung zusammen mit einer verbesserten Schlüsselverwaltung. Cloud-Verschlüsselung ist mit dem Abonnementpaket ServiceNow® Platform Encryption verfügbar.

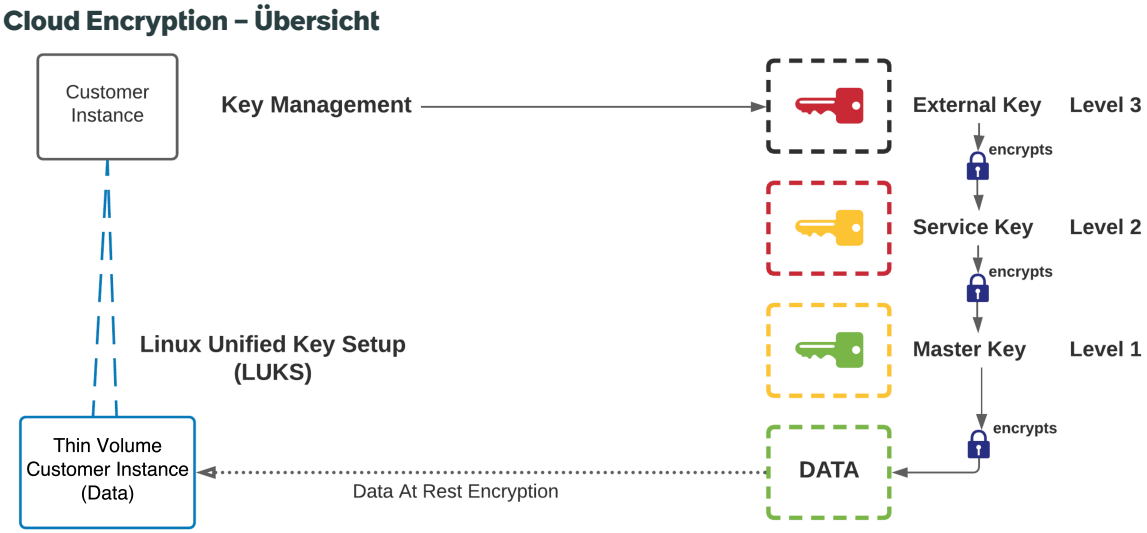
Cloud-Verschlüsselung bietet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aufgabentrennung.
- Rotation von ServiceNow verwalteten Schlüsseln.
- Option Vom Kunden verwaltete Schlüssel.

Hinweis:
Sie können diese Option verwenden, wenn Ihre Organisation die Verwendung von Schlüsselmaterial erfordert, das von Ihren eigenen kryptografischen Tools oder Bibliotheken, dem Schlüsselverwaltungssystem des Unternehmens oder dem Hardware-Sicherheitsmodul (HSM) generiert wurde. Details siehe Schlüsselverwaltungsvorgänge.

Das folgende Diagramm zeigt, wie Cloud-Verschlüsselung funktioniert.



Das Modul Cloud-Verschlüsselung „ Key Management“ besteht aus den folgenden Submodulen:

- Schlüsselverwaltungsvorgänge:
  - Greifen Sie auf die Liste der Schlüssel zu.
  - Schlüsselrotationsvorgänge durchführen.
  - Vom Kunden verwalteten Schlüssel zurückziehen.
- Schlüsselverwaltungstransaktionen:

  Verweisen Sie auf alle Transaktionen, die für die verwendeten Schlüssel aufgetreten sind.

  Verwenden Sie Ihren eigenen kundenverwalteten Schlüssel für die Verschlüsselung.

Unter bestimmten Umständen kann bei Verwendung von kundenverwalteten Schlüsseln eine Anforderung zum Zurückziehen des Schlüssels gewählt werden. Sie müssen zuerst die Funktion zum Zurückziehen des Schlüssels von Kundenservice und Support anfordern und einen rechtlichen Nachtrag ausfüllen.

Die Option Quorum Control Policy Settings (Quorum-Steuerungsrichtlinieneinstellungen) wird verfügbar, wenn die Widerrufsfunktion aktiviert wird. Andernfalls ist das Modul im Menü nicht sichtbar. Diese Funktion kann nur aktiviert werden, wenn kundenverwaltete Schlüssel verwendet werden. Mit dieser Richtlinie können Einstellungen in Bezug auf das Quorum konfiguriert werden, wenn die Auszahlungsfunktion aktiviert ist. Weitere Informationen zu dieser Funktion finden Sie unter Quorum-Steuerungsrichtlinie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Verschlüsselung unterstützt die MariaDB-Datenbank sowohl für Produktions- als auch für Nicht-Produktionsinstanzen. Postgres mit Swarm64-Erweiterungen werden für ServiceNow Lesereplikatdatenbanken unterstützt.

Weitere Informationen zur Lizenzierung von Cloud-Verschlüsselungfinden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

Damit lizenzierte Kunden die Verschiebung einer Instanz zu Cloud Encryption anfordern können, folgen Sie den Anweisungen in KB1117369 . Sie müssen über die Rolle „Kundenadministrator“ oder „Partneradministrator“ verfügen, um das Servicekatalogelement zum **Aktivieren der Cloud-Verschlüsselung in Ihrer Instanz**anzufordern. Die Aktivierung dieser Funktion erfordert ein einstündiges Wartungsfenster.

Schlüsselverwaltungsvorgänge

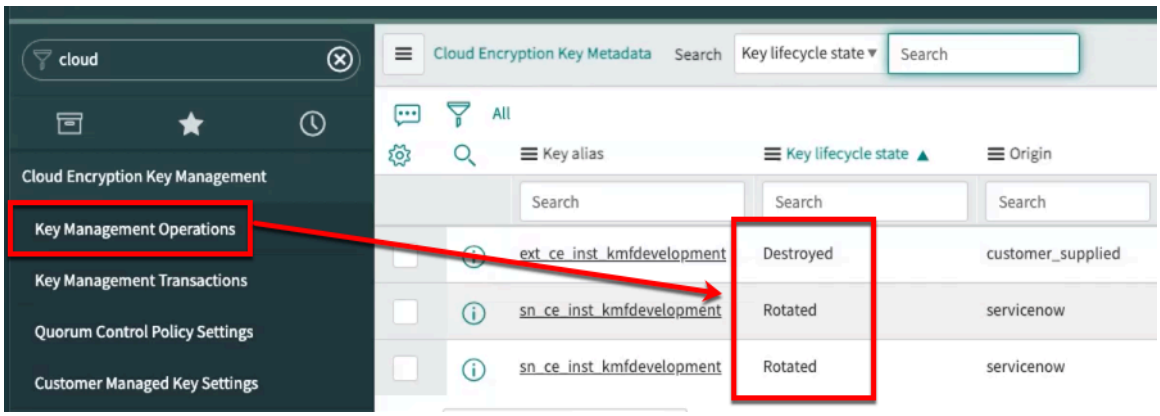
Das Submodul Key Management Operations bietet Zugriff zum Anzeigen und Verwalten aller mit ServiceNow Cloud-Verschlüsselungverwendeten Verschlüsselungsschlüssel.

Erste Schritte mit Cloud Encryption

Wichtige Lebenszyklusstatus

Es gibt jeweils nur einen aktiven Schlüssel im System. Wenn Sie einen Schlüssel auswählen, greifen Sie auf die Aktivität für den ausgewählten Schlüssel zu, z. B. welche Schlüssel rotiert oder zurückgezogen wurden, sowie den entsprechenden Zeitstempel.

Der Lebenszyklusstatus des Schlüssels wird entsprechend dem durchgeführten Schlüsselverwaltungsvorgang aktualisiert.



Weitere Informationen finden Sie unter Rotieren Sie einen von ServiceNow verwalteten Schlüssel oder Rotieren Sie einen kundenverwalteten Schlüssel.

Hinweis:
Der Schlüsselrotationsprozess kann bis zu 20 Minuten dauern.

Rotieren Sie einen von ServiceNow verwalteten Schlüssel

Rotieren Sie den aktiven verwalteten Schlüssel Cloud-Verschlüsselung ServiceNow.

Vorbereitungen
Erforderliche Rolle: kmf_admin, kmf_cryptomanager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Wenn Sie vom Kunden verwaltete Schlüssel verwenden, finden Sie weitere Informationen unter Rotieren Sie einen kundenverwalteten Schlüssel.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**.
   Die Liste Cloud-Verschlüsselung Schlüsselmetadaten wird geladen. Alle in Ihrer Instanz verwendeten Schlüssel werden aufgelistet. Es kann jeweils nur ein Schlüssel aktiv sein.

   Wenn Sie zum ersten Mal auf das Modul Cloud-Verschlüsselung zugreifen, sind Schlüsseleinträge verfügbar, nachdem eine erste Schlüsselrotation durchgeführt wurde. Ein verwalteter Schlüssel von ServiceNow ist der Standardwert im System.

2. Wählen Sie den aktiven Schlüssel aus der Tabelle aus.
   Die Tabelle „Schlüsseldefinition“ wird mit allgemeinen Informationen zu Ihrem von ServiceNow generierten Schlüssel angezeigt.

3. Klicken Sie auf die Schaltfläche **Schlüssel** rotieren.
   Eine Benachrichtigung wird mit der Option angezeigt, die Schlüsselrotation fortzusetzen oder den Vorgang abzubrechen.

4. Klicken Sie auf **OK**, um den Schlüssel zu rotieren.
   Oben auf der Seite „Schlüsseldefinition“ wird eine Bestätigungsmeldung angezeigt.

5. Kehren Sie zum Bildschirm „Schlüsselverwaltungsvorgänge“ zurück, um die Tabelle Cloud-Verschlüsselung Schlüsselmetadaten zu aktualisieren.
   Einträge werden für den aktuell aktiven Schlüssel und den Schlüssel aufgelistet, der zur Rotation anstelle des aktuell aktiven Schlüssels generiert wird. Informationen zu den verschiedenen verfügbaren Status finden Sie unter Schlüssel-Lebenszyklusstatus des Key Management Framework.

   Der aktive Schlüssel wird mit der Schlüsselversion `0` aufgelistet, und der generierte Schlüssel hat die Version `1`.

6. Öffnen Sie den Eintrag für den ursprünglichen Schlüssel, um die Schlüsselverwaltungstransaktionen anzuzeigen.
   Weitere Informationen finden Sie unter Schlüsselverwaltungstransaktionen.
   Der zuvor aktive Schlüssel, Version `0`, wurde auf den Schlüssellebenszyklusstatus `Rotiert` aktualisiert, und der neue Schlüssel, Version `1`, lautet `Aktiv`.

Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor

Befolgen Sie diese Schritte, um Ihren vom Kunden verwalteten Schlüssel für den Upload in Ihre Instanz vorzubereiten.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager, sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird
Für einen vom Kunden verwalteten Schlüssel können Sie eine beliebige kryptografische Bibliothek oder HSM verwenden, um Ihren Schlüssel zu generieren. Dieser Schlüssel muss ein 256-Bit-AES-Schlüssel sein und von einem Cloud Encryption-Wrapping-Zertifikat mit einem RSAES_OAEP_SHA_256-Verschlüsselungsschema umschlossen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie das kryptografische OpenSSL-Tool zum Generieren Ihres Schlüssels verwenden, muss die OpenSSL-Version Version 1.1.1x oder höher sein.

Wenn Sie Ihren vom Kunden verwalteten Schlüssel mit Windowserstellen und umschließen, müssen Sie den umschlossenen Schlüssel über Bash-Shell-Supportanwendungen wie Git Bash generieren.

Prozedur

1. Generieren Sie mit OpenSSL einen zufälligen Wert, der als symmetrischer AES-256-Bit-Schlüssel verwendet werden soll.

   Aus Kompatibilitätsgründen muss Ihr symmetrischer Schlüssel die folgenden Attribute aufweisen:

Attribut	Wert
Schlüsseltyp	Auf dem AES-Algorithmus (Advanced Encryption Standard) basierender symmetrischer Schlüssel.
Schlüsselgröße	256 Bit (32 Byte)
Schlüssel-Wrapping-Anforderung	○ RSA-Verschlüsselungsalgorithmus ○ Optimum asymmetrische Verschlüsselungsauffüllung (OAEP) ○ SHA-256-Hash-Funktion (RSAES_OAEP_SHA_256) ○ Codiert mit Base64-Algorithmus

2. Speichern Sie den Schlüssel in einer Datei ähnlich wie „openedssl rand 32 > klartext_key.bin.

   Wichtig:
   Speichern Sie diese Datei zum späteren Nachschlagen an einem sicheren Ort. Dieser Schlüssel wird mit dem öffentlichen Schlüssel für den Upload umschlossen.

3. Extrahieren Sie den öffentlichen Schlüssel aus der heruntergeladenen Wrapping-Zertifikatdatei von Ihrer Instanz:

```
openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
```

   Hinweis:
   Informationen zum Herunterladen des Packzertifikats finden Sie unter.

4. Umschließen Sie den generierten Schlüssel mit dem öffentlichen Schlüssel, der mit dem Packzertifikat heruntergeladen wurde, und verwenden Sie den Algorithmus RSAES_OAEP_SHA_256:

```
cat plaintext_key.bin | openssl pkeyutl -encrypt -inkey public_key.pem -pubin -pkeyopt
 rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 | openssl base64 -A -out
 wrapped_key.txt
```

   Eine in diesem Befehl angegebene Datei enthält einen umschlossenen, vom Kunden verwalteten Schlüssel, der SN für den CMK-Prozess bereitgestellt werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zwischen ServiceNow- und kundenverwalteten Schlüsseln wechseln

Wechseln Sie zwischen einem vom Kunden verwalteten Schlüssel oder einem von ServiceNow verwalteten Schlüssel zur Verwendung in ServiceNow Cloud-Verschlüsselung.

Standardmäßig ist Ihre Instanz für die Verwendung von ServiceNow verwalteten Schlüsseln konfiguriert, und die Generierung von ServiceNow Verschlüsselungsschlüsseln ist aktiv. Administratoren können jedoch vom Kunden verwaltete Schlüssel verwenden. Sie können auch zu ServiceNow verwalteten Schlüsseln zurückkehren.

Rotieren Sie einen kundenverwalteten Schlüssel

Rotieren Sie Ihren vom Kunden verwalteten Schlüssel zu Ihrer Instanz, nachdem Sie Ihren vom Kunden verwalteten Schlüssel für Cloud-Verschlüsselungverpackt haben.

Vorbereitungen

Erforderliche Rolle: kmf_admin, kmf_cryptomanager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**.
   Die Liste der **Cloud-Verschlüsselungsschlüssel-Metadaten** wird geladen. Alle Schlüssel, die in Ihrer Instanz verwendet wurden, werden aufgelistet.
2. Öffnen Sie in der Liste **„Metadaten des Cloud-Verschlüsselungsschlüssels“** den Datensatz für Ihren aktiven Schlüssel.
   Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel mit dem **Schlüssellebenszyklusstatus**`Active`aus. In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. Klicken Sie im Schlüsseldefinitionsdatensatz auf die Schaltfläche **Schlüssel** rotieren.
4. **Führen Sie im Fenster „Vom Kunden verwalteten Schlüssel** hochladen“ die aufgeführten Schritte aus.

   a. Wählen Sie **Wrapping-Zertifikat herunterladen aus**.
   Die `Datei public_certificate....zip` wird auf Ihren lokalen Computer heruntergeladen und zum Umschließen Ihres vom Kunden verwalteten Schlüssels verwendet.

   > ⚠ **Warnung:**
   > Vermeiden Sie potenzielle Probleme im Zusammenhang mit Zertifikaten, indem Sie das Packzertifikat jedes Mal herunterladen, wenn Sie zu einem vom Kunden verwalteten Schlüssel rotieren oder zu diesem wechseln.

   b. Wählen Sie **Durchsuchen** aus, um Ihren vom Kunden verwalteten Schlüssel hochzuladen. Suchen Sie dann Ihren verpackten Verschlüsselungsschlüssel, und wählen Sie ihn aus.
   Um eine andere Datei auszuwählen, wählen Sie die Datei aus, und wählen **Sie Entfernen**.

   c. Schließen Sie das Fenster „Anhänge“.

   d. Klicken Sie auf **OK**, um Ihren Schlüssel hochzuladen.
   Wenn der Schlüssel im richtigen Format vorliegt, wird eine Bestätigungsmeldung angezeigt. Andernfalls wird eine Fehlermeldung angezeigt. Die Schlüsseldatei wird an den Schlüsseldefinitionsdatensatz angehängt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Tabelle „Schlüsselverwaltungstransaktionen“ werden die Schritte zum Herunterladen des Zertifikats und zum Hochladen des Schlüssels aufgelistet. Weitere Informationen zu den Anforderungsschritten finden Sie unter Schlüsselverwaltungstransaktionen.

5. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** , um die Liste der Schlüssel anzuzeigen.
   In der Liste der Schlüssel sehen Sie einen neuen Datensatz für Ihren vom Kunden verwalteten Schlüssel. Dieser neue Schlüssel hat den **Ursprungswert** „ **customer_supplie“** und befindet sich im Status **„Aktiv** “. Ihr vorheriger Schlüssel befand sich im Status „ **Rotiert“**.

Wechseln Sie zu einem vom Kunden verwalteten Schlüssel

Verwenden Sie Ihren vom Kunden verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Vorbereitungen

Erforderliche Rolle: kmf_admin oder kmf_cryptomanager

Um zu einem kundenverwalteten Schlüssel zu wechseln, müssen Sie einen verpackten kundenverwalteten Schlüssel bereithalten, der im Rahmen dieser Schritte hochgeladen werden kann. Weitere Informationen zur Vorbereitung dieses Schlüssels für den Upload finden Sie unter Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor. Nach dem Hochladen Ihres Schlüssels initiiert dieser Prozess eine Schlüsselrotation zu Ihrem neuen Schlüssel.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**.
2. Öffnen Sie in der Liste **„Metadaten des Cloud-Verschlüsselungsschlüssels“** den Datensatz für Ihren aktiven Schlüssel.
   Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel mit dem **Schlüssellebenszyklusstatus**`Active`aus. In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. Klicken Sie im Abschnitt „ **Zugehörige Links** “ des Formulars auf den Link **Zu kundenverwaltetem Schlüssel** wechseln.
4. Klicken Sie im Dialogfeld **Zu kundenverwaltetem Schlüssel** wechseln auf die Schaltfläche **Verwalteten Schlüssel** hochladen.
5. Führen Sie im Dialogfeld „ **Vom Kunden verwalteten Schlüssel** hochladen“ die aufgeführten Schritte aus.

   a. Wählen Sie **Wrapping-Zertifikat herunterladen aus**.

   > ⚠ **Warnung:**
   > Vermeiden Sie potenzielle Probleme im Zusammenhang mit Zertifikaten, indem Sie das Packzertifikat jedes Mal herunterladen, wenn Sie zu einem vom Kunden verwalteten Schlüssel rotieren oder zu diesem wechseln.

   b. Wählen Sie **Durchsuchen**aus, und befolgen Sie die Eingabeaufforderungen, um Ihren Schlüssel auszuwählen und von Ihrem Gerät hochzuladen.

   c. Wählen Sie **Zu kundenverwaltetem Schlüssel wechseln aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Instanz generiert eine Anforderung zum Wechsel zu Ihrem vom Kunden verwalteten Schlüssel. Im aktuellen Formular können Sie sehen, dass sich der **Schlüssellebenszyklusstatus** des ursprünglich aktiven Schlüssels in **Rotiert**geändert hat.

6. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** , um die Liste der Schlüssel anzuzeigen.
   In der Liste der Schlüssel sehen Sie einen neuen Datensatz für Ihren vom Kunden verwalteten Schlüssel. Dieser neue Schlüssel hat den **Ursprungswert** „ **customer_supplie“** und befindet sich im Status **„Aktiv** “.

Ergebnisse

Ihre Instanz verwendet jetzt Ihren vom Kunden verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Wichtig:
Stellen Sie sicher, dass eine Kopie Ihres Verschlüsselungsschlüssels immer an einem sicheren Ort für Schlüsselverwaltungsvorgänge verfügbar ist. Ohne diesen Schlüssel ist der Zugriff auf Ihre Instanz möglicherweise nicht möglich.

Wechseln Sie zu einem von ServiceNow verwalteten Schlüssel

Wechseln Sie von einem vom Kunden verwalteten Schlüssel zurück zu einem verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Vorbereitungen

Erforderliche Rolle: kmf_admin oder kmf_cryptomanager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**.
2. Öffnen Sie in der Liste **„Metadaten des Cloud-Verschlüsselungsschlüssels“** den Datensatz für Ihren aktiven Schlüssel.
   Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel mit dem **Schlüssellebenszyklusstatus**Activeaus. In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. Klicken Sie im Abschnitt „ **Zugehörige Links** “ des Formulars auf den Link **Zu von ServiceNow verwaltetem Schlüssel** wechseln.
4. **Wählen Sie im Dialogfeld „Zu ServiceNow-verwaltetem Schlüssel** wechseln“ die Schaltfläche **Zu ServiceNow** -verwaltetem Schlüssel wechseln.
   Die Instanz generiert eine Anforderung zum Wechsel zu einem von ServiceNow verwalteten Schlüssel. Im aktuellen Formular können Sie sehen, dass sich der **Schlüssellebenszyklusstatus** des ursprünglich aktiven Schlüssels in **Rotiert**geändert hat.
5. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** , um die Liste der Schlüssel anzuzeigen.
   In der Liste der Schlüssel sehen Sie einen neuen Datensatz für einen von ServiceNow verwalteten Schlüssel. Dieser neue Schlüssel hat den **UrsprungswertServiceNow** und befindet sich im Status **Aktiv**.

Planen Sie die Schlüsselrotation

Legen Sie einen Zeitplan für die automatische Rotation Ihrer von ServiceNow verwalteten Schlüssel fest. Dieser Prozess löscht automatisch einen Verschlüsselungsschlüssel und ersetzt den alten Schlüssel durch einen neu generierten kryptografischen Schlüssel. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, kann dieser Zeitplan Sie daran erinnern, Ihre benutzerdefinierten Schlüssel manuell zu rotieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Einstellungen für geplante Schlüsselrotation**.
2. Aktivieren Sie das Kontrollkästchen **Geplante Schlüsselrotation aktivieren**.
3. Füllen Sie die verbleibenden Felder entsprechend Ihren Geschäftsanforderungen aus.

Einstellungen für geplante Schlüsselrotation

Feld	Beschreibung
Anzahl der Monate zwischen Schlüsselrotationen (maximal 60 Monate)	Anzahl der Monate zwischen Schlüsselrotationen. Dieser Wert ist standardmäßig 12 und kann maximal 60 Monate haben.
Wochentag für die Schlüsselrotation	Wochentag, an dem die Schlüsselrotation durchgeführt wird.
Uhrzeit für die Schlüsselrotation	Uhrzeit, zu der die Schlüsselrotation ausgeführt wird.
Datum und Uhrzeit der nächsten Schlüsselrotation	Datum und Uhrzeit der nächsten geplanten Schlüsselrotation. Dieser Wert kann nicht direkt bearbeitet werden und wird basierend auf Ihren Auswahlmöglichkeiten automatisch berechnet.
Angabe, wie viele Tage vor der Schlüsselrotation die Erinnerung gesendet werden soll (maximal 15 Tage)	Anzahl der Tage vor dem Datum Ihrer Schlüsselrotation, an denen Ihre Instanz Benachrichtigungen sendet.
E-Mail-Benachrichtigungen werden an die folgende Liste Ihrer genehmigten Sicherheitsadministratoren gesendet	Liste der Benutzer, die Benachrichtigungen zur Schlüsselrotation erhalten. Der **Systemadministrator** befindet sich standardmäßig in dieser Liste.

4. Wählen Sie **Absenden**.
   Nachdem Sie „Absenden“ ausgewählt haben, wird oben im Formular eine Benachrichtigung angezeigt. Die Benachrichtigungen bestätigen Ihre Schlüsselrotation und Ihren Benachrichtigungszeitplan.

⚠ Warnung:

Jede geplante Schlüsselrotation verfügt über eine eindeutige Signatur, die die Integrität einer Aufgabe sicherstellt und nicht autorisierte Änderungen erkennt. Die Signatur für eine regelmäßige Aufgabe ist für jede Instanz eindeutig. Wenn Sie eine geplante Schlüsselrotationsaufgabe von einer Quellinstanz A in eine Zielinstanz B klonen, schlägt die Signaturvalidierung der geplanten Aufgabe in Instanz B fehl. In diesem Fall können Sie die Signatur neu erstellen, indem Sie das Kontrollkästchen **Geplante Schlüsselrotation** aktivieren deaktivieren und dann erneut aktivieren. Weitere Informationen zu diesem Problem finden Sie unter KB1247113 .

Ziehen Sie einen vom Kunden verwalteten Schlüssel zurück

Nachdem die Funktion zum Zurückziehen kundenverwalteter Schlüssel aktiviert wurde, wird ein Zurücknahmevorgang auf der Seite „Schlüsselverwaltungsvorgänge“ verfügbar. Schlüssel- und Quorum-Genehmigungsvorgänge können ebenfalls verwaltet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: kmf_admin, kmf_cryptomanager

Dieser Abschnitt gilt nur, wenn Sie Cloud Encryption Zurückziehen und erneut liefern, ein optionales Add-on zu Cloud-Verschlüsselung, lizenziert haben.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > > **Vorgänge der Schlüsselverwaltung**.
2. Wählen Sie den aktiven kundenverwalteten Schlüssel aus der Tabelle aus.
   Die Tabelle „Schlüsseldefinition“ wird mit allgemeinen Informationen zu Ihrem Kundenschlüssel angezeigt. Eine Funktion zum Zurückziehen eines Schlüssels ist jetzt verfügbar.
3. Wählen Sie die **Option Schlüssel** zurückziehen aus, um den Auszahlungsprozess auszulösen.

Warnung:

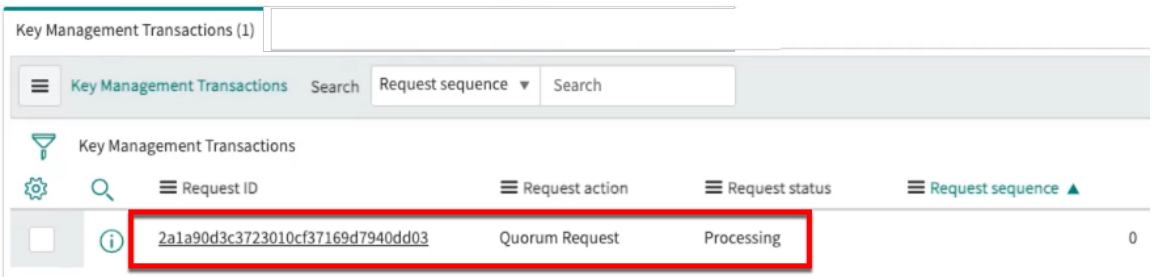
Eine Warnmeldung Schlüssel zurückziehen wird angezeigt. Das Zurückziehen des Schlüssels löst ein Herunterfahren Ihrer Instanz aus, bis ein Wiederherstellungsvorgang mit dem zurückgezogenen Schlüssel ausgeführt wird.

Gefahr:

Sie können einen Wiederherstellungsvorgang nur mit demselben Schlüssel ausführen, der zurückgezogen wurde. Wenn Sie zu einem anderen Schlüssel rotieren möchten, müssen Sie dies tun, nachdem Sie den zurückgezogenen Schlüssel wiederhergestellt haben.

Wenn der zurückgezogene vom Kunden verwaltete Schlüssel nicht innerhalb des Zeitrahmens wiederhergestellt wird, für den ServiceNow Sicherungen aufbewahrt (Details finden Sie in der SOP für Sicherung und Wiederherstellung [Standard Operating Procedure]), sind Ihre Instanzdatenbanksicherungen nicht mehr zugänglich. Auf diese Weise verlorene Sicherungsdaten können nicht wiederhergestellt werden.

4. Klicken Sie auf **OK**, um den Schlüssel zurückzuziehen.
   Wählen Sie **Abbrechen** aus, wenn Sie Fragen zur Funktion zum Zurückziehen des Schlüssels haben. Sie kehren zum Bildschirm Schlüsseldefinition zurück, und eine Bestätigungsmeldung wird angezeigt.
5. Aktualisieren Sie die Seite Schlüsseldefinition, um die ausstehende Auszahlungsanforderung anzuzeigen.



Wenn die Quorum Control-Richtlinie aktiviert wurde, muss der Genehmigungs-Workflow erfolgreich abgeschlossen werden, um die Schlüsselzurücknahme abzuschließen. Details siehe Verwalten Sie Quorum Control.

Stellen Sie einen vom Kunden verwalteten Schlüssel erneut bereit

Nach Abschluss eines Vorgangs zum Zurückziehen eines Schlüssels muss Ihr vom Kunden verwalteter Schlüssel erneut in Ihrer Instanz bereitgestellt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: kmf_admin, kmf_cryptomanager

Hinweis:
Dieser Abschnitt gilt nur, wenn Sie Cloud Encryption Zurückziehen und erneut bereitstellen lizenziert haben.

Prozedur

1. Wechseln Sie zu Now Support, und navigieren Sie zu **Servicekatalog** > **Katalog** > **Instanzenverwaltung** > **Instanzwiederherstellung – Verwalteten Schlüssel erneut bereitstellen**.
2. Klicken Sie auf **Anforderung**.
3. **Wählen** Sie im Fenster „ **Instanzwiederherstellung – Verwalteten Schlüssel erneut** liefern“ Ihre Instanz in der Dropdown-Liste Instanz auswählen aus.
4. Laden Sie das Packzertifikat herunter, indem Sie auf den Text des **Packzertifikats** klicken.

   Warnung:
   Sie müssen jedes Mal, wenn Sie einen vom Kunden verwalteten Schlüssel rotieren oder hochladen, ein neues Wrapping-Zertifikat herunterladen.

5. Bereiten Sie Ihren Schlüssel für den Upload vor.
   Details zu diesem Vorgang finden Sie unter Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor.
6. Klicken Sie im Abschnitt **Schritt 4** auf **Durchsuchen und hochladen**, um den umschlossenen Schlüssel von Ihrem lokalen Gerät hochzuladen.
   Nachdem Ihr Schlüssel hochgeladen wurde, wird er unter **„Folgende Datei wurde erfolgreich**hochgeladen“ angezeigt. Wenn Sie den Schlüssel erneut hochladen müssen, klicken Sie auf **Datei entfernen,** und laden Sie Ihren Schlüssel erneut hoch, wie in den vorherigen Schritten beschrieben.
7. Klicken Sie auf **Schlüssel rotieren**, um die erneute Lieferung abzuschließen.

Quorum-Steuerungsrichtlinie

Die Quorum-Kontrollrichtlinie gibt die Mindestanzahl von Genehmigungen an, die unter der Gesamtzahl der ausgewählten Genehmiger erforderlich ist, um das Quorum für den vom Kunden verwalteten Schlüsselentzug zu erreichen.

Warnung:
Sie müssen einen rechtlichen Nachtrag unterzeichnen, um die Funktion zum Zurückziehen des Schlüssels zu aktivieren. Die Option Quorum Control Policy Settings (Quorum-Steuerungsrichtlinieneinstellungen) wird verfügbar, wenn die Widerrufsfunktion aktiviert ist. Andernfalls ist das Modul im App-Menü nicht sichtbar. Nach dem Zurückziehen des Schlüssels ist Ihre Instanz nicht mehr verfügbar, bis der Verschlüsselungsschlüssel erneut bereitgestellt wird und wieder aktiv ist.

Unter bestimmten Umständen möchten Sie möglicherweise eine Schlüsselentnahme erstellen. Sie müssen zuerst die Schlüsselentzugsfunktion von Kundenservice und Supportanfordern.

Die Quorum-Kontrollrichtlinie gibt die Mindestanzahl von Genehmigungen an, die unter der Gesamtzahl der ausgewählten Genehmiger erforderlich ist, um das Quorum für den vom Kunden verwalteten Schlüsselentzug zu erreichen. Zum Beispiel gibt es insgesamt fünf Genehmiger, aber nur vier Genehmigungen sind erforderlich, um das Quorum zu erreichen. Wenn vier Genehmigungen eingeholt wurden, wird die Auszahlungsanforderung verarbeitet und der Schlüssel eingezogen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Immer wenn ein Zurücknahmevorgang in einer Gruppe ausgeführt wird, die für die Quorum-Genehmigung aktiviert ist, wird ein Workflow für die Quorum-Genehmigung ausgelöst. Eine E-Mail-Benachrichtigung wird an alle Benutzer gesendet, die die Genehmigung erteilen können. Aufgaben werden auch in den Accounts der Genehmiger generiert, die ihnen im Dashboard angezeigt werden, wenn sie sich bei ihrem ServiceNow -Account anmelden.

Die Benutzer können Genehmigungen über die -Instanz, per E-Mail oder über die Seite „Schlüsselverwaltungsvorgänge“ erteilen. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erreicht ist.

Sobald die Mindestanzahl von Genehmigern erreicht ist, ist das Quorum erreicht und der Schlüsselentzug wird ausgelöst. Die Zurücknahme wird durchgeführt und protokolliert, einschließlich der Namen der Benutzer, die die Anforderung genehmigt haben.

Setup-Details finden Sie unter Konfigurieren Sie die Einstellungen für die Quorum Control-Richtlinie.

Konfigurieren Sie die Einstellungen für die Quorum Control-Richtlinie

Befolgen Sie diese Schritte, um die Einstellungen für die Quorum Control-Richtlinie zu konfigurieren.

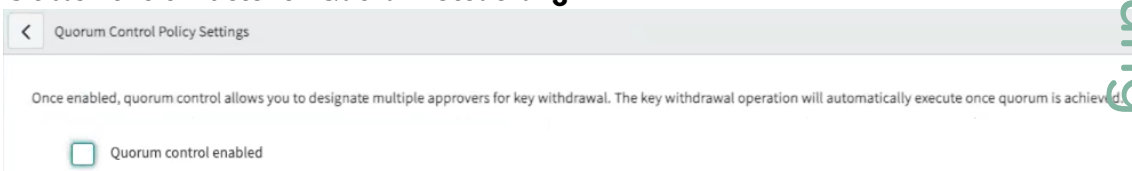
Vorbereitungen
Erforderliche Rolle: kmf_admin, kmf_cryptomanager

Warum und wann dieser Vorgang ausgeführt wird

> **⚠ Warnung:**
> Sie müssen einen rechtlichen Nachtrag unterzeichnen, um die Funktion zum Zurückziehen des Schlüssels zu aktivieren. Die Option Quorum Control Policy Settings (Einstellungen für Quorum Control-Richtlinie) wird verfügbar, wenn die Widerrufsfunktion aktiviert ist. Andernfalls ist das Modul im App-Menü nicht sichtbar. Nach dem Zurückziehen des Schlüssels ist Ihre Instanz nicht mehr verfügbar, bis der Verschlüsselungsschlüssel wieder aktiv ist.

Prozedur

1. Fordern Sie die Schlüsselentzugsfunktion von Kundenservice und Supportan.
2. Navigieren zu **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Einstellungen für Quorum Control-Richtlinie**.
3. Aktivieren Sie das **Kontrollkästchen Quorum-Steuerung**

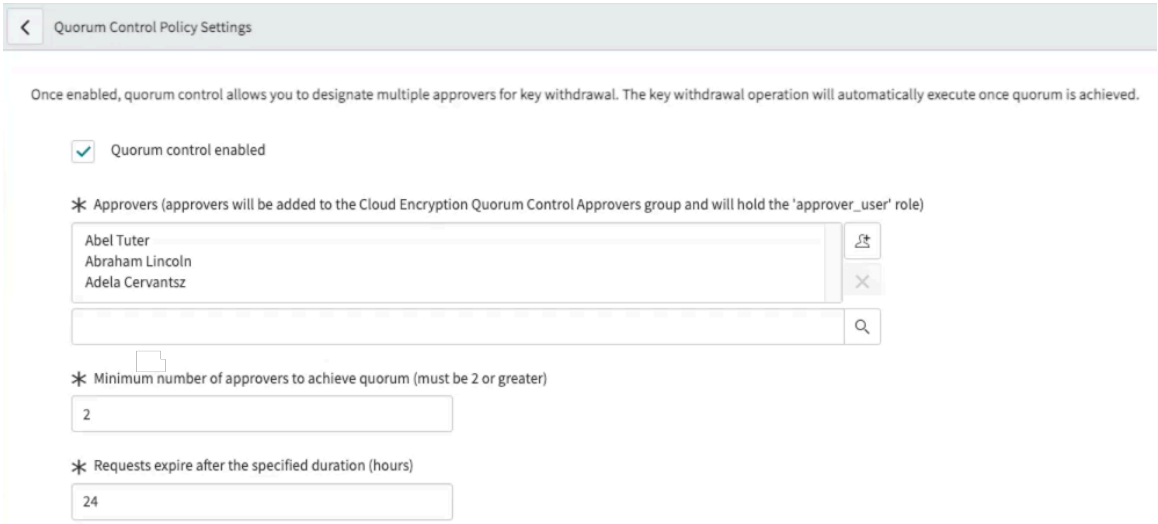


aktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Felder werden angezeigt, die zum Konfigurieren der Quorum-Steuerung erforderlich



sind.

4. Füllen Sie die Felder aus, um das Formular auszufüllen.

5. Klicken Sie auf **Absenden**.
   Eine Bestätigungsmeldung wird angezeigt.

Nächste Maßnahme

Die Auszahlungsaktionen sind in Schlüsselverwaltungsvorgängeverfügbar.

Verwalten Sie Quorum Control

Nachdem ein Workflow für einen Auszahlungsvorgang ausgelöst wurde, können Quorum-Aktionen auf der Seite „Schlüsselverwaltungsvorgänge“ verwaltet werden. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erreicht ist.

Vorbereitungen

Erforderliche Rolle: kmf_admin oder kmf_cryptomanager

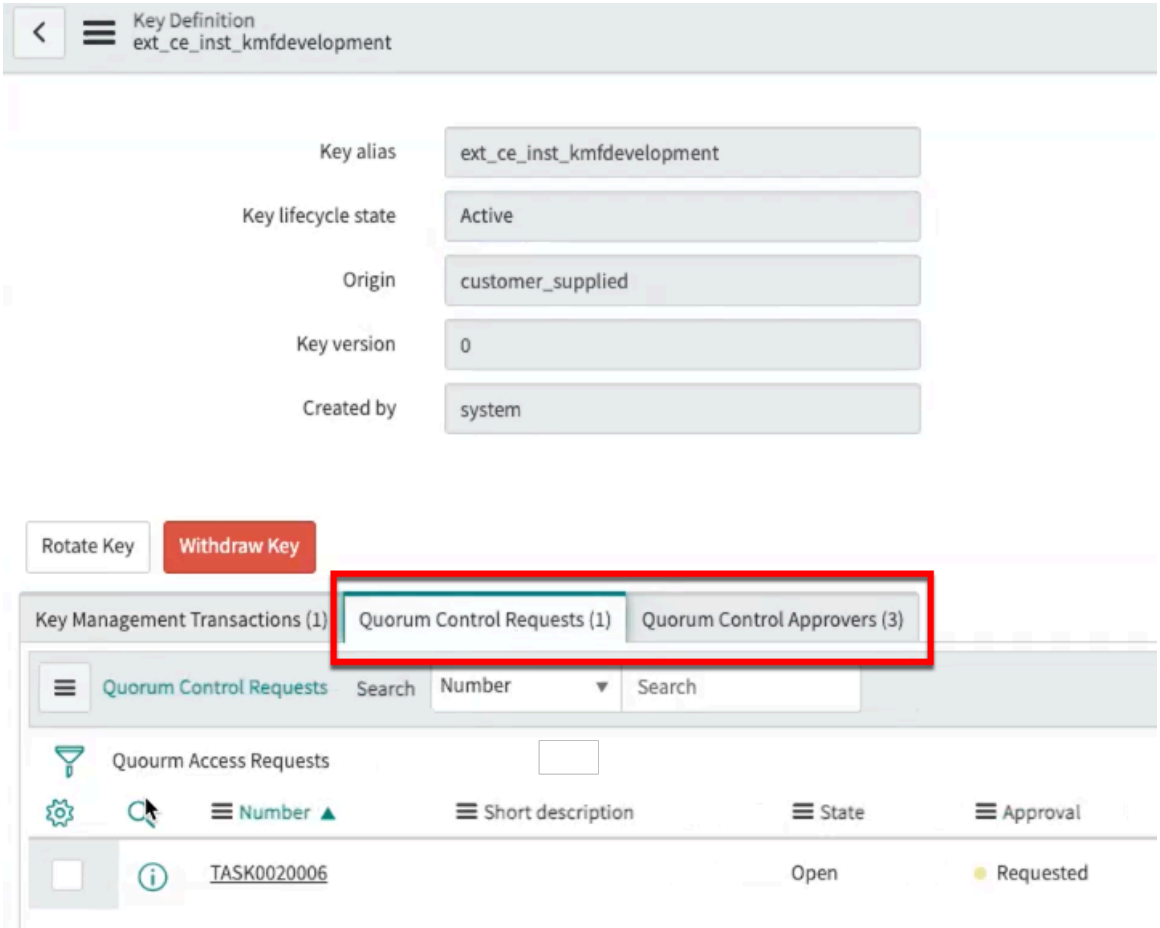
Wenn das Quorum genehmigt oder abgelehnt wurde, erhält die anfordernde Person des Schlüsselentzugs eine E-Mail mit der Information, ob das Quorum erreicht oder abgelehnt wurde.

Prozedur

1. Führen Sie die Schritte aus, um einen vom Kunden verwalteten Schlüssel aus Schlüsselverwaltungsvorgängezurückzuziehen.
2. Zeigen Sie die Registerkarten **Quorum Control-Anforderungen** und **Quorum Control-Genehmiger an**.

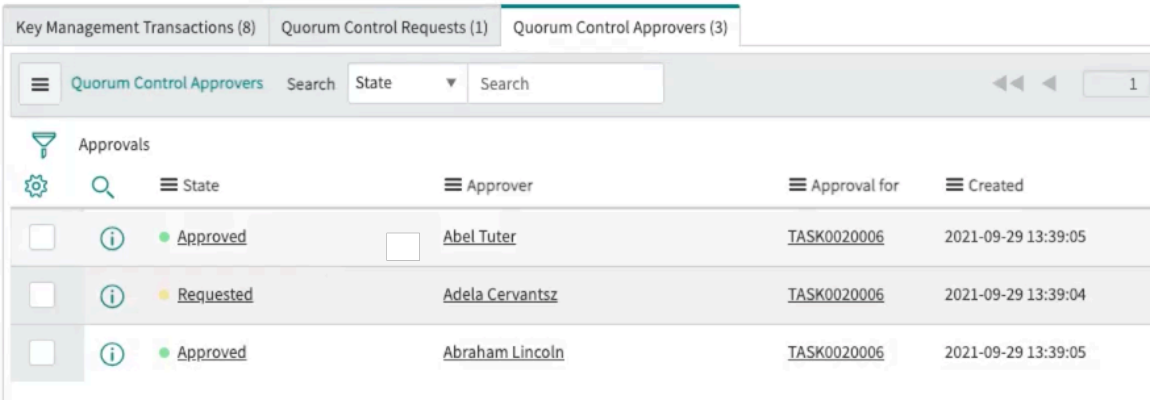
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Öffnen Sie die **Quorum Control-Anforderungen** Registerkarte, um die tatsächlich erstellte Anforderung anzuzeigen.
   - Status:
     - Offen: Die Aktion zum Zurückziehen des Schlüssels wartet auf das Erreichen des Quorums.
     - Geschlossen – vollständig: Das Quorum wurde erfüllt, und für diese bestimmte Quorum-Anforderung kann keine weitere Aktion durchgeführt werden.
   - Genehmigung:
     - Angefordert: Genehmigungs-E-Mails wurden gesendet, und der Workflow wurde ausgelöst, um das Quorum zu erreichen.
     - Genehmigt: Der Schlüssel wird zurückgezogen, und die Instanz wird heruntergefahren.
     - Abgelehnt: Die Quorum-Anforderung wird abgebrochen, und es wird keine weitere Aktion für diese Anforderung ausgeführt. Zum Zurückziehen des Schlüssels ist eine neue Auszahlungsanforderung erforderlich.
4. Öffnen Sie die Registerkarte Quorum Control-Genehmiger, um die Liste der Genehmiger und den Status der Genehmigungsanforderung anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Status:

- Angefordert: Der Genehmiger hat noch keine Maßnahmen in Bezug auf die Genehmigungsanforderung ergriffen.
- Genehmigt: Die Anforderung wurde entweder über die E-Mail oder über die Genehmigungsseite genehmigt.

5. Wechseln Sie zur Registerkarte **Schlüsselverwaltungstransaktionen**, um den Fortschritt des Anforderungsschritts für das Zurückziehen des Schlüssels anzuzeigen.
   - Schritt 0 – Quorum-Anforderung: Die tatsächliche Quorum-Anforderung. Die Quorum-Anforderung muss abgeschlossen sein, um die Schritte zum Zurückziehen des Schlüssels auszulösen.
   - Schritt 1 – Schlüsselzurücknahme: Der Schritt zum Zurückziehen des Schlüssels. Diese besteht aus den Schritten zwei bis sieben.
   - Schritt 2 – Request_preparation: Erstellt eine Anforderung zum Auslösen sowie für Wrapping und Rotation.
   - Schritt 3 – request_integrity_check: Validiert, dass die Anforderung berechtigt und sicher ist.
   - Schritt 4 – request_validation: Überprüft, ob eine Anforderung ausgeführt wird. Es kann jeweils nur eine Rotationsanforderung verarbeitet werden.
   - Schritt 5 – hsm_key_delete: Ruft KeySecure auf, um den aktiven Schlüssel zu löschen.
   - Schritt 6 – key_metadata_withraw: Konvertiert den aktiven Lebenszyklusstatus der Schlüsselmetadaten in „zerstört“.
   - Schritt 7 – post_withraw: Ruft auf, um die Instanz herunterzufahren.

Genehmigen oder verweigern Sie eine Anforderung zur Quorum-Kontrolle

Genehmigen oder verweigern Sie eine Anforderung zur Quorum-Kontrolle.

Warum und wann dieser Vorgang ausgeführt wird
Wenn eine Quorum-Anforderung erstellt wurde, ist die Mindestanzahl von Genehmigungen durch die Mitglieder erforderlich. Nachdem ein Workflow für einen Auszahlungsvorgang ausgelöst wurde, können Quorum-Aktionen mit verschiedenen Methoden verwaltet werden. Die Benutzer können Genehmigungen über die Seite „Schlüsselverwaltungsvorgänge“, „Meine Genehmigungen“ in der Instanz oder direkt über die Anforderungs-E-Mail erteilen. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erreicht ist.

Dieses Verfahren beschreibt, wie Sie eine Quorum-Anforderung über die Seite „Schlüsselverwaltungsvorgänge“ genehmigen oder ablehnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: kmf_admin, kmf_cryptomanager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Transaktionen der Schlüsselverwaltung** > **Quorum Control-Genehmiger**.
2. Wählen Sie Ihren Benutzernamen aus der Tabelle aus.
3. Genehmigen oder verweigern Sie die Anforderung.

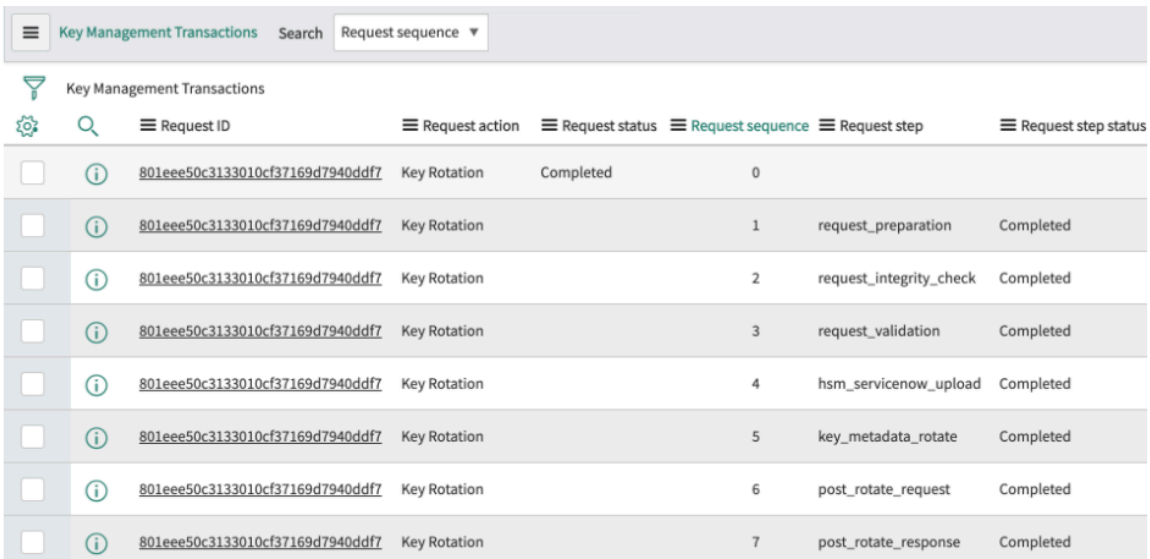
Schlüsselverwaltungstransaktionen

Das Submodul „Key Management Transactions“ (Schlüsselverwaltungstransaktionen) zeigt alle Transaktionen an, die für die Schlüssel in Ihrer ServiceNow -Instanz aufgetreten sind.

- Eine Schlüsseltransaktion wird wie folgt definiert:
  - Besteht aus mehreren Anforderungsschritten.
  - Eine einzelne *Anforderungs-ID* wird für alle Anforderungsschritte verwendet.
  - Der erste Schritt, Anforderungssequenz 0, einer Transaktion gibt den aktuellen Status der gesamten Transaktion an.

    Wie in der folgenden Abbildung zu sehen ist, hat der anfängliche Schritt 0 den Gesamtanforderungsstatus *Abgeschlossen*.
- Folgendes kann für die Transaktion durch den einzelnen Anforderungsschritt identifiziert werden:
  - Die Reihenfolge der einzelnen Schritte in einer Transaktion kann anhand der Sequenznummer für den Schritt identifiziert werden.
  - Der Status jeder Transaktion ist durch den Status des Anforderungsschritts sichtbar.
  - Wenn Schritte nach dem ersten Schritt fehlschlagen, hat die Gesamttransaktion den Status Fehlgeschlagen. Wenn alle Schritte abgeschlossen sind, wird der Transaktionsstatus ebenfalls abgeschlossen.

Der folgende Bildschirm ist ein Beispiel für die Art von Informationen, die mit einer Schlüsselrotation ServiceNow angezeigt werden.



Request ID	Request action	Request status	Request sequence	Request step	Request step status
801eee50c3133010cf37169d7940ddf7	Key Rotation	Completed	0		
801eee50c3133010cf37169d7940ddf7	Key Rotation		1	request_preparation	Completed
801eee50c3133010cf37169d7940ddf7	Key Rotation		2	request_integrity_check	Completed
801eee50c3133010cf37169d7940ddf7	Key Rotation		3	request_validation	Completed
801eee50c3133010cf37169d7940ddf7	Key Rotation		4	hsm_servicenow_upload	Completed
801eee50c3133010cf37169d7940ddf7	Key Rotation		5	key_metadata_rotate	Completed
801eee50c3133010cf37169d7940ddf7	Key Rotation		6	post_rotate_request	Completed
801eee50c3133010cf37169d7940ddf7	Key Rotation		7	post_rotate_response	Completed

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle werden die Feldinformationen angezeigt, die auf der Seite „Schlüsselverwaltungstransaktionen“ verfügbar sind.

Transaktionen der Schlüsselverwaltung

Feld	Beschreibung
Anforderungs-ID	Eindeutige vom System generierte ID für die ausgeführte Aktion Eine Anforderungs-ID wird für alle Anforderungsschritte verwendet.
Anforderungsaktion	Zeigt die Aktion für den ausgeführten Tastenvorgang an.
Anforderungsstatus	• Wird verarbeitet: Eine Anforderung wurde eingegeben, sie wurde jedoch noch nicht abgeschlossen. • Abgeschlossen: Die Anforderung wurde erfolgreich abgeschlossen. • Fehlgeschlagen: Ein Problem ist aufgetreten, und der Prozess wurde nicht abgeschlossen. **Hinweis:** Wenden Sie sich an Kundenservice und Support, und geben Sie die Anforderungsnummer an, bei der der Fehler aufgetreten ist.
Schlüssel-Alias	Alphanumerischer Eintrag.
Status des Schlüssellebenszyklus	Definitionen finden Sie unter Schlüssel-Lebenszyklusstatus des Key Management Framework.
Quelle	• ServiceNow Schlüssel • Vom Kunden verwalteter Schlüssel
Schlüsselversion	Wenn ein Schlüssel rotiert, wird die Versionsnummer erhöht.
Anforderungssequenz	Zeigt die Reihenfolge an, in der eine Anforderung im System verarbeitet wird.
Anforderungsschritt	Zeigt an, ob während der Schlüsselrotation ein Schritt im System verarbeitet wird. Die Anzahl und der Inhalt der Schritte variieren je nach Art der durchgeführten Schlüsseloperation. 1. request_preparation: Erstellt eine Anforderung zum Auslösen sowie für Umbruch und Rotation. 2. request_integrity_check: Validiert, dass die Anforderung berechtigt und sicher ist. 3. request_validation: Validiert, dass eine Anforderung ausgeführt wird. Es kann jeweils nur eine Rotationsanforderung verarbeitet werden. 4. attachment_process: Extrahiert das umschlossene Schlüsselmaterial aus dem Anhang. (Zusätzlicher Schritt beim Rotieren eines kundenverwalteten Schlüssels.) 5. HSM<key type> _upload: Lädt das umschlossene Schlüsselmaterial in HSM, KeySecure, hoch. 6. key_metadata_rotate: Generiert die neuen Schlüsselmetadaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transaktionen der Schlüsselverwaltung (Fortsetzung)

Feld	Beschreibung
	7. post_rotate_request: Sendet eine Anforderung zum Ausführen der Schlüsselrotation. 8. post_rotate_response: Antwort, um die Schlüsselrotation basierend auf der Anforderung der Kundeninstanz durchzuführen. **Hinweis:** Geben Sie den Anforderungsschritt an Kundenservice und Support weiter, um den Statusverlauf zu analysieren, falls ein Anforderungsschritt nicht abgeschlossen wird.
Anforderungsschritt-Status	• Abgeschlossen: Rotation ist erfolgreich. • Fehlgeschlagen: Rotation ist nicht erfolgreich. **Hinweis:** Geben Sie den Anforderungsschritt an Kundenservice und Support weiter, um den Statusverlauf zu analysieren, falls ein Anforderungsschritt nicht abgeschlossen wird.

Cloud Encryption-Protokollierung

Erfahren Sie mehr über Protokollierungsoptionen für Cloud-Verschlüsselung.

Cloud Encryption-Protokollierungstabellen

Verwenden Sie diese Tabellen, um Protokollierungsinformationen zu Cloud Encryption-Transaktionen in Ihrer Instanz zu finden.

Tabelle	Beschreibung
Cloud Encryption-Metadaten [dare_key_metadata]	Cloud Encryption Metadata erfasst wichtige Metadaten der Lebenszyklusverwaltung. In dieser Tabelle finden Sie wichtige Lebenszyklus-, Status- und Versionsinformationen. Diese Tabelle wird nach jeder Schlüsseloperation aktualisiert.
Schlüsselverwaltungstransaktionen [dare_key_request]	Schlüsselverwaltungstransaktionen erfasst Informationen zu Schlüsselverwaltungstransaktionen. In dieser Tabelle finden Sie die Protokollierung für jeden Schritt einer Transaktion. Die Tabelle zeichnet alle Fehlerinformationen für eine Transaktion im **Fehlermeldungsfeld** auf.
Sys-Audits [sys_audit]	In der Tabelle „Sys-Audits“ werden Einfügungen und Aktualisierungen für alle geprüften Datensätze in Ihrer Instanz erfasst. In dieser Tabelle finden Sie Änderungen an Datensätzen in Ihrer Instanz, wann die Änderungen vorgenommen wurden und welches Benutzerkonto die Änderung initiiert hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

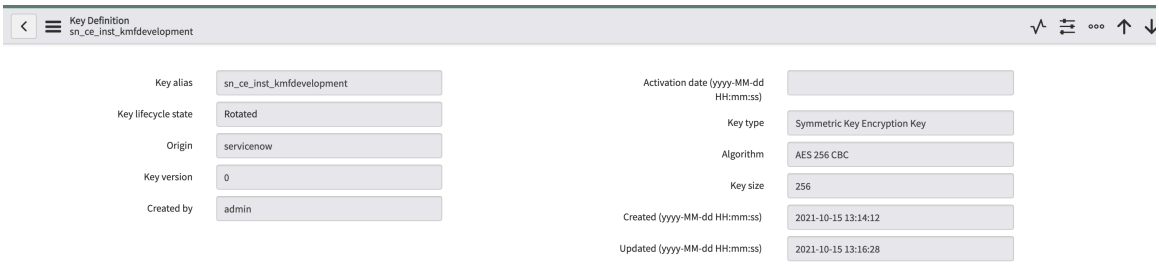
Schlüsselrotationsvorgänge überwachen

Verwenden Sie die Tabelle „Metadaten des Cloud-Verschlüsselungsschlüssels“ [dare_key_metadata], um Informationen zum Lebenszyklus Ihres Schlüssels zu erhalten. In dieser Tabelle finden Sie Informationen wie Herkunft, Aktivierungsdatum, Status und Version Ihrer Schlüssel.

Verwenden Sie die Tabelle „Schlüsselverwaltungstransaktionen“ [dare_key_request], um Transaktionen von Schlüsselvorgängen zu überwachen. In dieser Tabelle finden Sie alle Anforderungen, die sich auf Ihre Schlüssel beziehen, einschließlich Status, Status und Schritt im Prozess, in dem sich die Anforderung befindet. Abgeschlossene Anforderungen werden in dieser Tabelle mit dem Status „ **Abgeschlossen** “ gespeichert.

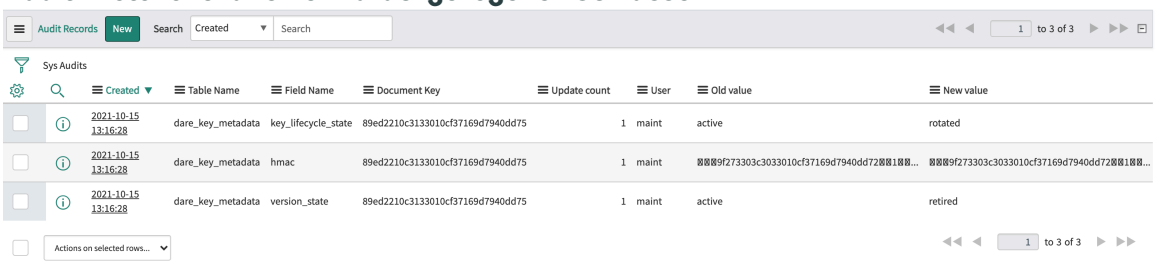
Dieses Beispiel zeigt einen Schlüsselrotationsvorgang. Während dieses Vorgangs wird der alte Schlüssellebenszyklusstatus von „aktiv“ in „rotiert“ und der Versionsstatus von „aktiv“ in „deaktiviert“ aktualisiert.

Schlüsseldefinition für einen rotierten Schlüssel



In der Tabelle „Sys-Audits“ [sys_audit] können Administratoren Änderungen an Datensätzen in der Tabelle „Cloud-Verschlüsselungsschlüssel-Metadaten“ [dare_key_metadata] sehen. Administratoren können sehen, welche Datensätze wann aktualisiert wurden. Die Protokolleinträge zeichnen auch das geänderte Feld sowie die alten und neuen Werte auf.

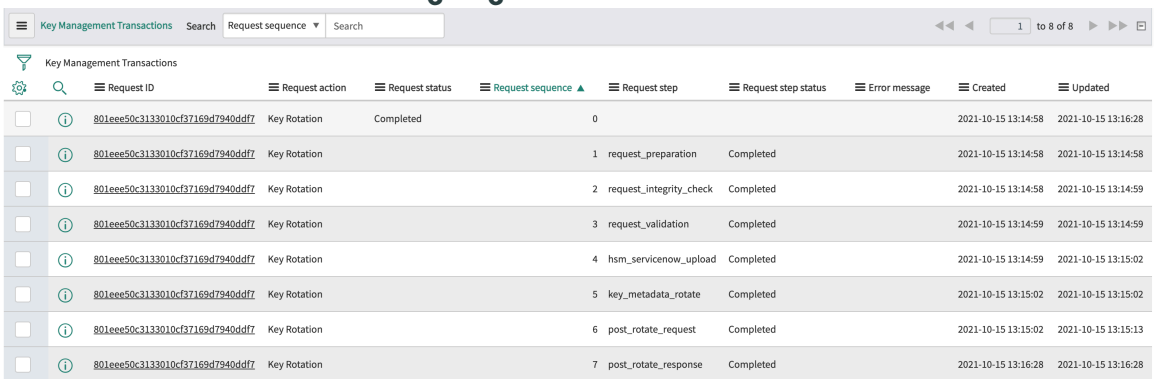
Audit-Protokolle für einen zurückgezogenen Schlüssel



Administratoren können die Datensätze in der Tabelle „Cloud-Verschlüsselungsschlüssel-Metadaten“ [dare_key_metadata] anzeigen. In den folgenden Audit-Datensätzen wurde der Anforderungsstatus von „In Verarbeitung“ in „Abgeschlossen“ geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Protokolle für einen zurückgezogenen Schlüssel



Key Management Transactions — Search: Request sequence — 1 to 8 of 8

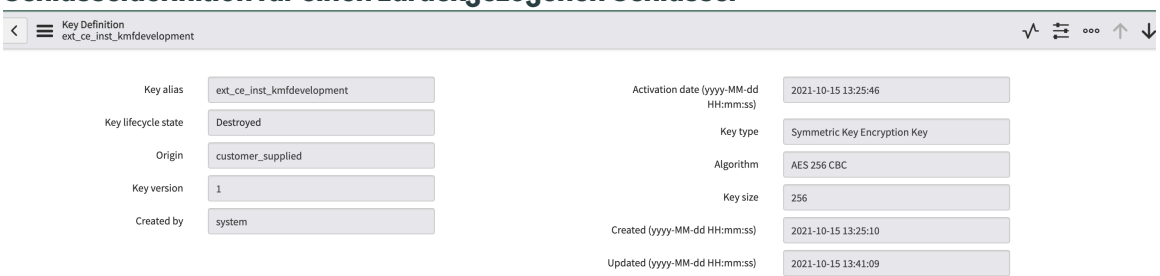
Request ID	Request action	Request status	Request sequence	Request step	Request step status	Error message	Created	Updated
801eee50c3133010cf37169d7940ddf7	Key Rotation	Completed	0				2021-10-15 13:14:58	2021-10-15 13:16:28
801eee50c3133010cf37169d7940ddf7	Key Rotation		1	request_preparation	Completed		2021-10-15 13:14:58	2021-10-15 13:14:58
801eee50c3133010cf37169d7940ddf7	Key Rotation		2	request_integrity_check	Completed		2021-10-15 13:14:58	2021-10-15 13:14:59
801eee50c3133010cf37169d7940ddf7	Key Rotation		3	request_validation	Completed		2021-10-15 13:14:59	2021-10-15 13:14:59
801eee50c3133010cf37169d7940ddf7	Key Rotation		4	hsm_servicenow_upload	Completed		2021-10-15 13:14:59	2021-10-15 13:15:02
801eee50c3133010cf37169d7940ddf7	Key Rotation		5	key_metadata_rotate	Completed		2021-10-15 13:15:02	2021-10-15 13:15:02
801eee50c3133010cf37169d7940ddf7	Key Rotation		6	post_rotate_request	Completed		2021-10-15 13:15:02	2021-10-15 13:15:13
801eee50c3133010cf37169d7940ddf7	Key Rotation		7	post_rotate_response	Completed		2021-10-15 13:16:28	2021-10-15 13:16:28

Protokollierung für Schlüsselentzugsvorgänge

Protokollierungsinformationen zum Zurückziehen des Schlüssels werden in der Tabelle „Audits“ [sys_audit] gespeichert. Diese Protokollierungsinformationen enthalten Informationen darüber, wer die Schlüsselentnahme initiiert hat und wann sie erfolgt ist.

Dieses Beispiel zeigt einen Schlüsselentzugsvorgang. Während dieses Vorgangs wird der Schlüssellebenszyklusstatus von „Generiert“ über „Aktiv“ und „Vernichtet“ aktualisiert. Die Schlüsselversion wird von „unbekannt“ über „aktiv“ auf „deaktiviert“ aktualisiert.

Schlüsseldefinition für einen zurückgezogenen Schlüssel

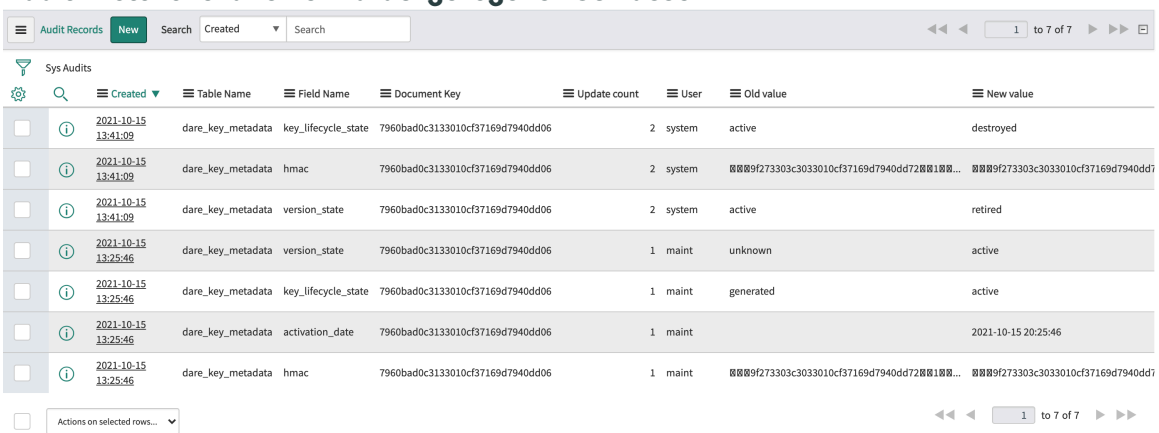


Key Definition
ext_ce_inst_kmfdevelopment

Key alias	ext_ce_inst_kmfdevelopment	Activation date (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:25:46
Key lifecycle state	Destroyed	Key type	Symmetric Key Encryption Key
Origin	customer_supplied	Algorithm	AES 256 CBC
Key version	1	Key size	256
Created by	system	Created (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:25:10
		Updated (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:41:09

Mit Blick auf die Tabelle „Sys-Audits“ [sys_audit] können Administratoren die Tabelle „Cloud-Verschlüsselungsschlüssel-Metadaten“ [dare_key_metadata] ändern.

Audit-Protokolle für einen zurückgezogenen Schlüssel



Audit Records — New — Search: Created — 1 to 7 of 7

Sys Audits

Created	Table Name	Field Name	Document Key	Update count	User	Old value	New value
2021-10-15 13:41:09	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	2	system	active	destroyed
2021-10-15 13:41:09	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	2	system	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7
2021-10-15 13:41:09	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	2	system	active	retired
2021-10-15 13:25:46	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	1	maint	unknown	active
2021-10-15 13:25:46	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	1	maint	generated	active
2021-10-15 13:25:46	dare_key_metadata	activation_date	7960bad0c3133010cf37169d7940dd06	1	maint		2021-10-15 20:25:46
2021-10-15 13:25:46	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	1	maint	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7

Actions on selected rows... — 1 to 7 of 7

Manipulationserkennung

Verwenden Sie die Manipulationserkennung, um die Sicherheit zu verbessern, indem nicht autorisierte Änderungen an Ihren Quorum-Steuerungseinstellungen erkannt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

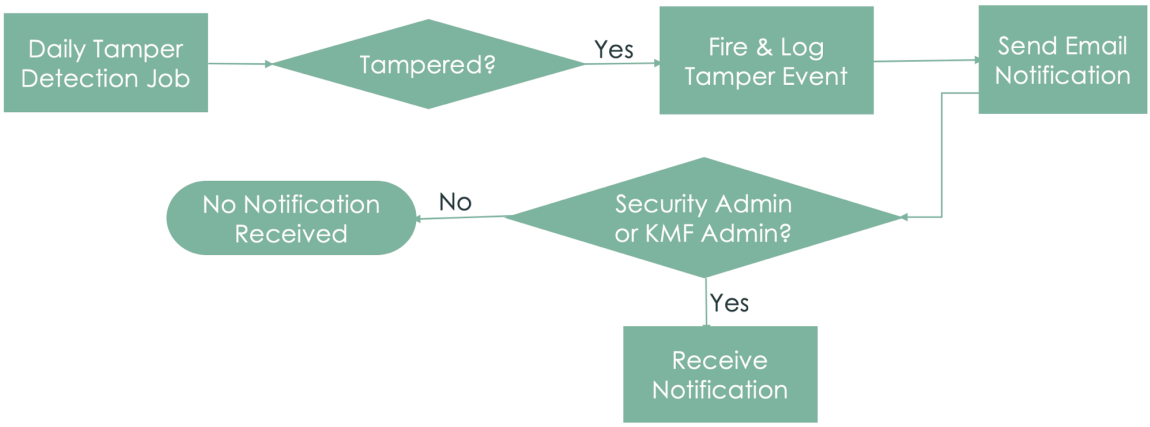
Manipulationserkennungsprozess

Wenn diese Option aktiviert ist, validiert die Manipulationserkennung Ihre Quorum-Steuerungseinstellungen, indem nach nicht autorisierten Änderungen (Manipulationen) gesucht wird. Bei der Manipulationserkennung wird ein Hash-basierter Nachrichtenauthentifizierungscode (HMAC) verwendet.

1. Wenn eine Einstellung geändert oder erstellt wird, erstellt Ihre Instanz einen HMAC. Der HMAC basiert auf dem Wert des Einstellungsdatensatzes (dare_property).
2. Wann immer Ihre Instanz diese Einstellungen verwendet, validiert die Manipulationserkennung sie mithilfe des HMAC.
3. Wenn die Einstellung erfolgreich validiert wird, kann sie von der Plattform verwendet werden, andernfalls nicht.

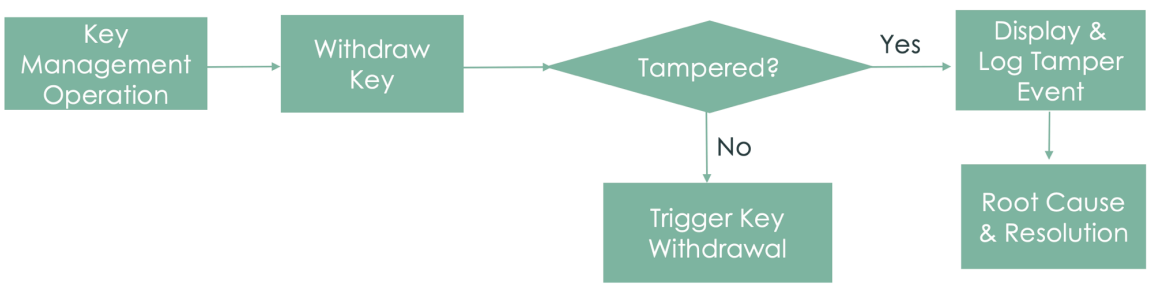
Die Manipulationserkennung wird täglich in Ihrer Instanz ausgeführt

Die Manipulationserkennung überprüft Ihre Einstellungen mithilfe einer täglichen geplanten Aufgabe auf Manipulationen und meldet Validierungsfehler in Ihren Knoten- und Sicherheitsprotokollen. Die Manipulationserkennung sendet eine Benachrichtigung an Sicherheits- und KMF-Administratoren bei Validierungsfehlern.



Die Manipulationserkennung wird ausgeführt, bevor ein Schlüsselentzug ausgeführt wird

Die Manipulationserkennung validiert auch Ihre Eigenschaften, wenn Sie eine Schlüsselentnahme anfordern. Wenn Ihre Einstellungen die Validierung nicht bestehen, wird die Schlüsselentnahme nicht ausgeführt. In diesem Fall müssen Sie alle Validierungsprobleme beheben, bevor der Schlüsselentzug erfolgen kann.



Identifizieren von Manipulationen

Die Manipulationserkennung aktualisiert Ihre Protokolle, wenn die Validierung fehlschlägt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validieren kann, werden diese Fehler in Ihren Knoten- und Sicherheitsprotokollen angezeigt. Der Protokolleintrag enthält die sys_id des Einstellungsdatensatzes (dare_property), dessen Validierung fehlgeschlagen ist.

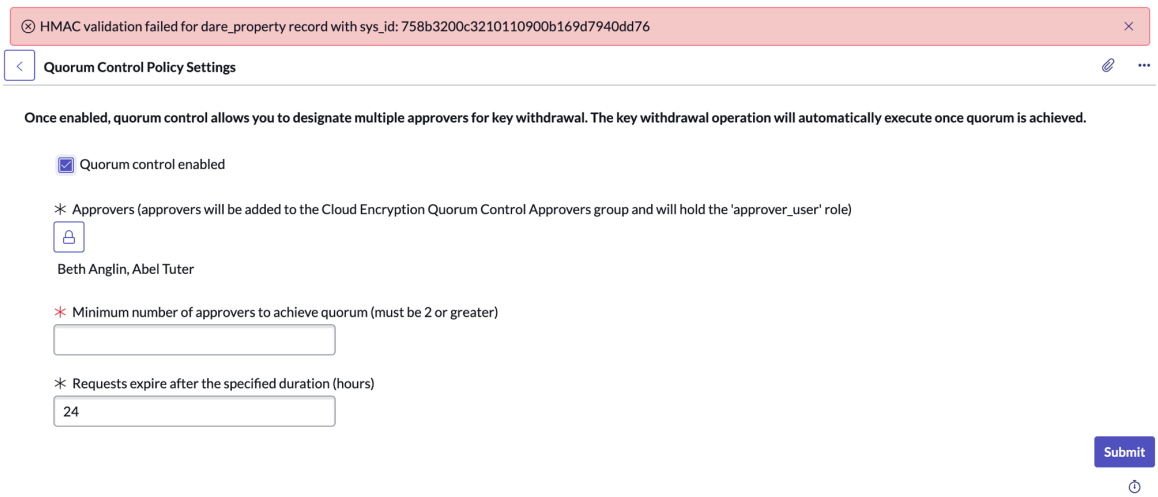
```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 776e3200c3210110900b169d7940dd76 failed HMAC validation

2022-06-28 13:47:35 (264) Default-thread-8
 B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 758b3200c3210110900b169d7940dd76 failed HMAC validation
```

Bei der Protokollierung werden ähnliche Informationen wie in diesen Beispielen angezeigt, wenn die Validierung fehlschlägt. Erfolgreiche Validierungen werden nicht in den Protokollen angezeigt.

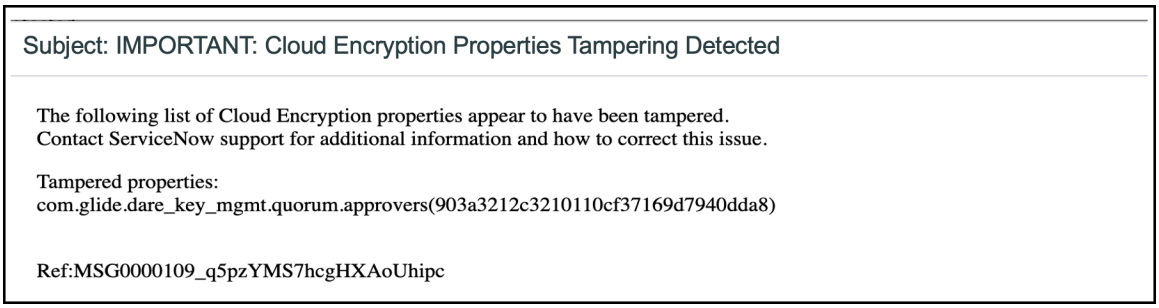
Bei der Manipulationserkennung wird auf der Seite mit den Quorum-Steuerungseinstellungen eine Warnmeldung angezeigt

Wenn die Validierung einer Quorum Control-Einstellung fehlgeschlagen ist, wird auf der Seite mit den Einstellungen für die Quorum Control-Richtlinie in Ihrer Instanz eine Warnung angezeigt. Die Warnung enthält die sys_id des Einstellungsdatensatzes (dare_property), dessen Validierung fehlgeschlagen ist.



Die Manipulationserkennung sendet Benachrichtigungen an Benutzer mit den Rollen `Security Admin` und `KMF Admin`.

Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validiert, erhalten Ihre Sicherheitsadministratoren und KMF-Administratoren eine Benachrichtigung ähnlich wie in diesem Beispiel.

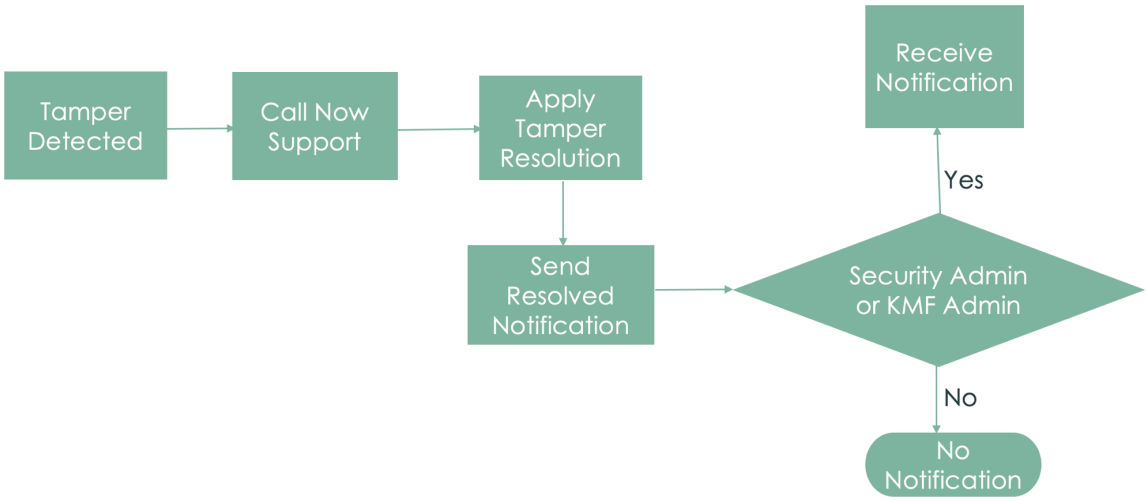


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beheben von Manipulationsproblemen mit ServiceNow Support

Wichtig:
Validierungsfehler bei der Manipulationserkennung können nur mit Hilfe des Supports von ServiceNow behoben werden.



Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validiert, wenden Sie sich an den ServiceNow -Support, um Unterstützung bei der Lösung des Problems zu erhalten. Nachdem ein Support-Mitarbeiter den Validierungsfehler behoben hat, erhalten Sicherheits- und KMF-Administratoren eine Benachrichtigung, dass das Problem gelöst wurde.

Subject: IMPORTANT: Cloud Encryption Properties Reset

At your request, ServiceNow support has reset the following list of Cloud Encryption properties to their default values.
If you did not request this action, contact ServiceNow support immediately.

Reset properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000116_0HAz8U1r59OmppqV8ysg

Datenbankverschlüsselung

ServiceNow® bietet Datenbankverschlüsselungs- (DBE) und Full-Disk-Verschlüsselungsmethoden für Kunden mit gesetzlichen Verpflichtungen zum Datenschutz, die möglicherweise einen Ruhezustandsschutz für alle Daten erfordern.

Wichtig:
Ab Release Washington DC wird die Datenbankverschlüsselung auf die zukünftige Einstellung vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter Cloud-Verschlüsselung mit Schlüsselverwaltung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen der Datenbankverschlüsselung kennen.

Anforderung

Erfahren Sie mehr darüber, wie Sie die Rotation von Datenbankschlüsseln anfordern können.

Referenz

Erfahren Sie mehr über Datenbankverschlüsselung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

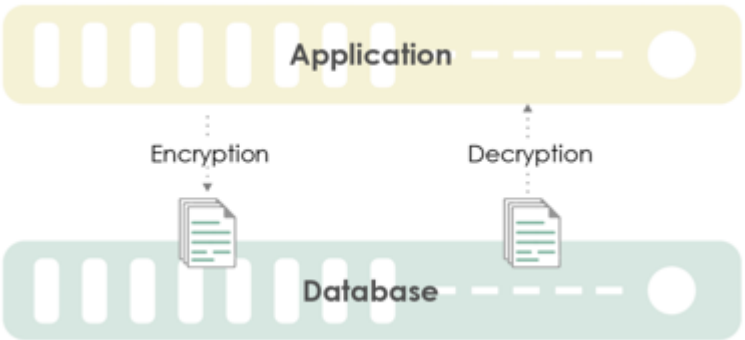
Datenbankverschlüsselung erkunden

ServiceNow® bietet Datenbankverschlüsselungs- (DBE) und Full-Disk-Verschlüsselungsmethoden für Kunden mit gesetzlichen Verpflichtungen zum Datenschutz, die möglicherweise einen Ruhezustandsschutz für alle Daten erfordern.

Wichtig:
Ab Release Washington DC wird die Datenbankverschlüsselung auf die zukünftige Einstellung vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter Cloud-Verschlüsselung mit Schlüsselverwaltung

Die Datenbankverschlüsselung ermöglicht den Schutz aller Daten mit symmetrischer AES-256-Verschlüsselung, unabhängig davon, ob die Datenbank online oder offline ist. Aus der Perspektive Now Platform fließen alle Daten in entschlüsselt.

- Die Datenbankverschlüsselung unterstützt die Verschlüsselung aller gespeicherten Daten in Echtzeit und bietet Schutz für Daten online und offline ohne Funktionalitätsverlust.
- Die vollständige Festplattenverschlüsselung schützt Offline-Daten bei Verlust oder Diebstahl der Festplatte.

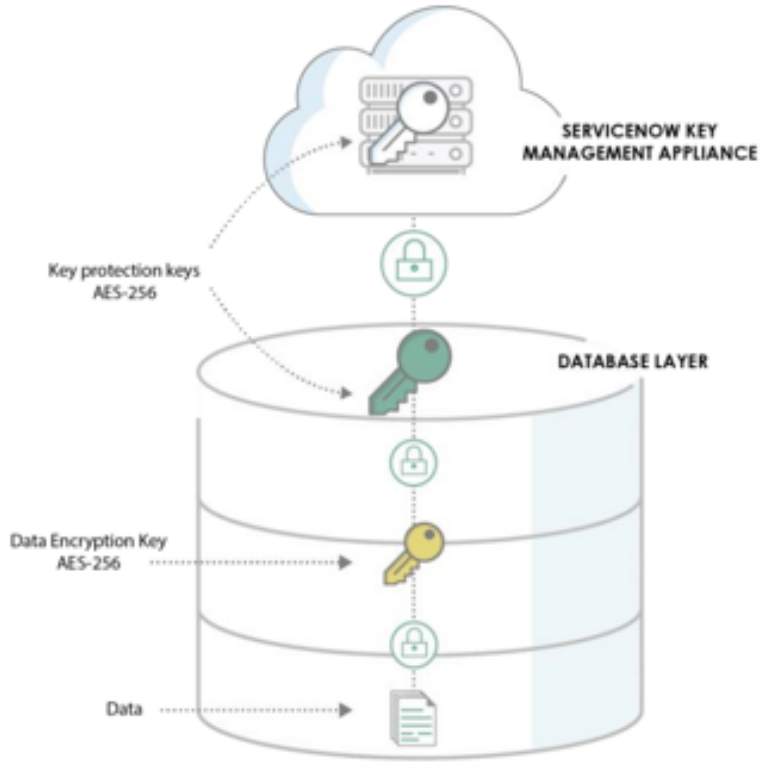


Bei der Datenbankverschlüsselung werden alle gespeicherten Daten verschlüsselt, und einzelne Datensätze oder Tabellen werden beim Zugriff im Speicher entschlüsselt. Neue oder geänderte Daten werden verschlüsselt, wenn sie in eine Tabelle eingegeben werden, und zugehörige Aktivitätsprotokolldateien (bin, redo, undo und error) werden ebenfalls verschlüsselt.

Die Datenbankverschlüsselung ist für Benutzer transparent, ohne Funktionalitätsverlust. Bei Verwendung dieser Funktion werden alle Instanzen zusammen mit dem Replikationsdatenverkehr und den Sicherungen verschlüsselt. Das Klonen von Instanzen ist weiterhin verfügbar, mit einer geringfügigen Auswirkung auf die Leistung bei Verwendung der Datenbankverschlüsselung von bis zu 5 %. Sowohl neue als auch vorhandene Instanzen in unterstützten Releases von Now Platform können die Datenbankverschlüsselung nutzen.

Wie dargestellt, speichert und verwaltet ServiceNow Schlüssel mithilfe einer dreistufigen Schlüsselhierarchie:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



1. Ein kundenspezifischer AES-256-Schlüssel wird von der Datenbank-Engine erstellt und zum Verschlüsseln der Daten verwendet.
2. Ein zweiter kundenspezifischer AES-256-Schlüssel wird von der Datenbank-Engine erstellt und zum Schutz des Schlüssels der ersten Ebene verwendet.
3. Ein dritter AES-256-Schlüssel wird von erstellt und in mit FIPS 140 validierten Schlüsselverwaltungsgeräten in den ServiceNow -Rechenzentren gespeichert. Dieser Schlüssel schützt den Schlüssel der zweiten Ebene und ist pro Kundeninstanz eindeutig.

Now Platform unterstützt auch die Datenbankverschlüsselung mit einem vom Kunden bereitgestellten Switch, DBE mit CCS. Dies ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie in der Datenbank nicht verwendet werden. Es verwendet die AES-Verschlüsselung nach Branchenstandard, ohne die Funktionalität zu beeinträchtigen. Die Datenbank verschlüsselt Daten beim Schreiben auf den Datenträger und entschlüsselt Daten beim Lesen vom Datenträger. Das bedeutet, dass Anwendungen die Daten immer in einem unverschlüsselten Zustand haben, um die erforderliche Logik und Funktionen ohne Auswirkungen auszuführen.

Hinweis:
Datenbankverschlüsselung wird für lokale Instanzen nicht unterstützt.

Wenn Sie Ihre eigenen Schlüssel für die Datenbankverschlüsselung verwenden, finden Sie weitere Informationen unter Datenbankverschlüsselung mit kundengesteuertem Switch.

Datenbankschlüsselrotation wird angefordert

Rotieren Sie den Datenbankschlüssel jährlich oder nach Bedarf, indem Sie eine Anforderung an den Support senden.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Ab Release Washington DC wird die Datenbankverschlüsselung auf die zukünftige Einstellung vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter Cloud-Verschlüsselung mit Schlüsselverwaltung

Warum und wann dieser Vorgang ausgeführt wird

Die Schlüsselrotation erfolgt innerhalb von 24 Stunden vor dem Ablaufdatum in der Nacht, wobei der Service für die Instanz nicht unterbrochen wird.

Hinweis:
Derzeit ist die Schlüsselrotation nur in den Umgebungen ServiceNow Kommerziell, Government Community Cloud (GCC), Frankreich und Singapur verfügbar.

Prozedur

Wenden Sie sich an Kundenservice und Support, um eine der folgenden Schlüsselrotationsaktionen anzufordern:

- Registrieren Sie sich, um die jährliche Schlüsselrotation für alle festgelegten Instanzen durchzuführen.
- Rufen Sie einen Verlaufsbericht der letzten drei Schlüsselrotationen ab, der Folgendes enthält:
  - Instanzname.
  - Name und Version des Schlüssels
  - Datum und Uhrzeit der Rotation.
- Planen Sie eine frühe Schlüsselrotation außerhalb der geplanten jährlichen Rotation.

Datenbankverschlüsselung mit kundengesteuertem Switch

Datenbankverschlüsselung mit kundengesteuertem Switch (DBE with CCS) ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie in der Datenbank nicht verwendet werden.

Wichtig:
Ab Release Washington DC wird die Datenbankverschlüsselung auf die zukünftige Einstellung vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter Cloud-Verschlüsselung mit Schlüsselverwaltung

Übersicht

Die Datenbankverschlüsselung mit kundengesteuertem Switch verwendet die branchenübliche AES-Verschlüsselung, ohne die Funktionalität zu beeinträchtigen. Die Datenbank verschlüsselt Daten, wenn sie auf den Datenträger geschrieben und von der Datenbank entschlüsselt werden, wenn sie vom Datenträger gelesen werden. Anwendungen haben die Daten immer in einem unverschlüsselten Zustand, um die erforderliche Logik und Funktionen auszuführen.

DBE-CCS nutzt die native Technologie der Datenbank, die häufig als Tablespace Encryption oder transparente Datenverschlüsselung bezeichnet wird. Weitere Informationen zur Technologie finden Sie auf der MariaDB-Website unter „Tablespace Encryption“.

Für DBE-CCS müssen Sie einen HTTPS-REST-Serviceendpunkt einrichten, der regelmäßig den geheimen Schlüssel für die Instanz ServiceNow bereitstellt. Der CCS-Endpunkt gibt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dann den geheimen Kundenschlüssel zurück, der mit dem öffentlichen Schlüssel der Datenbankinstanz verschlüsselt ist.

Kundenendpunkt

Wichtig:
Ihre Organisation ist für die Einrichtung und Wartung Ihres CCS-Endpunkts allein verantwortlich. Die Kundenendpunktspezifikation wird in KB0789788 bereitgestellt.

Ein ServiceNow -Technologiepartner, Fortanix, ist verfügbar, um Ihren Kundenendpunkt für Sie zu implementieren. Wenden Sie sich direkt an den Technologiepartner, um Details zur Integration zu erhalten. Weitere Informationen finden Sie unter Fortanix Data Security Manager mit ServiceNow verwenden .

Unterstützung mehrerer ServiceNow -Versionen

Wichtig:
Datenbankverschlüsselung ist ein kostenpflichtiges Infrastrukturangebot, das unabhängig vom Release ist. Sie kann auf jedes unterstützte Release und auf neue oder vorhandene Instanzen angewendet werden.

Andere Referenzen

In den folgenden Referenzen finden Sie weitere Informationen zu DBE mit CCS:

Referenz	Beschreibung
KB0993681	Architektur des vom Kunden gesteuerten Switch für Datenbankverschlüsselung
KB0789788	Implementierungsleitfaden für DBE mit CCS

Hinweis:
Um auf KB-Artikel zugreifen zu können, müssen Sie sich zuerst bei Now Supportauthentifizieren.

Vollständige Festplattenverschlüsselung

Full Disk Encryption (FDE) wendet die Verschlüsselung nur auf das gesamte Speichersystem innerhalb des Datenbankservers an, da dies die einzige Komponente ist, die Kundendaten speichert. FDE schützt nur vor physischem Verlust oder Diebstahl von Speichergeräten. Wenn verschlüsselte Festplattenserver eingeschaltet sind und Daten bereitstellen, bietet die Verschlüsselung keinen zusätzlichen Schutz.

Vollständige Festplattenverschlüsselung

Die vollständige Festplattenverschlüsselung kann für stark regulierte Organisationen relevant sein, kann jedoch die Bereitstellung eines Kunden ServiceNow erheblich kosten. Von ServiceNow getroffene Maßnahmen zur Minimierung von Verlust oder Diebstahl von Speichergeräten können ebenfalls ein Faktor bei der Auswahl sein.

Aus der Perspektive Now Platform fließen alle Daten in entschlüsselt.

Kommerzielle Umgebungen verwenden Full Disk Encryption (FDE) mit Hardware oder Speichergeräten, die nach FIPS 140 validiert sind und sich im Validierungsprozess befinden, zusammen mit einer dedizierten Hardwareoption ServiceNow. FDE gilt für die Hardware

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

selbst und bietet daher eine Verschlüsselung im Ruhezustand für alle Daten, die in jeder Ihnen zugewiesenen Instanz gespeichert sind.

Weitere Informationen zur Auswahl von FDE und dedizierten Hardwareoptionen erhalten Sie von Ihrem ServiceNow.

Edge Encryption

ServiceNow® Edge Encryption ™ verschlüsselt vertrauliche Daten in Ihrem Unternehmen, bevor sie über das Internet an Ihre ServiceNow -Instanz gesendet werden (Verschlüsselung während des Vorgangs), wo sie im Ruhezustand verschlüsselt bleiben.

Erkunden

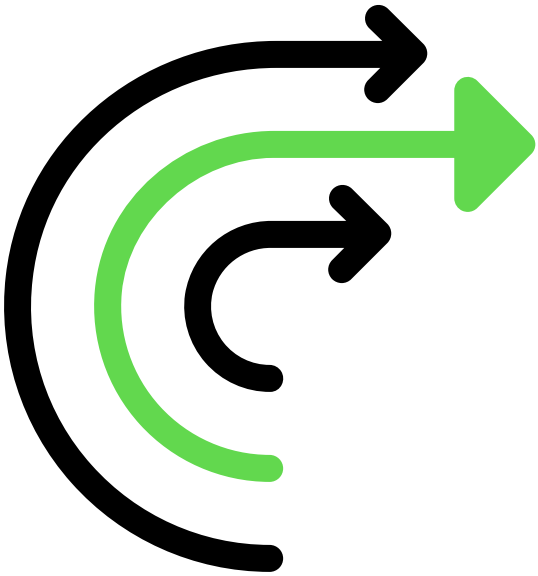
Lernen Sie die Funktionen und den Geschäftsnutzen von Edge Encryption kennen.

Planen

Machen Sie sich mit der Planung von Edge Encryption vertraut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren



Installieren Sie Edge Encryption.

Edge Encryption wird aktualisiert

Upgrade-

Erfahren Sie, wie Sie Edge Encryption aktualisieren.

Konfigurieren

Machen Sie sich mit der Konfiguration von Edge Encryption vertraut.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Encryption erkunden

Edge Encryption ist ein Netzwerkverschlüsselungssystem in Ihrem Netzwerk, das vertrauliche Daten während der Übertragung zwischen Ihrem Rechenzentrum und der ServiceNow-Cloud verschlüsselt und entschlüsselt.

Edge Encryption – Beschreibung

Edge wird auch als „clientseitige“ Verschlüsselung bezeichnet und erfordert, dass der gesamte bidirektionale Benutzerverkehr über Proxys geleitet wird, die in Ihrer Infrastruktur verwaltet werden. Sie haben die vollständige Kontrolle über Ihre Schlüsselverwaltung, da die Schlüssel in Ihrem Proxy in Ihrer Infrastruktur gespeichert werden. Now Platform kann Ihren Geheimtext nicht entschlüsseln, um auf Ihre Schlüssel zuzugreifen.

Die Funktion Edge Encryption ist eine zusätzliche Kostenoption, mit der Sie die End-to-End-Verschlüsselung Ihrer Daten und die Schlüsselverwaltung steuern können. Edge Encryption verwendet eine Proxy-Anwendung, die von ServiceNow bereitgestellt und von Ihnen in Ihrem eigenen Netzwerk installiert wird. Diese Proxy-Anwendung tokenisiert bestimmte Datenmuster oder verschlüsselt Zeichenfolgenfelder, Datumsfelder, Datums-/Uhrzeitfelder und Anhangdaten, bevor sie von Ihrer Umgebung an Ihre Instanz gesendet werden. Die Proxy-Anwendung entschlüsselt dieselben Daten ebenfalls nur innerhalb Ihres eigenen Netzwerks mit Schlüsseln, die nur in Ihrem eigenen Netzwerk gespeichert sind.

Die relevanten Verschlüsselungsschlüssel und die Konfiguration sind nur auf dem Edge-Proxy in Ihrem Netzwerk vorhanden und für ServiceNownicht sichtbar. Die Daten werden ab dem Moment verschlüsselt, in dem sie Ihre Umgebung verlassen, und erst beim Abruf entschlüsselt. Zu keinem Zeitpunkt sind die Daten im Nur-Text-Format für Systeme oder Mitarbeiter von ServiceNow zugänglich.

Edge Encryption – Benutzer

Nur ein Benutzer, der über einen Proxy-Server in Ihrem Netzwerk bei der Instanz angemeldet ist, kann verschlüsselte Daten im Klartext anzeigen. Ebenso kann Edge Encryption nur von einem security_admin-Benutzer konfiguriert und verwaltet werden, der sich über einen Proxy-Server in Ihrem Netzwerk bei einer Instanz angemeldet hat.

Da sich der Proxyserver in Ihrem Netzwerk befindet, besitzen und verwalten Sie die Verschlüsselungsschlüssel, und sie werden nie an die Instanz gesendet. Daher werden vertrauliche Daten von ServiceNow niemals im Klartext angezeigt.

Zusätzlich zur Konfiguration des Edge-Proxy und zur Verwaltung von Regeln sind Sie für die üblichen Anforderungen für den Betrieb eines Servers in Ihrer Umgebung verantwortlich (einschließlich Hosting, Routing, Sicherung, DNS-Konfiguration usw.), um Ihre Edge-Proxys zu aktivieren und zu unterstützen.

Verschlüsselung und Tokenisierung

Edge Encryption unterstützt sowohl die Verschlüsselung (durch Verschlüsselungskonfigurationen) als auch die Tokenisierung (durch Verschlüsselungsmuster) für den Schutz Ihrer vertraulichen Informationen.

Verschlüsselungskonfigurationen

Sie können einzelne Felder mit Verschlüsselungskonfigurationen verschlüsseln. Edge Encryption unterstützt AES mit 128-Bit- und 256-Bit-Verschlüsselungsschlüsseln. Edge Encryption unterstützt standardmäßige, gleichstellungserhaltende und ordnungserhaltende Verschlüsselungstypen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neben Anlagen können Sie folgende Feldtypen verschlüsseln:

- Datum
- E-Mail
- Datum/Uhrzeit
- HTML
- IP-Adresse
- Journal
- Journaleingabe
- Mehrzeiliger Text
- Einzeiliger Text
- Zeichenfolge
- URL

Hinweis:

Wenn dem Aktivitätsstrom ein Journal Feld hinzugefügt wird, das für die Verschlüsselung markiert ist, werden alle Benutzereingaben in das Feld im Aktivitätsstrom verschlüsselt.

Multi-Byte-Zeichen innerhalb der unterstützten Feldtypen können verschlüsselt werden.

Sie können auch die folgenden Servicekatalog-Variablentypen verschlüsseln:

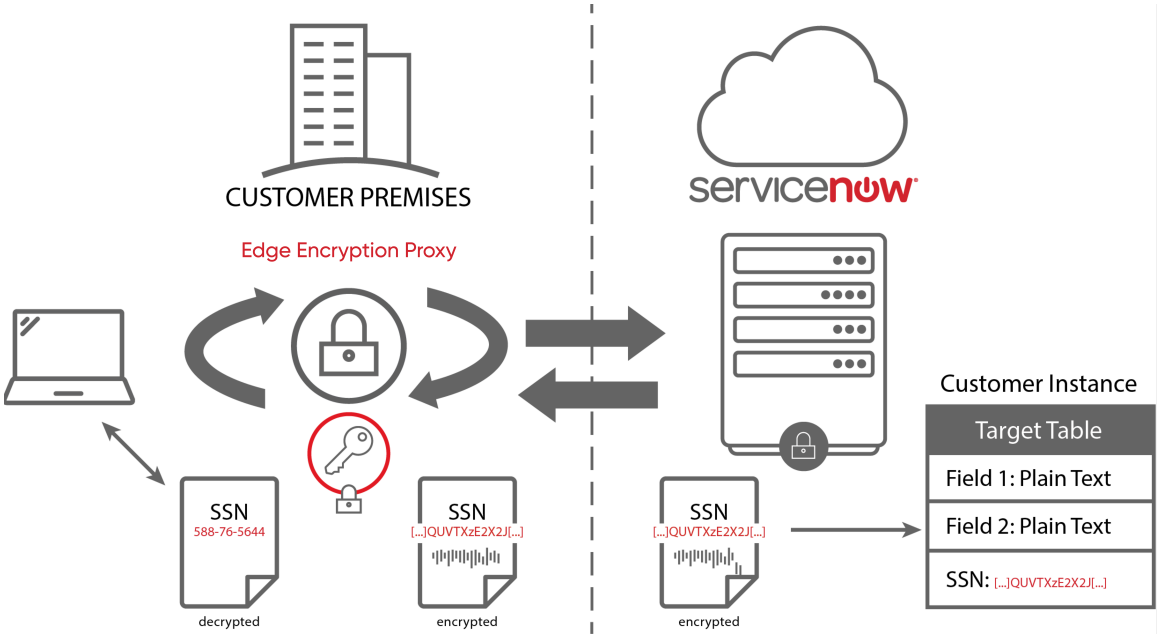
- Zeichenfolgentypen
  - Einzeiliger Text
  - Mehrzeiliger Text
  - Breite einzeilige Textzeile
- Datum
- Datum/Uhrzeit
- URL
- E-Mail
- HTML
- IP-Adresse

Verschlüsselungsmuster

Sie können Verschlüsselungsmuster verwenden, um Zeichenketten zu tokenisieren, die regulären Mustern wie Sozialversicherungs- und Kreditkartennummern entsprechen. Verschlüsselungskonfigurationen sollten zwar die primäre Verschlüsselungsmethode sein, verwenden Sie jedoch Verschlüsselungsmuster als Ergänzung, um vertrauliche Informationen außerhalb verschlüsselter Felder zu schützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Der Edge Encryption Proxy-Server erfordert nur eine MySQL-Datenbank in Ihrem Netzwerk, wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden. Klartextwerte werden in der Proxy-Datenbank in Ihrem Netzwerk gespeichert. Aus diesem Grund ist es wichtig, dass Sie Ihre Proxy-Datenbank schützen und regelmäßig sichern. Empfehlungen finden Sie unter Komponenten der Edge Encryption.



Edge Encryption auf Now Platform

Edge Encryption fungiert als Gateway zwischen Ihrem Browser und Ihrer ServiceNow-Instanz. Der Datenverkehr Ihres Browsers wird durch das Gateway auf dem Weg zur ServiceNow-Instanz. Das Gateway wiederum ist so konfiguriert, dass ausgehende Daten, die zur Verschlüsselung markiert sind, verschlüsselt werden. Eingehender Datenverkehr wird über das Gateway entschlüsselt, und der Endbenutzer sieht im Browser Klartext. Der Vorteil dieser Implementierung in Bezug auf die Sicherheitskontrolle besteht darin, dass die Verschlüsselung und die Schlüsselverwaltung extern über ServiceNow erfolgen.

Vor- und Nachteile

Wie bei Verschlüsselung auf Spaltenebene Enterprise und der Verschlüsselung auf Spaltenebene führt Edge Encryption aufgrund der zusätzlichen Sicherheit zu funktionalen Einschränkungen innerhalb einer Instanz. Der lokale Edge-Proxy bietet jedoch auch einige zusätzliche Funktionen im Zusammenhang mit der Sortierung im Vergleich zur Verschlüsselung auf Spaltenebene.

Vorteile:

- Edge Encryption bietet absolute Kontrolle darüber, wer Ihre Informationen sieht, und verhindert Datenschutzverletzungen.
- Informationen verbleiben auf Ihrem Proxy-Server und verlassen Ihr Netzwerk nie unverschlüsselt.
- Informationen werden während der Übertragung verschlüsselt, bevor sie die Instanz ServiceNow erreichen.
- Sie besitzen und verwalten alle Ihre eigenen Verschlüsselungsschlüssel. Niemand sonst, nicht einmal Mitarbeiter von ServiceNow, kann auf Ihre Schlüssel zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können die Stärke des Verschlüsselungsalgorithmus auswählen: AES-128 oder AES-256.
- Edge Encryption bietet die Möglichkeit, Zeichenfolgen, Datums- und Datums-/Uhrzeitfelder, Anhänge, URLs und Journale zu verschlüsseln.
- Edge Encryption bietet Standard-, Equal- und Order-Preserving-Verschlüsselung von Daten im Ruhezustand innerhalb der Datenbank und der Instanz.
- Mit Verschlüsselungsregeln können Sie benutzerdefinierte Skripts schreiben, die dem Proxy-Server genau mitteilen, was verschlüsselt werden soll und wo diese verschlüsselten Informationen in der Instanz abgelegt werden sollen. Diese Skripts sind nützlich, wenn die Datenstruktur nicht genau mit der Instanz ServiceNow übereinstimmt.
- Mit Verschlüsselungsmustern können Sie Informationen wie Passwörter tokenisieren.

Nachteile:

- Edge Encryption erfordert einen zusätzlichen Netzwerk-Hop durch das Edge-Proxy-Cluster und zusätzliche Verarbeitung, was den Datenverkehr verzögern kann. Die zusätzliche Verarbeitungsverzögerung der Anwendung Edge Encryption ist im Vergleich zum Netzwerk-Hop vernachlässigbar.
- Die Verwaltung eigener Verschlüsselungsschlüssel kann komplex und zeitaufwändig sein.
- Sie können maximal zwei Schlüssel verwalten, ohne die Flexibilität zu haben, unterschiedliche Schlüssel für verschiedene Teilmengen von Spalten/Daten oder für verschiedene Rollen zu definieren usw
- Edge Encryption hat den Nebeneffekt, dass der Server oder die Plattform die Daten nicht entschlüsseln kann, um die entschlüsselten Daten zu manipulieren. Daher können Funktionalität und Datenverarbeitung auf Now Platform beim Verschlüsseln von Spalten mit Edge Encryption eingeschränkt sein.

Was Sie wissen müssen, bevor Sie beginnen

Da Verschlüsselung und Tokenisierung die Art Ihrer Daten ändern, kann Edge Encryption sich auf andere Instanzprozesse auswirken. Prüfen Sie vor der Nutzung von Edge Encryption sorgfältig die Auswirkungen auf Ihre Instanz.

Da der Proxy-Server in Ihrem Netzwerk installiert und verwaltet wird, erfordert Edge Encryption eine Netzwerkadministration und -verwaltung. Überprüfen Sie die Netzwerkanforderungen, um eine reibungslose Implementierung sicherzustellen.

Lesen Sie die folgenden Themen, um die Auswirkungen nachzuvollziehen, die Edge Encryption auf Ihre Instanz hat:

- Die Edge Encryption planen
- Edge Encryption-Systemanforderungen
- Umgebungsgröße Ihrer Edge Encryption anpassen
- Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen
- Edge Encryption – Einschränkungen
- Schlüsselverwaltung für Edge Encryption

Komponenten der Edge Encryption

Edge Encryption besteht aus dem Edge Encryption Proxy-Server, der auf einem Server in Ihrem Netzwerk ausgeführt wird, und dem Edge Encryption Plugin, das auf Ihrer ServiceNow-Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

installiert werden muss. Wenn Sie Verschlüsselungstypen oder Verschlüsselungsmuster mit Ordnungserhaltung verwenden, muss auch eine Proxy-Datenbank in Ihrem Netzwerk installiert sein.

Proxy-Anwendung

Beim Durchlaufen des Proxyservers Edge EncryptionEdge Encryption können Sie mit dem Plugin [] angeben, welche Felder, Muster und Anhänge verschlüsselt werden sollen. Sie können auch Verschlüsselungsregeln verwalten, um bestimmte Anforderungen zu verschlüsseln, und Massenverschlüsselungsaufgaben planen.

Proxy-Server

Der Edge Encryption -Proxy-Server verwendet Verschlüsselungsregeln, um in einer HTTP-Anforderung zu identifizieren, was, wenn überhaupt, verschlüsselt werden muss, und verschlüsselt es, bevor die Anforderung an die Instanz weitergeleitet wird. Zur Entschlüsselung überprüft der Proxyserver Edge Encryption die HTTP-Antworten auf verschlüsselte Daten und entschlüsselt sie, bevor die Antwort an den Client zurückgesendet wird. Damit diese Entschlüsselung erfolgt, müssen alle HTTP-Anforderungen und -Antworten den Proxy-Server Edge Encryption durchlaufen. Diese HTTP-Anforderungen umfassen alle Anforderungen, die von einem Browser stammen, sowie SOAP- oder REST-Anforderungen.

Proxy-Datenbank

Wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden, verlassen sich Ihre Proxy-Server auf eine MySQL-Datenbank, die sich in Ihrem Netzwerk befindet. Alle Proxy-Server in Ihrem Netzwerk müssen dieselbe Datenbank verwenden.

Diese Tabellen sind in der Proxy-Datenbank enthalten.

Proxy-Datenbanktabellen

Name	Beschreibung
db_id	Eindeutige Datenbank-ID
edge_token_map	Verschlüsselungsmusterdaten
token_map	Ordnungserhaltende Verschlüsselungsdaten

Sichern Ihrer Proxy-Datenbank

Da Verschlüsselungsmuster von der Tokenisierung abhängen, werden Klartextwerte in Ihrer Proxy-Datenbank gespeichert. Wenn die Datenbank verloren geht, können Klartextwerte nicht wiederhergestellt werden. Es ist wichtig, dass Sie regelmäßige Sicherungen durchführen. Um Datenverlust zu vermeiden, sichern Sie Ihre Proxy-Datenbank gemäß ServiceNow Empfehlungen.

- Sichern Sie Ihre Datenbank alle 24 Stunden.
- Bewahren Sie die binären Protokolldateien der MySQL-Datenbank für mindestens zwei Tage auf. Nachdem eine Sicherung wiederhergestellt wurde, können Sie das binäre Protokoll verwenden, um die seit der letzten Sicherung verlorenen Daten wiederherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Encryption-Clients

Edge Encryption verwendet drei Clients, um die Instanz zu informieren, dass der Proxy ausgeführt wird, um Anforderungen zwischen dem Proxy und der Instanz zu synchronisieren und alle Endbenutzer-Anforderungen nach einer potenziellen Verschlüsselung an die Instanz weiterzuleiten.

Client	Beschreibung
Heartbeat/Keepalive-Client	Dafür verantwortlich, alle 5 Sekunden eine Anforderung an die ServiceNow-Instanz zu senden, um die Instanz wissen zu lassen, dass dieser Proxy betriebsbereit ist und ausgeführt wird. Die Anforderungen geben das Feld last_response_on in der Edge-Proxy-Tabelle vor und folglich auch den Proxy-Status. Falls bei Ihrem System Probleme beim Senden von Anforderungen auftreten, oder wenn die Anforderungen oder die Verarbeitung der Anforderungen verzögert wird, kann die Instanz den Proxy gegebenenfalls mit der Markierung „Keine Reaktion“ versehen, auch wenn die anderen Clients (einschließlich des Clients für den Benutzerdatenverkehr) einsatzbereit sind. Dieser Client steuert auch den Online-Status des Proxys in der Instanz. Die Eigenschaft *edgeencryption.proxy.keepalive.interval* steuert die Abfragehäufigkeit für diesen Client. Der Standardwert beträgt 5 (Sekunden).
Abfrage-/Synchronisierungs-Client	Verantwortlich für verschiedene Anforderungen, die vom Proxy zum Synchronisieren mit der Edge Encryption-Konfiguration (z. B. die zu verschlüsselnde Tabelle, Spalte oder Anlage sowie Schlüssel, Aufträge, Regeln und Tokenisierungsmuster) an die Instanz gesendet werden. Die Eigenschaft *edgeencryption.config.poll.interval* steuert die Abfragehäufigkeit für diesen Client. **⚠ Warnung:** Ändern Sie diese Einstellung nicht. Eine Änderung der Standardeinstellung der Proxy-Abfragehäufigkeit führt möglicherweise dazu, dass die Synchronisierung verzögert wird, wenn die Edge Encryption-Einstellungen für die Instanz aktualisiert werden.
Standard-/Benutzerdatenverkehrs-Client	Für alles andere verarbeitet dieser Client alle Endbenutzer-Anforderungen und leitet diese nach einer möglichen Verschlüsselung an die ServiceNow-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client	Beschreibung
	Instanz weiter. Dieser Client verarbeitet auch Antworten von der Instanz und leitet sie nach einer möglichen Entschlüsselung an den Endbenutzer weiter.

Schlüsselverwaltung für Edge Encryption

Sie sind für die Bereitstellung und Verwaltung der von Edge Encryption verwendeten Verschlüsselungscodes verantwortlich.

Dieses Thema bezieht sich auf Schlüssel für das Produkt Edge Encryption. Informationen zum Key Management Framework, das mit der Verschlüsselung auf Spaltenebene verwendet werden kann, finden Sie unter Key Management Framework.

Wenn Sie Verschlüsselungscodes erhalten und erstellen, die die von Edge Encryption verwendeten Verschlüsselungsarten unterstützen, beachten Sie Folgendes:

- Soll AES 128-Bit oder AES 256-Bit verwendet werden? Sie müssen einen Standard-AES 128-Bit-Verschlüsselungsschlüssel definieren, auch wenn er nicht verwendet wird.
- Gibt an, ob Dateisystem, Java KeyStore oder Enterprise Key Management (EKM) verwendet werden soll.
- Wann müssen die Verschlüsselungsschlüssel rotiert werden?
- Wann und ob ein Massenverschlüsselungsauftrag verwendet wird, um Daten mit dem neuen Schlüssel erneut zu verschlüsseln.

Vor dem Entfernen eines Schlüssels aus den Proxy-Konfigurationsdateien und dem Schlüsselspeicher müssen unbedingt alle Daten in der Instanz entschlüsselt werden, die den Schlüssel verwendet. Sie können dies tun, indem Sie einen neuen Verschlüsselungscode hinzufügen und einen Auftrag zur Massenrotation von Schlüsseln planen.

Schlüsselspeicher

Edge Encryption unterstützt die folgenden Arten der Schlüsselspeicherung.

Dateispeicher

Schlüssel werden in einer Datei in einem Dateisystem gespeichert, auf das der Edge Encryption Proxy Zugriff hat. In einer Datei gespeicherte Verschlüsselungsschlüssel werden nicht verschlüsselt. Der Schutz dieser Dateien liegt also in Ihrer Verantwortung.

Java KeyStore

Schlüssel werden im JCEKS KeyStore von Java gespeichert. Ein Java KeyStore ist durch ein Passwort geschützt. Daher ist es sicherer als das Speichern von Schlüsseln in einer Datei im Dateispeicher. Ein einzelner Java KeyStore kann mehrere Schlüssel speichern. Die Schlüssel werden durch einen Schlüsselalias identifiziert, wodurch die Verwaltung mehrerer Schlüssel vereinfacht wird.

Enterprise Key Management (EKM)

Schlüssel werden mit den Schlüsselverwaltungssystemen SafeNet KeySecure oder Unbound Technology gespeichert und abgerufen.

Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen keystore.jceks im Verzeichnis Schlüsselspeicher geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie einen anderen Schlüsselspeicher als das Basissystem Java JCEKS KeyStore verwenden, müssen Sie den öffentlichen Schlüssel ServiceNow in Ihren Schlüsselspeicher importieren. Der Alias für den öffentlichen Schlüssel lautet `servicenow`.

Zusätzlich zu den Verschlüsselungsschlüsseln wird im Java JCEKS KeyStore das RSA-Schlüsselpaar zum digitalen Signieren der in der Instanz gespeicherten Verschlüsselungskonfigurations- und Verschlüsselungsregeln und das digitale Zertifikat gespeichert, das der Proxy Edge Encryption verwendet, um eine sichere Verbindung mit den Browsern und allen anderen Clients herzustellen.

SafeNet-Schlüsselversionsverwaltung für Edge Encryption

Verwenden Sie die SafeNet-Schlüsselversionsverwaltung, um das Wechseln der Schlüssel zu vereinfachen. Anstatt für jeden neuen Schlüssel einen Alias zu erstellen, behält die SafeNet-Schlüsselversionsverwaltung denselben Alias bei und erhöht die Version.

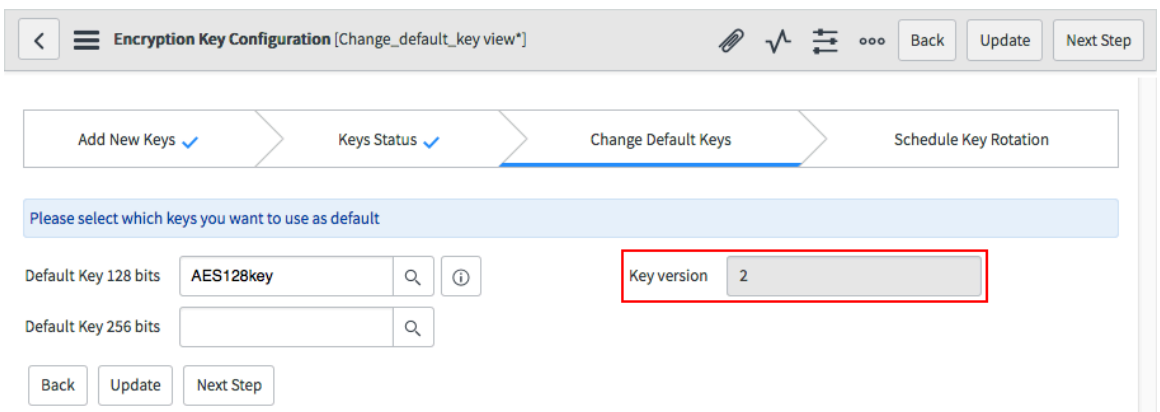
Sie müssen die Schlüssel-Versionsverwaltung in SafeNet einrichten, bevor Sie die SafeNet-Schlüssel-Versionsverwaltung auf dem Edge-Proxy-Server konfigurieren können.

Hinweis:
Vor der Version London installierte Edge-Proxys unterstützen SafeNet-Schlüssel, jedoch keine Versionsverwaltung von SafeNet-Schlüsseln. Wenn Sie versehentlich einen versionierten Schlüssel auf einem Kingston-Proxy oder einem älteren Proxy verwenden, erkennt der London-Proxy oder der spätere Proxy beim Upgrade auf die Version London oder höher dieses Problem, und um möglichen Datenverlust zu vermeiden, startet der Proxy nicht.

Sie müssen zunächst einen Auftrag für eine Massenschlüsselrotation oder einen einzelnen Schlüsselrotationsauftrag planen, um den alten SafeNet versionierten Schlüssel durch einen nicht versionierten Schlüssel zu ersetzen, und dann bei Bedarf einen neuen SafeNet versionierten Schlüssel erstellen. Dieser neue versionierte Schlüssel kann sicher für den Proxy London oder höher verwendet werden, und Sie können den Proxy neu starten.

Konfiguration des Verschlüsselungsschlüssels

Bei Verwendung von mit SafeNet versionierten Schlüsseln enthält der Abschnitt „Ändern des Abschnitts Standardschlüssel im Formular zur Konfiguration des Verschlüsselungsschlüssels“ neue Felder für die **Schlüsselversion** der standardmäßigen 128-Bit- und 256-Bit-Schlüssel. Die Felder für die **Schlüsselversion** sind ausgegraut und können nicht bearbeitet werden.

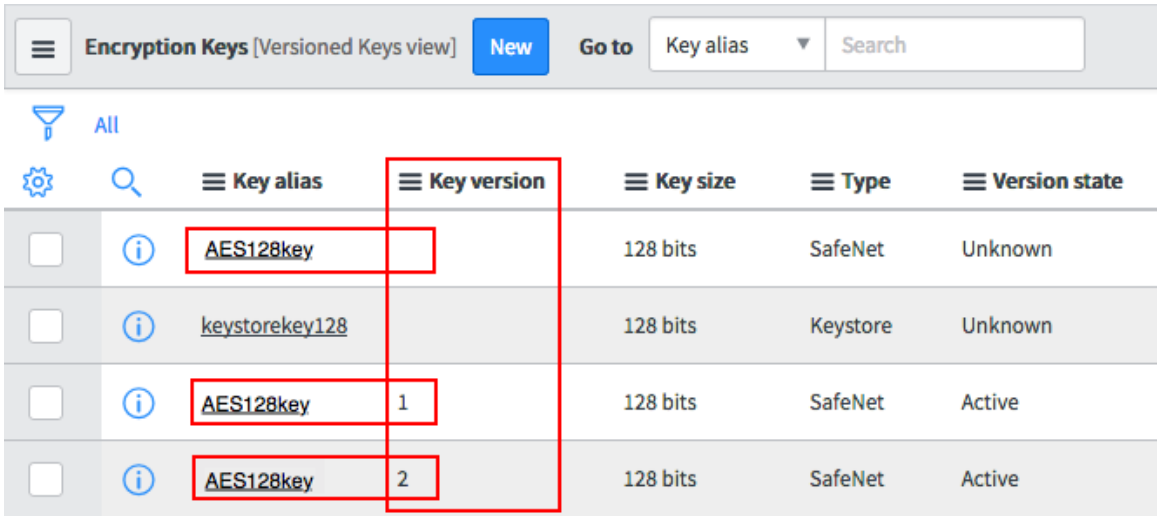


Hinweise zu Verfahren siehe Verschlüsselungsschlüssel für die Instanz konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Versionierte Schlüssel

Wenn Sie versionierte SafeNet-Schlüssel verwenden, navigieren Sie zu **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Alle Schlüssel**, versionierte Schlüssel enthalten die **Schlüsselversion**.



Für die ersten Einträge, die Sie im Abschnitt „Standardschlüssel ändern“ des Formulars „Konfiguration der Verschlüsselungsschlüssel“ vornehmen, wird keine Versionsnummer angezeigt. Wenn der Proxy-Server einen Schlüssel von SafeNet anfordert, fügt das System eine neue Zeile für den Aliasnamen und die **Schlüsselversion** hinzu.

Im obigen Beispiel ist **AES128key** dreimal aufgeführt:

- Die erste Auflistung ohne angegebener **Schlüsselversion** ist der erste Eintrag.
- Die zweite Auflistung mit **1** in der Spalte **Schlüsselversion** ist die erste Version des von SafeNet zurückgegebenen Schlüssels.
- Die dritte Auflistung mit **2** in der Spalte **Schlüsselversion** ist die zweite Version des von SafeNet zurückgegebenen Schlüssels.
- Da andere Versionen des Schlüssels von SafeNet zurückgegeben werden, werden neue Zeilen hinzugefügt, um die jetzt verwendete **Schlüsselversion** aufzuzeichnen.

Verschlüsselungskonfigurationen und -muster

Mit Edge Encryption können Felder verschlüsselt und Zeichenketten tokenisiert werden.

Verschlüsselungskonfigurationen

Sie können einzelne Felder mit Verschlüsselungskonfigurationen verschlüsseln. Edge Encryption unterstützt AES mit 128-Bit-Verschlüsselungsschlüsseln. Wenn die Richtliniendateien der Java Cryptography Extension (JCE) für die Beschränkung der Gültigkeitsdauer installiert sind, unterstützt Edge Encryption AES-256-Bit-Verschlüsselungsschlüssel für jeden Verschlüsselungstyp. Edge Encryption unterstützt die folgenden Arten von Verschlüsselungskonfigurationen.

Standardverschlüsselung

Der verschlüsselte Wert eines Felds unterscheidet sich jedes Mal, wenn das Feld verschlüsselt wird, auch wenn der Feldwert gleich bleibt. Standardverschlüsselung ist die robusteste Form der Verschlüsselung. Felder, die Standardverschlüsselung verwenden, können nicht sortiert, gruppiert oder gefiltert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gleichstellungserhaltende Verschlüsselung

Der verschlüsselte Wert eines Felds ist derselbe, wenn der Feldwert derselbe bleibt. Unterstützt Gleichstellungsvergleiche und Gruppieren nach Operationen in einem Feld.

Hinweis:
Wenn für ein Feld, das bereits Daten enthält, die gleichstellungserhaltende Verschlüsselung ausgewählt wird, werden bei der Gruppierung nach Aktion für das Feld möglicherweise keine Felder mit demselben Wert gruppiert, wenn eines verschlüsselt ist und das andere nicht.

Ordnungserhaltende Verschlüsselung

Verwendet Token und Verschlüsselung, um Daten in Ihrer Proxy-Datenbank zu sichern. Unterstützt Gleichstellungsvergleiche, Gruppieren nach Operationen und die Möglichkeit der Datensortierung. Der ordnungserhaltende Verschlüsselungstyp wird nur unterstützt, wenn eine MySQL-Datenbank für den Edge Encryption Proxy-Server konfiguriert ist.

Hinweis:
Wenn die ordnungserhaltende Verschlüsselung verwendet wird und die Proxy-Datenbank inaktiv ist, können Aktualisierungen an Feldern mit ordnungserhaltender Verschlüsselung vorgenommen werden. Die Sortierreihenfolge ist jedoch beim Versuch, Daten anhand dieser Felder zu sortieren, nicht korrekt. Gruppen funktionieren ebenfalls nicht wie erwartet. Wenn die Proxy-Datenbank wieder betriebsbereit ist, planen Sie einen Auftragstoken-Reparaturauftrag ein, um fehlende Token zu reparieren.

Verschlüsselungstypen

Die folgenden Verschlüsselungstypen sind gemäß abnehmender Sicherheitsqualität aufgeführt.

Verschlüsselungstyp	Beschreibung
Standard AES 256	Felder können nicht gefiltert, sortiert oder verglichen werden.
Standard AES 128	Felder können nicht gefiltert, sortiert oder verglichen werden.
Gleichstellungserhaltung von AES 256	Felder können mit Gleichstellungsvergleichen gefiltert werden.
Gleichstellungserhaltung von AES 128	Felder können mit Gleichstellungsvergleichen gefiltert werden.
Ordnungserhaltung von AES 256	Felder können sortiert und Gleichstellungsfilterung verwendet werden. Erfordert die Verwendung einer MySQL-Datenbank in Ihrem Netzwerk.
Ordnungserhaltung von AES 128	Felder können sortiert und Gleichstellungsfilterung verwendet werden. Erfordert die Verwendung einer MySQL-Datenbank in Ihrem Netzwerk.

Verschlüsselungsmuster

Sie können vertrauliche Daten in Zeichenfolgen mithilfe von Verschlüsselungsmustern schützen. Sobald ein Verschlüsselungsmuster gespeichert und aktiviert ist, identifiziert der Edge Encryption Proxy-Server Zeichenfolgen, die dem Muster in Anforderungen entsprechen. Nach der Suche wird die Klartextzeichenfolge in der Proxy-Datenbank gespeichert und in der Instanz durch ein Token ersetzt. Verwenden Sie Verschlüsselungsmuster, um Zeichenketten zu kennzeichnen, die regulären Mustern entsprechen, z. B. Sozialversicherungs- und Kreditkartennummern. Wir empfehlen, dass Verschlüsselungskonfigurationen die primäre Verschlüsselungsmethode sind. Verwenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie jedoch Verschlüsselungsmuster als Ergänzung, um vertrauliche Informationen zu finden und zu schützen, die außerhalb verschlüsselter Felder gefunden werden.

Hinweis:
Der Edge Encryption Proxy-Server erfordert nur eine MySQL-Datenbank in Ihrem Netzwerk, wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden. Klartextwerte werden in der Proxy-Datenbank in Ihrem Netzwerk gespeichert. Aus diesem Grund ist es wichtig, dass Sie Ihre Proxy-Datenbank schützen und regelmäßig sichern. Empfehlungen finden Sie unter Komponenten der Edge Encryption.

Zugehörige Informationen

Felder mit Verschlüsselungskonfigurationen verschlüsseln

Zeichenketten mithilfe von Verschlüsselungsmustern tokenisieren

Mit Edge Encryption installiert

Edge Encryption installiert Tabellen zum Speichern verschlüsselungsbezogener Daten, Systemeigenschaften zum Konfigurieren des Standardverhaltens und die Rolle edge_encryption zur Verwaltung von Edge Encryption.

Mit Edge Encryption installierte Tabellen

Edge Encryption fügt die folgenden Tabellen hinzu.

Edge Encryption-Konfiguration [sys_encryption_configuration]

Enthält verschlüsselte Felder und Tabellen, für die Anhänge verschlüsselt werden.

Edge Encryption-Regel [sys_encryption_rule]

Enthält für jede Regel einen Datensatz. Eine Regel hat einen Namen, die Bedingung für deren Verwendung, ein Skript und ein Auftragsfeld.

Edge Encryption Ungültiges Einfügeprotokoll [sys_edge_encryption_invalid_insert_log]

Enthält Protokollnachrichten, die für Versuche erstellt wurden, unverschlüsselte Daten in einem verschlüsselten Feld zu speichern.

Edge Encryption-Proxy [sys_encryption_proxy]

Enthält Informationen zur Verschlüsselungs-Proxy-Anwendung.

Edge-Proxy-Verschlüsselungstyp [sys_proxy_encryption_type]

Wird zum Aktivieren und Deaktivieren von Verschlüsselungstypen im Verschlüsselungsformular verwendet.

Ausführung des Verschlüsselungsauftrags [sys_encryption_job_execution]

Unterstützt Aufträge zur Massenverschlüsselung.

Blockausführung des Verschlüsselungsauftrags [sys_encryption_job_execution_chunk]

Unterstützt Aufträge zur Massenverschlüsselung.

Geplanter Verschlüsselungsauftrag [sysauto_encryption_job]

Listet geplante Aufträge für die Verschlüsselung, Entschlüsselung, Schlüsselrotation, Auftragstokenreparatur und Datenbankwiederherstellung auf.

Verschlüsselungsschlüsselkonfiguration [sys_encryption_key_configuration]

Listet die Standard-Verschlüsselungsschlüssel auf.

Verschlüsselungsschlüssel [sys_encryption_key]

Listet die verfügbaren Schlüssel und Schlüsselattribute auf.

Proxy-Verschlüsselungsschlüssel [sys_encryption_proxy_key]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listet Proxy-Verschlüsselungsschlüssel auf.

Mit Edge Encryption installierte Eigenschaften

Edge Encryption fügt die folgenden Eigenschaften hinzu.

Hinweis:
Um die Tabelle „Systemeigenschaften“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter `sys_properties.list` ein.

glide.edge.pattern.disallowed.chars

Eine Liste von Zeichen, die in Mustern nicht zulässig sind.

- **Typ**: eine Zeichenkette einer durch Komma getrennten Liste von Werten
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

glide.edge.pattern.min.size

Die minimal zulässige Mustergröße. Das Erlauben kleinerer Muster bedeutet, mehr Übereinstimmungen zu finden, was den Aufwand erhöht.

- **Typ**: Zahl
- **Standardwert**: 5
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.logging.destination

Wo Nachrichten protokolliert werden.

- **Typ**: Zeichenfolge
- **Standardwert**: Datei
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.logging.verbosity

Die zu verwendende Protokollierungsstufe.

- **Typ**: Zeichenfolge
- **Standardwert**: Info
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.encryption.proxy.buildtag

Die in Ihrer Instanz registrierte Proxy-Version.

- **Typ**: Zeichenfolge
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.cleartext.allowed

Bei „Wahr“ kann Klartext in einem verschlüsselten Feld gespeichert werden. Dies geschieht, wenn ein Benutzer auf die Instanz zugreift, ohne den Edge Encryption Proxy zu verwenden. Bei „Falsch“ verhindert das System, dass Klartext in einem verschlüsselten Feld gespeichert wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Typ**: Boolesch
- **Standardwert**: false
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

Die Edge Encryption planen

Die erfolgreiche Implementierung von Edge Encryption erfordert Planung und Vorbereitung.

Beantworten Sie die folgenden Fragen bereits in der Planungsphase.

- Welche Felder sollen verschlüsselt werden?
- Welche Verschlüsselungstypen sollen verwendet werden?
- Wie viele Edge Encryption Proxys werden benötigt? Empfehlungen und Überlegungen finden Sie unter Umgebungsgröße Ihrer Edge Encryption anpassen.
- Wo befindet sich die MySQL-Datenbank, wenn ein ordnungserhaltender Verschlüsselungstyp oder ein Verschlüsselungsmuster verwendet werden soll?
- Welches Schlüsselmanagementsystem soll verwendet werden?

Systemadministratoren, Netzwerkadministratoren und Mitglieder des Sicherheitsteams haben unterschiedliche Aufgaben bei der Implementierung von Edge Encryption zu erfüllen.

- Systemadministratoren benötigen die Sicherheitsadministratorrolle. Der Systemadministrator muss:
  - Die Edge Encryption Proxy-Anwendung herunterladen.
  - Ein Edge Encryption Benutzerkonto für die Proxys einrichten, die zur Verbindung mit der Instanz verwendet werden sollen. Dem Benutzer muss die Rolle edge_encryption zugewiesen werden.
  - Die Verschlüsselungsschlüssel konfigurieren und die Standardschlüssel festlegen.
  - Edge Encryption auf der Instanz konfigurieren.
  - Verschlüsselungsaufträge planen.
  - Edge Encryption überwachen.
  - Verschlüsselungsregeln erstellen und bearbeiten.
- Ihr Netzwerkadministrator muss:
  - Die Edge Encryption Proxy-Anwendung installieren.
  - Die Netzwerkadressen für die Proxy-Server und die Proxy-Datenbank kennen, die zur Aufrechterhaltung der Verschlüsselungs- und Verschlüsselungsmuster verwendet wird.
  - Die Proxy-Datenbank installieren, die zur Aufrechterhaltung der Verschlüsselung und Verschlüsselungsmuster verwendet werden soll.
  - Die Proxy-Anwendung starten und stoppen.
  - Die Verschlüsselungsverwaltung durchführen.
  - Bestimmen, wie Benutzer zu Verschlüsselungs-Proxy-Anwendungen zugeordnet werden. Dies kann mit DNS-Einstellungen oder Routing-Regeln erfolgen und ist netzwerkspezifisch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mehrere Proxy-Server verwalten.
- Load-Balancer-Pools und -Einstellungen konfigurieren.

- Ihr Sicherheitsadministrator muss die Verschlüsselungstypen festlegen, die jedem Feld zugewiesen werden sollen.

Edge Encryption-Systemanforderungen

Sie können die Edge Encryption-Proxy-Anwendung auf Servern oder virtuellen Computern ausführen, auf denen Microsoft Windows oder Linux ausgeführt wird. Damit eine optimale Leistung erzielt wird, stellen Sie sicher, dass Ihre Konfiguration diese Anforderungen erfüllt.

Java-Anforderungen

Der Hostcomputer, auf dem der Proxyserver Edge Encryption installiert oder ausgeführt wird, muss eine unterstützte Version von Java enthalten. Derzeit unterstützte Versionen sind Java 11.0.6 oder höher in der 11.x-Versionsreihe

Hinweis:
Java 8 wird ab Release Utah nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit dem Proxy Edge Encryption auf Java 11, bevor Sie versuchen, die Version Edge Encryption des Proxys [Utah zu installieren.

Hinweis:
Java lässt Schlüssel mit unbegrenzter Stärke nicht automatisch zu. Sie müssen die Verwendung von AES 256-Bit-Verschlüsselung speziell aktivieren.

Unterstützung für OpenJDK

Now Platform unterstützt OpenJDK Version 11.

Mindestkonfiguration für Proxy-Server

Ein Proxy-Server erfordert die folgende Mindestkonfiguration:

- Mindestens 4 GB Arbeitsspeicher pro Proxy-Server (für die meisten Bereitstellungen werden 6 GB empfohlen).

  Hinweis:
  Der Proxy-Server-Host muss mindestens 1 GB Arbeitsspeicher mehr aufweisen als der Proxy-Server. Der Proxy-Server-Host benötigt 1 GB zusätzlich für Betriebssystem-Services. Wenn Sie beispielsweise einen Proxy-Server zur Verwendung von 4 GB Arbeitsspeicher konfigurieren, müssen Sie mindestens 5 GB Arbeitsspeicher auf dem Proxy-Server-Host installieren.

  Da der Proxy-Server mindestens 4 GB Arbeitsspeicher benötigt, werden 32-Bit-JREs und 32-Bit-Betriebssysteme ab dem Release London nicht mehr unterstützt.

- CPU mit mindestens 3 GHz (4-Kern-CPU wird für eine optimale Leistung empfohlen).
- Mehrere einem Load Balancer nachgeschaltete Proxy-Server. Die Anzahl der benötigten Proxy-Server hängt von der Anzahl der Anwendungsknoten, der Anzahl der gleichzeitigen Benutzer und der Anzahl der für Failover-Zwecke benötigten Server ab. Weitere Informationen finden Sie unter Umgebungsgröße Ihrer Edge Encryption anpassen.
- Möglichkeit der Ausführung zusammen mit anderen Diensten, abhängig von der Serverauslastung und der Ressourcenverfügbarkeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Proxy-Servern unterstützte Systeme

Die folgenden Systeme werden unterstützt:

Unterstütztes System	Beschreibung
Windows Server-Editionen 2012, 2012-R2, 2016 und 2019	• Virtuelle Maschinen oder physische Hardware • 64-Bit-Systeme
Linux	• Virtuelle Maschinen oder physische Hardware • 64-Bit-Systeme Auf 64-Bit-Linux-Systemen muss die 32-Bit GNU C-Bibliothek (glibc) installiert werden. Der Installationsbefehl für CentOS lautet `yum install glibc.i686`.

Versionsanforderungen für Proxy-Server

Halten Sie Ihre Edge Encryption -Proxy-Version mit Ihrer ServiceNow -Instanzversion synchron (gleicher Hauptrelease, z. B. Tokyo). Um Ausfallzeiten während des Upgrade-Vorgangs zu vermeiden, ist der Proxy Edge Encryption abwärtskompatibel. Es ist jedoch wichtig, so bald wie möglich ein Upgrade durchzuführen, um sicherzustellen, dass Benutzer auf neue Funktionen und wichtige Fehlerbehebungen zugreifen können.

Verbindungsanforderungen des Proxy-Servers

Der Proxy-Server, auf dem die Edge Encryption-Anwendung ausgeführt wird, muss mit den Computern in Ihrem Netzwerk kommunizieren können. Stellen Sie sicher, dass der Proxy-Server über folgende Netzwerkprivilegien verfügt:

Netzwerkprivileg	Beschreibung
Firewallzugriff	Konfigurieren Sie alle Firewalls zwischen dem Proxy-Server und den Clientgeräten so, dass sie eine Verbindung zulassen. Wenn in Ihrem Netzwerk eine demilitarisierte Zone (DeMilitarized Zone, DMZ) verwendet wird, sodass Ihr lokales Netzwerk (LAN) um eine zusätzliche Sicherheitsebene erweitert wird, und Ihre Netzwerksicherheitsprotokolle den Portzugriff innerhalb des Netzwerks auf die DMZ beschränken, müssen Sie möglicherweise einen Proxy-Server auf einem Computer in der DMZ bereitstellen.
Netzwerkzugriff	Konfigurieren Sie jeden Client so, dass der Proxy-Server eine Verbindung mit ihm herstellen kann. Wenn Sie aufgrund der Netzwerksicherheit keine neuen Computer konfigurieren können, die eine Verbindung zu den Clients herstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkprivileg	Beschreibung
	können, installieren Sie den Proxy-Server auf einem vorhandenen Computer mit Verbindungsberechtigungen.
Instanz-Zugriff	Stellen Sie sicher, dass der Proxy-Server über einen Netzwerkzugriff auf die Instanz verfügt. Stellen Sie sicher, dass Sie das vom Proxy-Server verwendete Netzwerk so konfigurieren, dass Datenverkehr über den TCP-Port 443 zugelassen wird.
Netzwerk-Konto	Installieren Sie den Proxy-Server mit dem Konto eines lokalen oder Domänenadministrators.

Anforderungen an das Datenbanksystem für die Ordnungserhaltung und die Tokenisierung

Für die ordnungserhaltende Verschlüsselung und das Verschlüsselungsmuster müssen Sie eine Oracle MySQL-Datenbank für den Edge Encryption-Proxy-Server konfigurieren. Bei einer ordnungserhaltenden Verschlüsselung kann ein beliebiger Vergleichsvorgang direkt auf verschlüsselte Daten angewendet werden, ohne dass die Daten erst entschlüsselt werden müssen. Mit Verschlüsselungsmustern können Sie Zeichenfolgenmuster durch Token ersetzen (sog. Tokenisierung), bevor sie an die Datenbank gesendet und darin gespeichert werden. Verwenden Sie aufgrund der Größe der MySQL-Datenbank einen dedizierten Proxy-Server, um die Datenbank für die ordnungserhaltende Verschlüsselung und die Tokenisierung auszuführen.

Die Mindestanforderungen für das Datenbanksystem umfassen:

MySQL-Datenbank	Anforderung
Version	MySQL-Datenbanken, Versionen 5.7 und 8.0 **Hinweis:** Die MySQL-Versionen 5.5 und 5.6 werden nicht mehr getestet und haben das Ende des Supports erreicht.
BS	64-Bit-Systeme
CPU	CPU mit mindestens 2 GHz (4-Kern-CPU wird für eine optimale Leistung empfohlen)
RAM	16 GB
Datenträger	Storage Area Network (SAN) oder lokaler Speicher (RAID 10 empfohlen)
Größe	Bestimmt durch die Anzahl potenzieller Datensätze multipliziert mit der Datensatzgröße. Weitere Informationen finden Sie unter Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen.
Konfiguration	Cluster für hohe Verfügbarkeit. Wenn Sie nicht sicher sind, wie Sie Ihren MySQL-Server konfigurieren, wenden Sie sich an MySQL , um Informationen zur Konfiguration zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Umgebungsgröße Ihrer Edge Encryption anpassen

Die Auswahl der Anzahl von Proxy-Servern für Ihre Umgebung ist von hoher Bedeutung. Berücksichtigen Sie die Anzahl der Benutzer, die Redundanzanforderungen und die akzeptable Latenzzeit.

Redundanz

Verwalten Sie redundante Proxy-Server für den Fall eines Hardwarefehlers. Proxy-Server sollten einem Load Balancer nachgeschaltet sein, um einen funktionalen Pfad für alle Benutzer bereitzustellen, wenn ein Proxy-Server nicht erreichbar ist. Stellen Sie sicher, dass immer mindestens zwei Proxy-Server verfügbar sind.

Größe

Die Größe bezieht sich auf die Anzahl der Proxy-Server, die erforderlich sind, um zusätzliche Latenzzeiten zu vermeiden, die durch die Verschlüsselung von Daten entstehen. Je nach Verwendung möchten Sie möglicherweise die Latenzzeit reduzieren, indem Sie zusätzliche Proxy-Server hinzufügen. Wenn beispielsweise regelmäßige Massenverschlüsselungen ausgeführt werden, fügen Sie zur Handhabung der Last zusätzliche Proxy-Server hinzu oder führen Sie die Massenverschlüsselungen bei geringer Benutzerlast durch. Außerdem beeinflusst die Hardware, auf der der Proxy-Server ausgeführt wird, die Leistung und Latenz. Proxy-Server, die auf Hardware mit schnelleren CPUs, mehr CPUs und mehr RAM laufen, haben einen höheren Durchsatz als langsamere, begrenzte Systeme.

In den folgenden Richtlinien wird davon ausgegangen, dass der Proxy-Server mindestens die Mindesthardwareanforderungen erfüllt. So bestimmen Sie die Anzahl der Proxy-Server:

- Erwägen Sie, für jeweils zwei Anwendungsknoten in der Instanz einen Proxy-Server einzurichten.
- Richten Sie aus Gründen der Redundanz mindestens zwei Proxy-Server hinter einem Load Balancer ein.
- Fügen Sie für jeweils 500 gleichzeitige Benutzer einen zusätzlichen Proxy-Server hinzu.
- Fügen Sie je nach gewünschter Redundanz weitere Proxy-Server für das Failover hinzu.

Für eine Instanz mit 2.000 Benutzern sollten Sie beispielsweise mindestens fünf Proxy-Server einem Load Balancer nachgeschaltet sein. Diese Berechnung umfasst einen Proxy-Server für jeweils 500 Benutzer und einen zusätzlichen Proxy-Server für Failover. Bestimmen Sie im Voraus, wann Sie sich einem Schwellenwert von 500 Benutzern nähern, und platzieren Sie einen anderen Proxy-Server im Load-Balancer-Pool.

Load Balancers

Um Anforderungen zu verteilen und die Antwortzeit des Servers zu verbessern, verteilen Sie Proxy-Server in einem Load-Balancer-Pool. Konfigurieren Sie Load Balancer für die Verwendung nach der Methode der „wenigsten Verbindungen“. Diese Methode verbindet Anfragen mit dem Proxy-Server mit den wenigsten aktiven Verbindungen, wodurch die Überlastung eines einzelnen Proxys verhindert wird.

CPU-Auslastung

Da Datenverschlüsselung und Tokenisierung CPU-intensive Operationen erfordern, sind CPU-Spitzen während der Datenverschlüsselung normal und zu erwarten. Wenn die CPU-Auslastung mehrere Minuten lang über 80 % liegt, bedeutet dies wahrscheinlich, eine zu hohe Auslastung des Proxy-Servers. In diesem Fall erhöht sich die Latenz für den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitraum, in dem die CPU-Auslastung hoch ist. Wenn die Latenz bestehen bleibt, kann das Hinzufügen eines weiteren Proxy-Servers zur Verringerung der Latenz beitragen.

Arbeitsspeicher

Der Proxy-Server muss über mindestens 4 GB RAM verfügen (empfohlen sind 6 GB). Legen Sie die anfänglichen und oberen Speichergrenzen des Proxy-Servers auf die empfohlenen Einstellungen fest.

Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen

Wenn Sie ordnungserhaltende Verschlüsselung oder Verschlüsselungsmuster verwenden, bestimmen Sie die Größe Ihrer MySQL-Datenbank, indem Sie die Anzahl der potenziellen Datensätze mit der Datensatzgröße multiplizieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie eine dedizierte Maschine, um die Datenbank für die Ordnungserhaltung und die Tokenisierung auszuführen. Führen Sie die Datenbank nicht auf derselben Hardware wie der Proxy-Server aus.

Prozedur

1. Bestimmen Sie die potenzielle Anzahl von Datensätzen, die Felder enthalten können, die mit auftragserhaltender Verschlüsselung verschlüsselt sind.
   a. Multiplizieren Sie die Anzahl der Verschlüsselungskonfigurationen mithilfe der auftragserhaltenden Verschlüsselung mit der Anzahl der Datensätze, auf die jede Konfiguration angewendet wird.
   b. Um Wachstum zu ermöglichen, multiplizieren Sie das Ergebnis mit drei.
2. Multiplizieren Sie das Ergebnis aus Schritt 1 mit 1.536.
   1.536 ist die durchschnittliche Größe eines Datensatzes in Bytes.
3. Wenn Sie Verschlüsselungsmuster verwenden, führen Sie die Schritte 1 und 2 für Datensätze mit Token aus, und fügen Sie das Ergebnis zur Summe hinzu.

Ergebnisse
Der berechnete Wert ist die empfohlene Größe in Bytes für Ihre auftragserhaltende und tokenisierende Datenbank.

Edge Encryption – Einschränkungen

Edge Encryption wirkt sich auf Systemfunktionen aus. Bewerten Sie sorgfältig die Auswirkungen der Verschlüsselung eines Feldes.

Feldtypeinschränkungen

Sie können nur die folgenden Feldtypen verschlüsseln:

- Datum
- E-Mail
- Datum/Uhrzeit
- HTML
- IP-Adresse
- Journal

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Journaleingabe
- Mehrzeiliger Text
- Einzeiliger Text
- Zeichenfolge
- URL

Die folgenden Feldtypen können Sie nicht verschlüsseln:

- Auswahlfelder
- Virtuelle Felder
- Felder in Systemtabellen mit Ausnahme bestimmter Felder in sys_user
- Systemfelder in Tabellen
- Zahlenfelder oder Felder, die mit einem Schema für die automatische Nummerierung verbunden sind
- Alle anderen oben nicht aufgeführten Feldtypen

Zusätzliche Einschränkungen:

- Wenn ein Journalfeld verschlüsselt ist, ist die **Schaltfläche** Veröffentlichen inaktiv, auch wenn mehrere Journalfelder vorhanden sind und nur eines dieser Felder verschlüsselt ist.
- Verschlüsselte Felder sind in den Feldern **„Gehe zu“** und „Header-Filter“ nicht verfügbar.
- Bei der Verschlüsselung von Feldern, die als Index verwendet werden, können Sie nur die Verschlüsselungstypen für die Ordnungserhaltung und Gleichstellungserhaltung verwenden. Indizierte Felder können nicht mit dem Standardverschlüsselungstyp verschlüsselt werden.

Weitere Informationen finden Sie unter Feldtypen .

Einschränkungen für das Filtern und Suchen

Standardverschlüsselung

Wenn Sie ein Feld vom Typ Zeichenfolge, Datum, Datum/Uhrzeit oder URL mit einer Feldkonfiguration für eine Standardverschlüsselung als linken Operanden in einem Filter auswählen, sind keine Filteroptionen verfügbar.

Gleichstellungserhaltende Verschlüsselung

Wenn Sie ein Feld vom Typ Zeichenfolge, Datum, Datum/Uhrzeit oder URL mit einer Feldkonfiguration für die gleichstellungserhaltende Verschlüsselung als linken Operanden in einem Filter auswählen, sind folgende Operatoren verfügbar:

- **ist**
- **ist nicht**
- **ist leer**
- **ist nicht leer**

Ordnungserhaltende Verschlüsselung

Wenn Sie ein Zeichenfolgenfeld mit einer verschlüsselten Feldkonfiguration als linken Operanden in einem Filter auswählen, sind neben **is**, **is not**, **is empty**und **is not empty**die folgenden Operatoren verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **größer als**
- **weniger als**

Wenn Sie ein Datums- oder Datums-/Uhrzeitfeld mit einer verschlüsselten Feldkonfiguration als linken Operanden in einem Filter auswählen, sind die folgenden Operatoren zusätzlich zu **is**, **is not**, **is empty**und **is not empty**verfügbar:

- **nach**
- **vor**
- **nach oder am**
- **vor oder an**

Auswahl von Datum sowie von Datum/Uhrzeit

Verwenden Sie für Datumsfelder die Datumsauswahl, um das Datum anzugeben:

Verwenden Sie für Datums-/Uhrzeitfelder die Datums- und Uhrzeitauswahl, um das Datum und die Uhrzeit anzugeben: Datums-

Listen-Bedingungsfilter

Die Optionen **Übereinstimmungen anzeigen** und **Herausfiltern** werden in Listen unterstützt. Nur genaue Übereinstimmungen werden zurückgegeben oder herausgefiltert.

Hinweis:
Das Hinzufügen von verschlüsselten Feldern in Bedingungsfiltern wird in Skripts wie UI-Richtlinien und Business-Regeln unterstützt.

Konfigurationseinschränkungen

Einschränkungen und Verhalten von Verschlüsselungskonfigurationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nachdem Sie der Konfigurationstabelle Edge Encryption ein Feld hinzugefügt haben, können Sie den Konfigurationsdatensatz nicht löschen. Wenn Sie ein Feld nicht mehr verschlüsseln möchten, deaktivieren Sie den Datensatz in der Edge Encryption-Konfigurationstabelle und planen Sie einen Verschlüsselungsauftrag zum Entschlüsseln der Daten.
- Wenn ein Feld in einer übergeordneten Tabelle für die Verschlüsselung markiert ist, wird das Feld auch in allen vererbten Tabellen verschlüsselt. Wenn beispielsweise das Feld **Kurzbeschreibung** in der Aufgabentabelle verschlüsselt ist, wird der Inhalt des Felds **Kurzbeschreibung** in der Incident-Tabelle verschlüsselt.
- Wenn ein von einer übergeordneten Tabelle geerbtes Feld als verschlüsselt markiert ist, kann das Feld in der übergeordneten Tabelle nicht verschlüsselt werden. Wenn beispielsweise die **Kurzbeschreibung** in der Incident-Tabelle als verschlüsselt markiert ist, kann die **Kurzbeschreibung** in der Aufgabentabelle nicht verschlüsselt werden. In diesem Beispiel können Sie die **Kurzbeschreibung** in der Problemtabelle verschlüsseln.
- Wenn ein Feld mit einer definierten Verschlüsselungskonfiguration in ein beliebiges Format exportiert wird, enthält die Ausgabe auch dann verschlüsselte Werte, wenn sie über den Proxy-Server exportiert werden.
- Sie können keine Daten in ein Feld mit einer definierten Verschlüsselungskonfiguration importieren.
- Sie können geerbte Felder für Datum und Datum/Uhrzeit nicht verschlüsseln. Datums- oder Datums-/Uhrzeitfelder, die von einer übergeordneten Tabelle geerbt werden, werden nicht in der Dropdown-Liste des **Spaltenfelds** aufgeführt, und Sie können keine Verschlüsselungskonfigurationen für Datum oder Datum/Uhrzeit für diese Felder erstellen.
- Sie können ein Feld vom Typ Zeichenfolge oder URL nur von einer übergeordneten Tabelle oder einer untergeordneten Tabelle verschlüsseln, nicht jedoch von beiden.

Instanzeinschränkungen

Auswirkungen der Verwendung von Edge Encryption auf die Instanz:

- Back-End-Logik kann verschlüsselte Daten nicht verarbeiten. Wenn die Instanz verschlüsselte Daten enthält, werden Business Rules, Back-End-Skripts oder Back-End-Funktionen, die auf der Auswertung der Daten im verschlüsselten Feld basieren, nicht ordnungsgemäß ausgeführt.

  Hinweis:
  Daten, die mit gleichstellungserhaltender oder ordnungserhaltender Verschlüsselung verschlüsselt sind, bestehen weiterhin Äquivalenzprüfungen, wenn sie mit einem identischen verschlüsselten Wert verglichen werden.

- Da die E-Mail-Verarbeitung von den E-Mail-Systemen direkt an die -Instanz erfolgt und nicht den Edge-Proxy durchlaufen kann, können per E-Mail ein- oder ausgehende Daten nicht vom Edge-Proxy verschlüsselt oder entschlüsselt werden.
  - Daten und Anhänge in eingehenden E-Mails werden nicht verschlüsselt.
  - Daten und Anhänge in ausgehenden E-Mails bleiben verschlüsselt und können nicht entschlüsselt werden.
- Auf dem Server ausgeführte Skripts können verschlüsselte Daten nicht ändern.
- Globale Suche wird nicht unterstützt. Da die globale Suche versucht, sowohl verschlüsselte als auch Klartextdaten zu durchsuchen, sind die Ergebnisse möglicherweise nicht wie erwartet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verschlüsselte Daten können nicht kopiert und in einen Datensatz eingefügt werden, in dem das Feld nicht verschlüsselt ist.
- Abhängig vom ausgewählten Verschlüsselungstyp wird die Benutzeroberflächenfunktionalität für die verschlüsselten Felder reduziert. Beispielsweise kann die Möglichkeit zum Vergleichen, Gruppieren, Sortieren und Suchen beeinträchtigt werden Generell gilt: Je stärker die gewählte Verschlüsselung, desto mehr Funktionalität wird eingeschränkt.
- Abgesehen von Java KeyStore, SafeNet und Unbound Technology wird keine Verwaltung von Software- oder Hardware-Verschlüsselungsschlüsseln von Drittanbietern unterstützt.
- Obwohl mehrere mit einer einzelnen Instanz verbundene Proxyserver unterstützt werden, sind Verwaltung und Überwachung des Verschlüsselungs-Proxy-Clusters nicht verfügbar. Jeder Proxy muss separat verwaltet werden.
- Systemkonfigurationen wie Auslastung und Anzahl der verschlüsselten Felder können sich auf die Leistung der verschlüsselten Felder auswirken.
- Der Edge Encryption Proxy-Server kann nur eine Verbindung zu einer einzelnen Instanz herstellen.
- Wenn Ihre Instanz eine Oracle-Datenbank verwendet und das Feld „Zeichenfolge“, das Sie zur Verschlüsselung markieren, länger als 2925 Zeichen ist, kann dieses Feld nicht sortiert werden, auch wenn die Verschlüsselung mit Reihenfolgenerhaltung ausgewählt ist.
- Wenn Ihre Instanz eine Oracle-Datenbank verwendet, ist Unicode AL32UTF8 der einzige unterstützte Zeichensatz.
- Verschlüsselte Daten können nicht in Berichten verwendet werden.
- Edge Encryption kann nicht mit Datenarchivierung verwendet werden.

Edge Encryption wird installiert

Sie können einen Edge Encryption Proxy manuell oder mithilfe des interaktiven Installers Edge Encryption installieren.

Java-Anforderungen

Der Hostcomputer, auf dem der Proxyserver Edge Encryption installiert oder ausgeführt wird, muss eine unterstützte Version von Java enthalten. Derzeit unterstützte Versionen sind Java 11.0.6 oder höher in der 11.x-Versionsreihe

Hinweis:
Java 8 wird ab Release Utah nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit dem Proxy Edge Encryption auf Java 11, bevor Sie versuchen, die Version Edge Encryption des Proxys [Utah zu installieren.

Proxy-Server installieren

Das Installieren von Edge Encryption beinhaltet diese Schritte.

- Installieren Sie die Edge Encryption Proxy-Anwendung auf einem Server in Ihrem Netzwerk mithilfe des interaktiven oder des manuellen Installationsprogramms.
- Generieren Sie das RSA-Schlüsselpaar für die digitale Signatur von Verschlüsselungskonfigurationen und Verschlüsselungsregeln.
- Installieren Sie die Java Cryptography Extension (JCE), wenn Sie die AES 256-Verschlüsselung verwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie eine sichere SSL-Verbindung verwenden, beziehen Sie ein Serverzertifikat und importieren Sie es in den Java KeyStore.
- Richten Sie Ihren Schlüsselspeicher und den Verschlüsselungsschlüssel ein.
- Wenn ordnungserhaltende Verschlüsselungstypen oder Verschlüsselungsmuster verwendet werden sollen, richten Sie eine MySQL-Datenbank auf einem Computer in Ihrem Netzwerk ein.
- Stellen Sie die gewünschten Eigenschaften ein. Eigenschaften befinden sich in der Konfigurationsdatei edgeencryption.properties.
- Legen Sie fest, dass ein Proxy-Server eine vertrauenswürdige Quelle ist, sodass Edge Encryption Anforderungen von diesem Proxy-Server verarbeiten kann.

Zugriff auf den Proxy-Server

Verweisen Sie nach Abschluss der Installation den Browser jedes Benutzers auf den Edge Encryption Proxy mit dem URL-Format: `<host>:<port>`. Werte werden durch die Host- und Port-Eigenschaften in der Datei edgeencryption.properties bestimmt.

Ein Beispiel mit folgenden Werten:

Eigenschaft	Beispielwert
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

Ein Client greift unter der folgenden Adresse auf den Proxy-Server zu: `http://hostname.mycompany.com:8081/`.

Hinweis:
DNS-Einstellungen und Routing-Regeln können verwendet werden. Host- und Portwerte werden von Ihrem Netzwerkadministrator festgelegt.

Edge Encryption anfordern

Das Edge Encryption Plugin (com.glide.edgeencryption) ist als separates Abonnement erhältlich.

Vorbereitungen

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktions- oder Test- und Entwicklungsumgebung Ihrer Organisation.

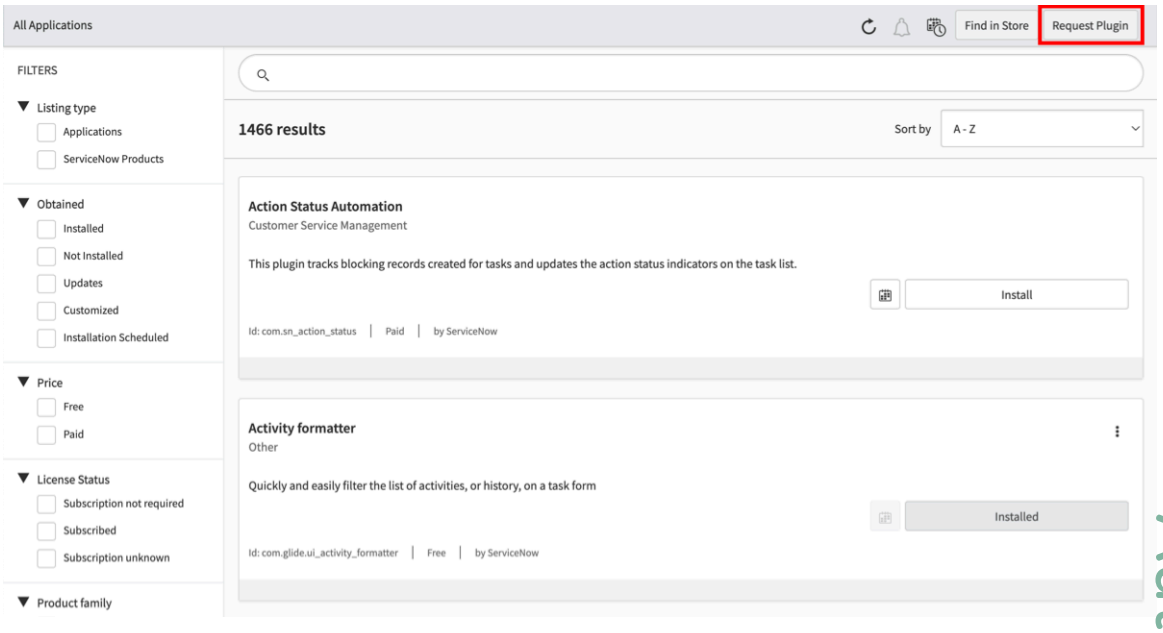
Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: keine

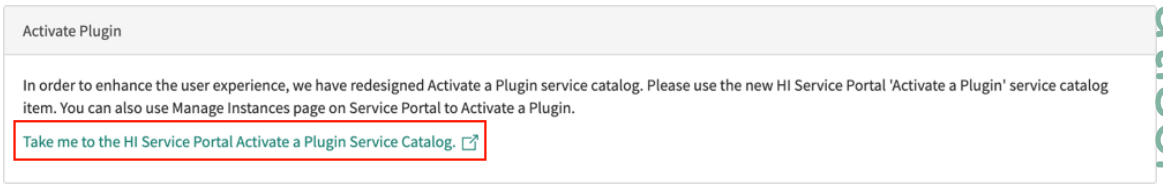
Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.

5. Wählen Sie **Aktionen > Plugin aktivieren** aus.

6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
	Datum und Uhrzeit zum Aktivieren des Plugins.

Automatische Übersetzung

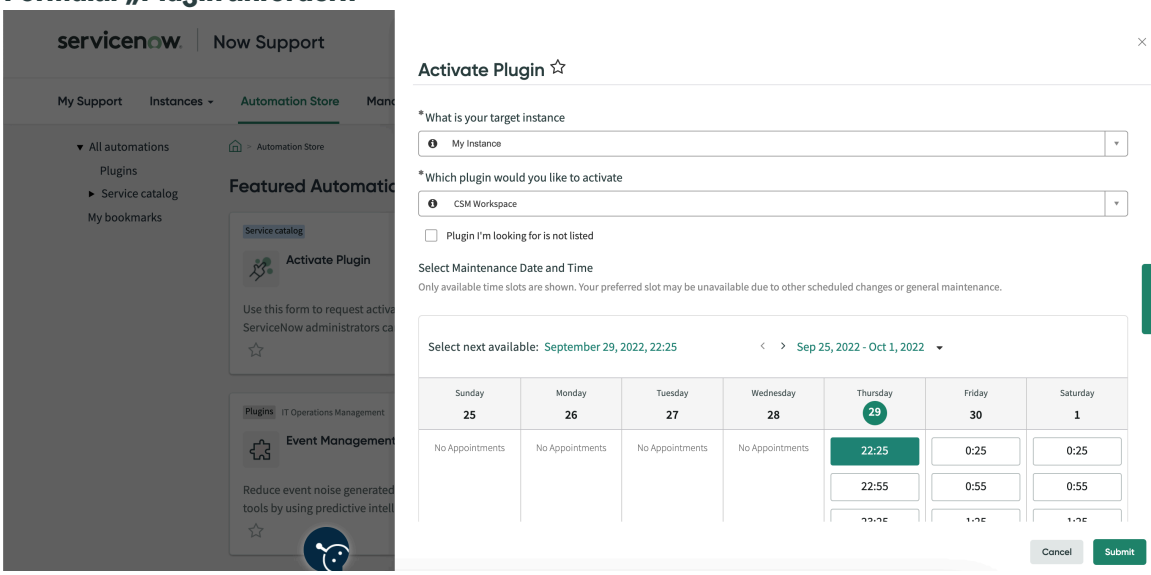
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	**Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Plugins aus dem Servicekatalog anfordern [KB0751715] im Now Support Knowledge Base.

Benutzerkonto für die Edge Encryption einrichten

Die Edge Encryption Proxys stellen als Benutzer eine Verbindung mit der Instanz her, um Informationen zur Verschlüsselungskonfiguration zu erhalten und zu aktualisieren. Erstellen Sie zu diesem Zweck ein Benutzerkonto, und weisen Sie dem Benutzer die Edge Encryption-Rolle zu.

Vorbereitungen

Das Edge Encryption Plugin muss installiert sein, bevor Sie die Rolle zuweisen können.

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie auf Ihrer ServiceNow-Instanz ein Benutzerkonto, das von den Edge Encryption Proxy-Anwendung verwendet werden soll.
2. Weisen Sie dem Benutzer die edge_encryption-Rolle zu.

Proxy-Server für die Edge Encryption herunterladen

Laden Sie die Edge Encryption Proxy-Server-Anwendung aus Ihrer Instanz herunter, und kopieren Sie die Datei auf jeden Computer, auf dem der Edge Encryption Proxy-Server ausgeführt werden soll.

Vorbereitungen

Bevor Sie dieses Verfahren starten, muss das Edge Encryption Plugin auf Ihrer Instanz installiert und aktiviert sein.

Hinweis:
Der Proxy Edge Encryption wird offiziell nur von Oracle JRE unterstützt.

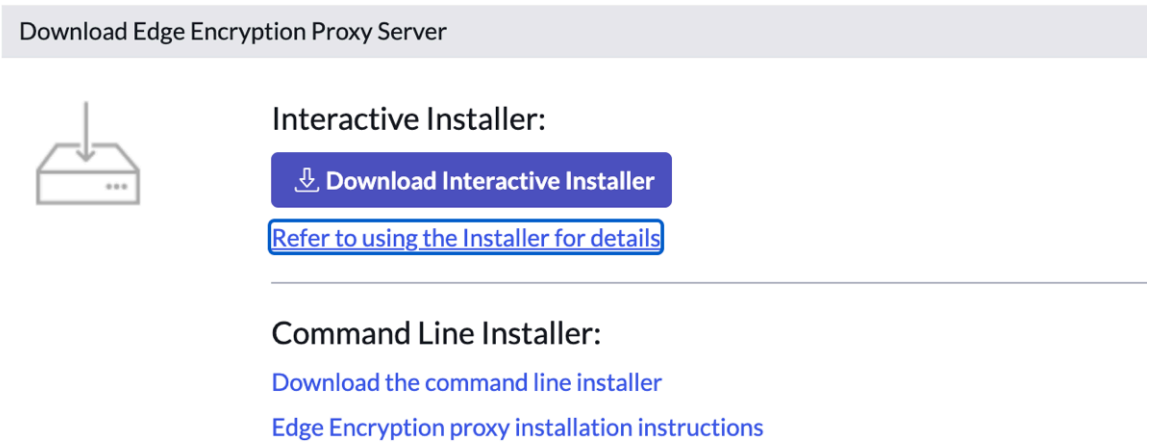
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**.
2. Um das interaktive Installationsprogramm zu verwenden, klicken Sie auf **Interaktives Installationsprogramm herunterladen**.

   Wenn Sie den Proxy-Server manuell installieren, wählen Sie die Betriebssystemversion für Ihren Proxy-Server aus.



Hinweis:
Da der Proxy-Server mindestens 4 GB Arbeitsspeicher zum Ausführen benötigt, werden 32-Bit-JREs und 32-Bit-Betriebssysteme ab dem Release Washington DC nicht mehr unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Kopieren Sie das Installationsprogramm auf jeden Computer, auf dem der Edge Encryption Proxy-Server ausgeführt werden soll.

Hinweis:
Wenn Sie den Proxyserver Edge Encryption manuell installieren, kopieren Sie die ZIP-Datei auf alle Computer, auf denen der Proxyserver Edge Encryption ausgeführt werden soll.

Nächste Maßnahme

Nach dem Herunterladen des Edge Encryption Installationsprogramms, Den Proxy-Server für die Edge Encryption mithilfe des interaktiven Installationsprogramms installieren. Bei manueller Installation, Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren.

Den Proxy-Server für die Edge Encryption mithilfe des interaktiven Installationsprogramms installieren

Installieren Sie den Edge Encryption Proxy-Server auf einem Windows- oder Linux-Computer mit dem interaktiven Installationsprogramm.

Vorbereitungen

Hinweis:
SafeNet KeySecure-Keystore-Dateien werden vom Edge Encryption Installationsprogramm nicht unterstützt. So verwenden Sie einen SafeNet KeySecure-Keystore: Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren.

Das Edge Encryption Plugin muss in Ihrer Instanz installiert und aktiviert sein, bevor Sie dieses Verfahren starten. Stellen Sie sicher, dass Java Version 11.0.6 oder höher auf dem Computer installiert ist, auf dem das Installationsprogramm Edge Encryption ausgeführt wird.

Erforderliche Rolle:

- security_admin auf Ihrer ServiceNow Instanz
- Lokaler oder Domänenadministrator auf einem Windows-Host
- Service-Benutzer mit vollem Dateisystemzugriff auf einem Linux-Host

Warum und wann dieser Vorgang ausgeführt wird

Nach der Installation eines neuen Proxy-Servers können Sie das Installationsprogramm erneut zur Durchführung von Tests ausführen, um Probleme bei der Installation zu erkennen oder die aktuellen Einstellungen zu ändern. Folgende Optionen stehen zur Verfügung:

- **Neu installieren**: Installieren Sie einen neuen Proxy-Server.
- **Installation überprüfen**: Führen Sie Tests durch, um Probleme bei einer früheren Installation zu erkennen und zu beheben.
- **Vorhandene neu installieren**: Führen Sie Tests durch, um Probleme in einer früheren Installation zu erkennen und zu beheben und vorhandene Einstellungen anzuzeigen oder zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie den Proxy-Server auf einem Linux-Computer an einem privilegierten Port (Port 80 oder 443) installieren, müssen Sie das Installationsprogramm als Root-Benutzer mit vollem Dateisystemzugriff ausführen. Um den Dateisystemzugriff nach der Installation des Proxy-Servers einzuschränken, können Sie die SetUID-Funktion im Proxy-Installationsprogramm verwenden. Um diese Funktion zu aktivieren, starten Sie das Installationsprogramm als „Root“ oder „Sudo Root“. Wenn Sie vom Installationsprogramm dazu aufgefordert werden, geben Sie den Benutzernamen und die Benutzergruppe eines nicht privilegierten Benutzers an. Der Proxy-Server wird mit den Dateisystemberechtigungen des angegebenen Benutzers installiert. Sie können diesen Schritt überspringen, um die Standardinstallation mit Root-Berechtigungen fortzusetzen.

Prozedur

Verwenden Sie das Installationsprogramm, um mehrere Proxys für Ihre Instanz auf mehreren Computern zu installieren. Stellen Sie dabei sicher, dass die folgenden Kriterien zutreffen:

- Alle Proxys müssen über dieselben Verschlüsselungsschlüssel und das gleiche RSA-Schlüsselpaar verfügen, mit dem Verschlüsselungskonfigurationen und -regeln digital signiert werden.
- Der Verschlüsselungsschlüssel muss der in der Instanz konfigurierte Standardschlüssel sein.
- Wenn eine Proxy-Datenbank als Teil der Installation eingerichtet wird, müssen alle Proxys dieselbe Proxy-Datenbank verwenden.

  Möglicherweise benötigen Sie eine Proxy-Datenbank für die gleichstellungserhaltende Verschlüsselung, die ordnungserhaltende Verschlüsselung oder Tokenisierung. Wenn keine dieser Funktionen verwendet wird, benötigen Sie keine Proxy-Datenbank.

Nächste Maßnahme
Informationen zur Verwendung von NVDA, einem Bildschirmleser für unterstützende Technologien, der zum Lesen von barrierefreien Java-Anwendungen entwickelt wurde, die für Tastaturbenutzer entwickelt wurden, finden Sie unter Windows 64-Bit-Host für die Verwendung von 32-Bit-NVDA mit Java-Anwendungen konfigurieren .

Legen Sie nach der Installation des Proxy-Servers Edge Encryptiondas anfängliche Arbeitsspeicherlimit und das obere Arbeitsspeicherlimit des Proxy-Servers fest.

Den Edge Encryption Proxy-Server (interaktives Installationsprogramm) installieren

Installieren Sie den Edge Encryption Proxy auf einem Windows- oder Linux-Computer.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Den Proxy-Server für die Edge Encryption herunterladen.
2. Öffnen Sie das Edge Encryption Proxy-Installationsprogramm.

Hinweis:
Bei der Installation auf einem Windows-Computer müssen Sie das Installationsprogramm als Administrator ausführen.

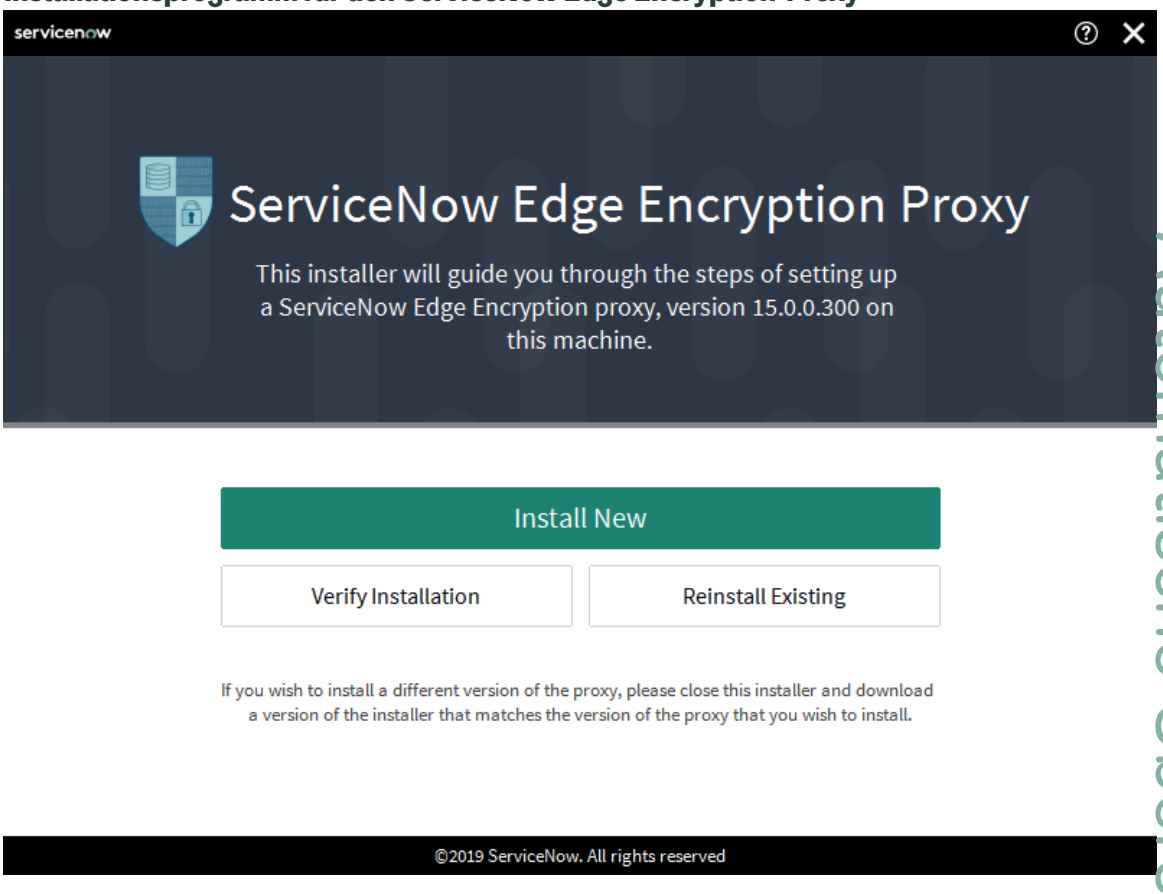
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um das Installationsprogramm als Administrator auf einem Windows-Computer auszuführen, klicken Sie mit der rechten Maustaste auf die Eingabeaufforderung, und wählen Sie **Als Administrator ausführen**.

b. Navigieren Sie in der Befehlszeile zu dem Verzeichnis, in dem sich die heruntergeladene JAR-Datei befindet.

c. Führen Sie den folgenden Befehl aus: `java -jar <Dateiname>.jar`.

Installationsprogramm für den ServiceNow Edge Encryption-Proxy



3. Um einen neuen Proxy-Server zu installieren, wählen Sie **Neu installieren**.
Wenn bereits ein Proxy installiert ist, können Sie das Installationsprogramm folgendermaßen ausführen:

- **Installation überprüfen**: Führen Sie Tests durch, um Probleme bei einer früheren Installation zu erkennen und zu beheben.
- **Vorhandene neu installieren**: Führen Sie Tests durch, um Probleme in einer früheren Installation zu erkennen und zu beheben und vorhandene Einstellungen anzuzeigen oder zu ändern.

4. Konfigurieren Sie **Installationsort** und **ServiceNow-Zielinstanz**.

a. Klicken Sie **Durchsuchen**, um einen Installationsort zu wählen, oder geben Sie manuell einen Installationspfad ein.

b. Geben Sie die URL der ServiceNow Zielinstanz ein.
Geben Sie das Protokoll und die Portnummer an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example
https://example.servicenow.com:443

c. Geben Sie den Benutzernamen und das Passwort für einen Benutzer mit der Rolle „edge_encryption“ auf der ServiceNow Zielinstanz ein.

5. Klicken Sie auf **Weiter**.
6. Konfigurieren Sie die **Verbindungseinstellungen** und **Proxy-Einstellungen**.

Einstellung	Beschreibung
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. **Hinweis:** Klicken Sie auf **FQDN erkennen**, um nach dem vollständig qualifizierten Domänennamen des Computers suchen und das Feld **Proxy-Host** automatisch auszufüllen. Zusammen mit dem Port definiert diese Eigenschaft die URL, die der Client für den Zugriff auf den Proxy-Server verwendet.
HTTP-Port	Port auf dem Proxy für die HTTP-Kommunikation.
HTTPS-Port	Port auf dem Proxy für die HTTPS-Kommunikation.
Proxy-Name	Proxy- und Service-Name. Der Proxy-Name muss eindeutig sein.
Proxy-Abrufintervall	Abrufintervall in Sekunden. Bei der Standardeinstellung dauert es 5 Sekunden, bis Änderungen der Verschlüsselungskonfiguration den Proxy-Server erreichen. Größere Werte führen dazu, dass die Instanz länger braucht, um Online-Proxys zu erkennen. **Hinweis:** Das Ändern der Standardeinstellung des Proxy-Abrufintervalls kann zu Erkennungsverzögerungen führen, wenn ein Proxy online geschaltet wird.
Proxy-Keep-Alive-Ping-Intervall	Zeit in Sekunden zwischen den vom Proxy an die Instanz ausgegebenen Pings. Pings werden regelmäßig ausgegeben, um die Verbindung zwischen dem Proxy und der Instanz zu überprüfen. Der Standardwert ist 10. Der Mindestwert ist 5.

7. Klicken Sie auf **Installieren**.
Der Edge Encryption Proxy-Server installiert. Die Installation kann einige Minuten in Anspruch nehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CyberArk-Eigenschaftsschutz konfigurieren

Konfigurieren Sie optional den CyberArk-Eigenschaftsschutz für das sichere Speichern der Edge Encryption-Passwörter in einem zentralen und sicheren digitalen Tresor.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen CyberArk AIM (Application Identity Management) erwerben und konfigurieren, bevor Sie CyberArk-Verbindungsparameter und geschützte Anmeldeinformationen für einen Proxy-Server konfigurieren können. Im Rahmen der Installation des AIM-Clients wird die Datei JavaPasswordSDK.jar im Installationsverzeichnis des AIM-Clients installiert. Der CyberArk-Tresor wird auf einem unabhängigen gehärteten Server installiert, und die AIM-Clients ermöglichen einen sicheren Zugriff auf diesen Server.

Hinweis:
Sie müssen den CyberArk AIM-Client auf jedem Host-Computer installieren, auf dem ein Edge-Proxy installiert ist.

Im Edge-Installationsprogramm müssen Sie den Speicherort der Datei JavaPasswordSDK.jar angeben, um die CyberArk-Verbindung zum Edge-Proxy einzurichten. Sie müssen auch andere Werte eingeben, die Sie während der Installation des AIM-Clients definiert haben.

Das Einrichten des CyberArk-Passwortspeichers ist optional. Wenn Sie den CyberArk-Passwortspeicher nicht einrichten möchten, klicken Sie auf den CyberArk-Bildschirmen auf **Überspringen**.

Prozedur

1. Auf der CyberArk Connection-Seite des Edge Encryption-Installationsprogramms geben Sie die CyberArk-Verbindungsparameter ein.

CyberArk-Verbindungsparameter

Einstellung	Beschreibung
Pfad zu PasswordSDK.jar	Der Pfad zur Datei JavaPasswordSDK.jar, die während der CyberArk-Konfiguration auf dem Windows-Hostcomputer installiert wurde.
App-ID	Die bei der CyberArk-Konfiguration eingegebene **App-ID**.
Safe-Name	Der bei der CyberArk-Konfiguration eingegebene **Safe-Name**.

2. Klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite „CyberArk-geschützte Anmeldeinformationen“ des Installationsprogramms die Anmeldeinformationen ein, die von CyberArk geschützt werden sollen.
   - Um einen einzigen Anmeldeinformationsnamen für alle geschützten Passwörter zu verwenden, wählen Sie die Checkbox **Einen Anmeldeinformationsnamen für alle Anmeldeinformationen anwenden**, geben Sie den Anmeldeinformationsnamen ein, und klicken Sie auf **Übernehmen**.
   - Geben Sie den Anmeldeinformationsnamen für eines oder mehrere der folgenden Felder ein. Anmeldeinformationsnamen sind die Benutzernamen, die während der CyberArk-Konfiguration für die SSH-Schlüssel eingegeben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CyberArk-geschützte Anmeldeinformationen

Einstellung	Beschreibung
Edge Encryption-Benutzer	Der CyberArk-Anmeldeinformationsname für einen Edge Encryption-Benutzer.
Schlüsselspeicher des Signaturschlüssels	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher des Signaturschlüssels.
HTTPS Cert-Schlüsselspeicher	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher der HTTP-Zertifizierung.
Schlüsselspeicher des Verschlüsselungsschlüssels	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher des Verschlüsselungsschlüssels.
Datenbank	Der CyberArk-Anmeldeiinformationsname für den Datenbankschlüsselspeicher.
SafeNet HTTPS Cert-Schlüsselspeicher	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher der SafeNet HTTP-Zertifizierung.
SafeNet-Server	Der CyberArk-Anmeldeinformationsname für den SafeNet-Server.
Forward Proxy	Der CyberArk-Anmeldeinformationsname für den Forward Proxy.

4. Klicken Sie auf **Weiter**.

Den Signaturschlüssel konfigurieren

Konfigurieren Sie den Signaturschlüssel nach der Installation des Proxy-Servers über das Edge Encryption Proxy-Installationsprogramm.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der Signaturschlüssel kennzeichnet Änderungen an Konfigurationen und Eigenschaften, die vom Proxy-Server vorgenommen werden. Der Signaturschlüssel muss ein asymmetrisches RSA-Schlüsselpaar in einem JCEKS KeyStore sein.

Hinweis:
Bei der Installation mehrerer Proxys muss jeder Proxy denselben Signaturschlüssel verwenden.

Prozedur

1. Wählen Sie auf der Seite „Signaturschlüssel“ des Edge Encryption Installationsprogramms den Schlüsselspeicher auf dem Host-Computer aus, um den Signaturschlüssel zu speichern.
   - **Einen neuen Java KeyStore erstellen**: Geben Sie Verzeichnisspeicherort, Name und Passwort für den neuen Keystore ein.
   - **Vorhandenen Keystore verwenden**: Geben Sie den Speicherort und das Passwort der Keystore-Datei ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie einen Signaturschlüssel aus oder erstellen Sie ihn.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Neuer Schlüssel**: Erstellen Sie einen Signaturschlüssel für diesen Proxy.
- **Vorhandenen Schlüssel verwenden**: Verwenden Sie ein RSA-Schlüsselpaar aus dem ausgewählten Schlüsselspeicher.
- **Vorhandenen Schlüssel importieren**: Importieren Sie ein RSA-Schlüsselpaar aus einem anderen Schlüsselspeicher. Navigieren Sie zur Keystore-Datei, geben Sie das Passwort für den Keystore ein und wählen Sie den Schlüsselalias aus. Geben Sie einen neuen Alias für den Schlüssel an.

4. Klicken Sie auf **Weiter**.

Das HTTPS-Zertifikat konfigurieren

Um Clients die Verbindung zum Edge Encryption Proxy-Server über eine sichere SSL-Verbindung zu ermöglichen, importieren Sie das HTTPS-Zertifikat in den Proxy-Server.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der Edge Encryption Proxy stellt das HTTPS-Zertifikat für Clients bereit, die versuchen, eine Verbindung herzustellen.

Prozedur

1. Wählen Sie auf der Seite „HTTPS-Zertifikat“ des Edge Encryption Installationsprogramms den Schlüsselspeicher zum Speichern des Zertifikats aus.
   - **Einen neuen Java KeyStore erstellen**: Geben Sie Verzeichnisspeicherort, Name und Passwort für den neuen Keystore ein.
   - **Vorhandenen Keystore verwenden**: Geben Sie den Speicherort und das Passwort der Keystore-Datei ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie ein Zertifikat aus oder importieren Sie es.
   Der Schlüsselalias ist der angegebene Alias für das Zertifikat.
   - **Vorhandenes Zertifikat verwenden**: Verwenden Sie ein vorhandenes Zertifikat im ausgewählten Schlüsselspeicher.
   - **Aus Datei oder KeyStore importieren**: Importieren Sie ein Zertifikat aus einem anderen Schlüsselspeicher oder einer CER-Datei. Navigieren Sie zum Keystore oder zur .CER-Datei, geben Sie das Passwort ein und wählen Sie den Alias aus. Sie müssen einen neuen Alias für das Zertifikat angeben.
4. Klicken Sie auf **Weiter**.

Den AES 128-Bit-Verschlüsselungsschlüssel konfigurieren

Nachdem Sie das HTTPS-Zertifikat über das Edge Encryption-Proxy-Installationsprogramm konfiguriert haben, konfigurieren Sie den AES 128-Bit-Verschlüsselungsschlüssel zum Verschlüsseln Ihrer Daten.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der Verschlüsselungsschlüssel ist entweder eine reine Textdatei im /Schlüssel-Verzeichnis oder ein geheimer Schlüssel in einem Schlüsselspeicher. Wenn Sie einen Keystore für Ihre AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel verwenden, müssen beide denselben Keystore verwenden.

Wenn Sie ein SSL-Zertifikat auf einem Edge-Proxy-Server aktualisieren, finden Sie weitere Informationen unter SSL-Zertifikat aktualisieren.

Prozedur

1. Wählen Sie den Ort des Verschlüsselungsschlüssels.
2. Klicken Sie auf **Next (Weiter)**.
3. Wählen oder erstellen Sie den Verschlüsselungsschlüssel.
4. Klicken Sie auf **Next (Weiter)**.
5. Konfigurieren Sie den Schlüssel in der Instanz gemäß den in Ihrem Installationsprogramm definierten Anforderungen.
   Um den Schlüssel in der Instanz zu konfigurieren, navigieren Sie zur Instanz und definieren Sie einen Standardschlüssel. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren. Stellen Sie sicher, dass Schlüsselalias, Größe und Typ den im Installationsprogramm definierten Anforderungen entsprechen.

Standardschlüsselanforderungen

6. Wenn der Schlüssel in der Instanz konfiguriert ist, kehren Sie zum Installationsprogramm zurück und klicken Sie auf **Nächster**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren

Nachdem Sie den AES 128-Bit-Schlüssel über das Edge-Proxy-Installationsprogramm konfiguriert haben, können Sie optional einen AES 256-Bit-Verschlüsselungsschlüssel zum Verschlüsseln Ihrer Daten konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der Verschlüsselungsschlüssel ist entweder eine reine Textdatei im /Schlüssel-Verzeichnis oder ein geheimer Schlüssel in einem Schlüsselspeicher. Wenn Sie einen Schlüsselspeicher für Ihre AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel verwenden, muss für beide Schlüssel derselbe Schlüsselspeicher verwendet werden. Wenn Sie keinen AES-256-Bit-Verschlüsselungsschlüssel konfigurieren möchten, wählen Sie **Überspringen**, um mit der Installation des Proxyservers fortzufahren.

Wenn Sie ein SSL-Zertifikat auf einem Edge-Proxy-Server aktualisieren, finden Sie weitere Informationen unter SSL-Zertifikat aktualisieren.

Prozedur

1. Wählen Sie den Ort des Verschlüsselungsschlüssels.
2. Wählen Sie **Weiter**.
3. Wählen oder erstellen Sie den Verschlüsselungsschlüssel.
4. Wählen Sie **Weiter**.
5. **Wahlweise:** Wenn Sie die AES-256-Bit-Verschlüsselung verwenden möchten, lesen Sie Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.
6. Um die AES-256-Bit-Verschlüsselung zu verwenden, müssen Sie auch den AES-256-Bit-Standardverschlüsselungsschlüssel für die Instanz konfigurieren.

   Navigieren Sie dazu zur -Instanz und definieren Sie einen Standardschlüssel. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren. Stellen Sie sicher, dass Schlüsselalias, Größe und Typ den im Installationsprogramm definierten Anforderungen entsprechen.
7. Nachdem der Schlüssel für die Instanz konfiguriert wurde, kehren Sie zum Installationsprogramm zurück, und wählen Sie **Weiter**aus.

Aktualisieren Sie das SSL-Zertifikat

Wenn Sie ein SSL-Zertifikat auf einem Edge-Proxy-Server aktualisieren, müssen Sie das alte Zertifikat löschen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie das SSL-Zertifikat auf dem Edge-Proxy-Server aktualisieren, müssen Sie auch das alte Zertifikat löschen. Andernfalls wird das alte Zertifikat (in Form eines Alias in der KeyStore-Datei) weiterhin verwendet, obwohl der Edge-Proxy-Server für die Verwendung des neuen Zertifikats konfiguriert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Listen Sie auf dem Edge-Proxy-Server die Einträge im Java KeyStore auf:

```
keytool -list -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
```

2. Entfernen Sie das alte SSL-Zertifikat:

```
keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype jceks -storepass
 MY_SUPER_PASSWORD
```

3. Fügen Sie das neue SSL-Zertifikat dem Java KeyStore hinzu.

Die Proxy-Datenbank für die Edge Encryption konfigurieren

Bei Verwendung von ordnungserhaltenden Verschlüsselungstypen oder Verschlüsselungsmustern können Sie optional die Edge Encryption-Proxy-Datenbankeigenschaften konfigurieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Für die Verwendung von bestandserhaltenden Verschlüsselungstypen oder Verschlüsselungsmustern ist eine in Ihrem Netzwerk ausgeführte MySQL-Datenbank erforderlich. Diese Aufgabe verbindet den Proxy mit der Datenbank, die Datenbank wird jedoch nicht installiert oder konfiguriert.

Hinweis:
Wenn Sie mehrere Proxy-Server verwenden, müssen alle Proxy-Server dieselbe Proxy-Datenbank verwenden. Die im Installationsprogramm eingegebenen Werte müssen für alle Proxy-Server gleich sein.

Prozedur

1. Bestätigen oder ändern Sie die Datenbank-URL, die den Speicherort der Proxy-Datenbank darstellt.
2. Geben Sie im Feld **Name** den Namen der Proxy-Datenbank ein.
   Der Standardwert ist *`edgeencryption`*.
3. Geben Sie den Benutzernamen und das Passwort für den Zugriff auf die Proxy-Datenbank ein.
4. Klicken Sie auf **Weiter**.

Den Proxy-Server der Edge Encryption starten

Nach dem Installieren und Konfigurieren eines Edge Encryption Proxys kann der Proxy aus dem Installationsprogramm gestartet werden.

Vorbereitungen

Erforderliche Rolle: admin

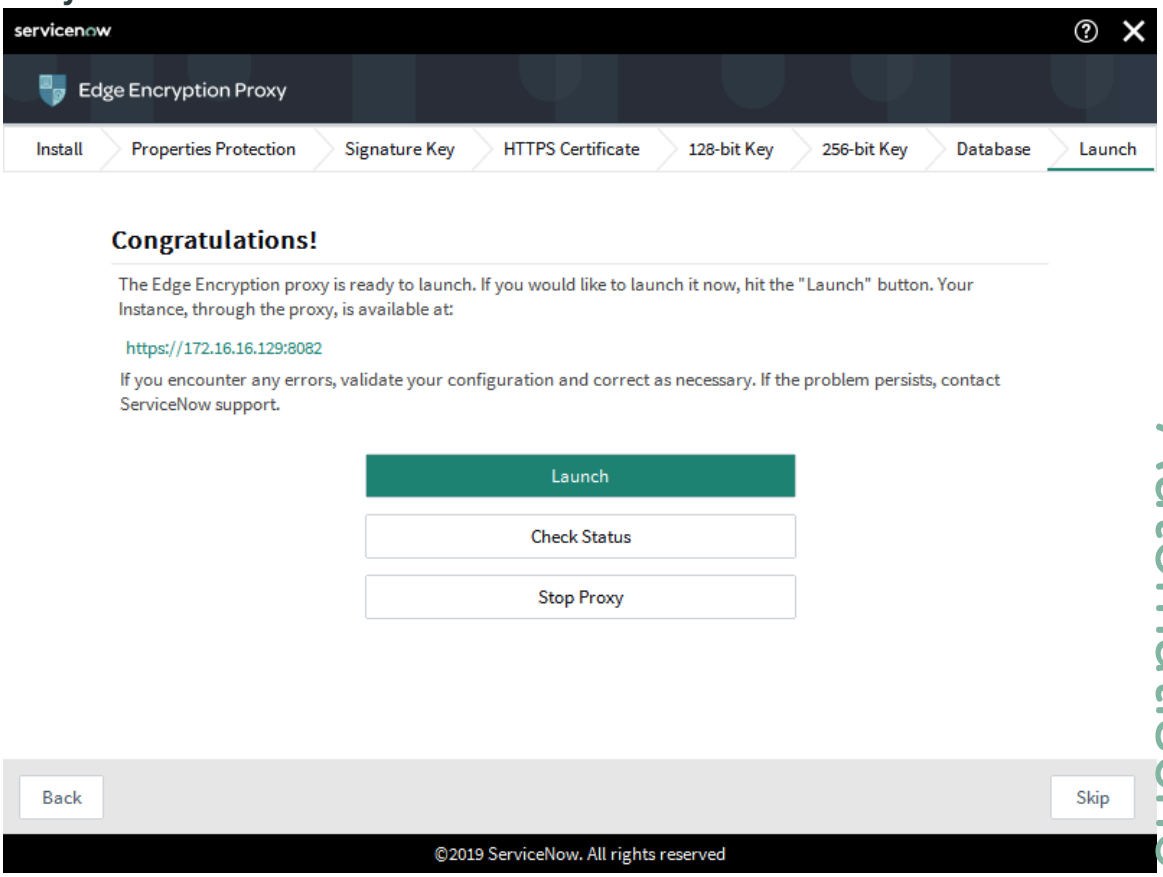
Prozedur

1. Kehren Sie nach der Konfiguration der Schlüssel für die Instanz und der Proxy-Datenbank zum Proxy-Installationsprogramm Edge Encryption zurück, und klicken Sie auf **Starten**.
2. Sie können bei Erkennen eines Problems oder zur Statusprüfung Ihres Proxy-Servers auf **Status prüfen**, um zu überprüfen, ob der Proxy ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Meldung zeigt den Proxy-Status an.

Proxy-Status



Nächste Maßnahme

Nach erfolgreicher Installation des Edge Encryption Proxy-Servers, Die anfängliche Speichergrenze des Proxy-Servers und die obere Grenze des Speicherbereichs festlegen.

Überprüfen Sie die Installation des Proxy-Servers für die Edge Encryption, und führen Sie eine Fehlerbehebung durch.

Nach dem Installieren des Edge Encryption Proxy können Sie die Installation überprüfen, um Probleme zu lokalisieren oder den Proxy zu starten und zu stoppen.

Vorbereitungen

Erforderliche Rolle: admin

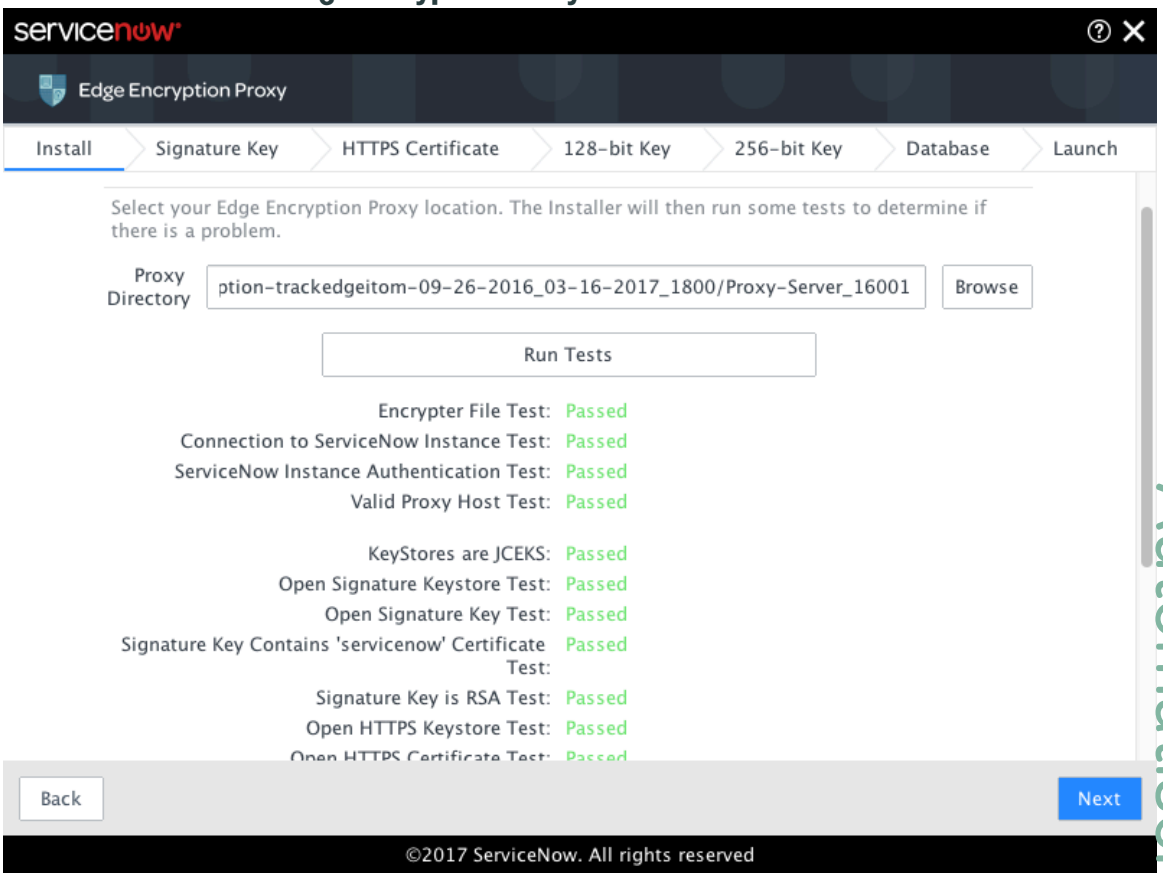
Prozedur

1. Öffnen Sie das Edge Encryption Proxy-Installationsprogramm.
2. Wählen Sie **Installation überprüfen**.
3. Klicken Sie auf **Proxy-Verzeichnis** und wählen Sie das Proxy-Verzeichnis.
4. Klicken Sie auf **Tests ausführen**.
   Testergebnisse werden angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installationstests des Edge Encryption-Proxy



5. Klicken Sie auf **Weiter**.
   Wenn ein Problem auftritt, können Sie das Installationsprogramm durchlaufen, um die Konfiguration zu korrigieren. Wenn keine Probleme auftreten, springt der Installer zur Seite **Starten**. Sie können den Proxy-Status überprüfen, den Proxy stoppen oder den Proxy aus der **Starten**-Seite starten.

Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren

Installieren Sie manuell mehrere Edge Encryption Proxy-Server in Ihrem Netzwerk.

Vorbereitungen

Erforderliche Rollen: security_admin auf Ihrer ServiceNow-Instanz und lokaler Administrator auf dem Host-Computer.

Wenn ordnungserhaltende Verschlüsselungstypen oder Verschlüsselungsmuster verwendet werden sollen, richten Sie eine MySQL-Datenbank auf einem Computer in Ihrem Netzwerk ein, sofern noch nicht vorhanden.

Hinweis:
Wenn Sie Verschlüsselungsschlüssel von Unbound Technology mit Edge Encryptionverwenden, installieren Sie den Proxyserver mit dem Befehlszeilen-Installationsprogramm auf dem ungebundenen Clientcomputer. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound-Technology-Client ausgeführt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Richten Sie einen Edge Encryption -Proxy-Server ein.
2. Stellen Sie sicher, dass der Proxy-Server erfolgreich ausgeführt wird.
3. Fügen Sie zusätzliche Proxy-Server für eine Instanz hinzu.
   Zusätzliche Server sorgen für eine optimale Umgebung. Unter Umgebungsgröße Ihrer Edge Encryption anpassen erfahren Sie, wie viele zusätzliche Proxy-Server benötigt werden.

Den Proxy-Server für die Edge Encryption installieren (Befehlszeilen-Installationsprogramm)

Installieren Sie einen Edge Encryption Proxy auf einem 64-Bit-Windows- oder Linux-Computer.

Vorbereitungen

Erforderliche Rolle: admin

Zum Ausführen des Installationsprogramms ist Java Version 11.0.6 oder höher in der 11.x-Versionsserie erforderlich.

Warum und wann dieser Vorgang ausgeführt wird

Installieren Sie den Edge Encryption Proxy-Server auf einem Computer in Ihrem Netzwerk mit dem entsprechenden Befehl für Ihren Zielcomputer. Bei der Installation des Edge Encryption Proxy-Servers auf einem Windows-Computer muss der Proxy-Server zusätzlich als Windows-Service installiert werden.

Wenn Sie den Proxy-Server der Edge Encryption aktualisieren, sichert das System den alten Proxy im Verzeichnis backup.dist-upgrade-<timestamp> unter dem aktuellen Installationsverzeichnis. Das Sicherungsverzeichnis wird während des Upgrade-Vorgangs erstellt und speichert die alten Proxy-Informationen.

Wenn Sie ein Upgrade über die Befehlszeile ausführen, kann eine dist-upgrade.log in dem Verzeichnis erstellt werden, in dem der Befehl ausgeführt wird. Das dist-upgrade.log enthält Protokolle für den Upgrade-Vorgang.

Bei einem fehlgeschlagenen Upgrade erstellt das System ein Verzeichnis failed-backup.dist-upgrade-<timestamp>. Zusätzlich kann logs/wrapper.log im ursprünglichen Proxy-Verzeichnis auch Fehlerinformationen enthalten.

Prozedur

1. Erstellen Sie das Installationsverzeichnis.
2. Laden Sie die Edge Encryption Proxy-Archivdatei in das Installationsverzeichnis herunter.
3. Öffnen Sie das Terminal und wechseln Sie in das Installationsverzeichnis.

> **Hinweis:**
> Bei der Installation auf einem Windows-Computer müssen Sie die Windows-Eingabeaufforderung mit Administratorrechten starten.

4. Führen Sie diesen Befehl für den Zielcomputer aus und ändern Sie die Variablen entsprechend Ihrer Konfiguration: `java -jar edgeencryption-<version>-all.jar -m install -n <ProxyName> --instancehost <host> -p <InstancePort> --protocol https`

Option	Variable	Beschreibung
Keine	Version	Versionsnummer des Edge Encryption Proxy, der zur

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Variable	Beschreibung
		Ausführung der aktuellen Operation verwendet wird.
-m	Modus	Die Operation oder der Modus, in dem ausgeführt werden soll (Installation oder Dist-Upgrade).
-n	ProxyName	Der Name der Verschlüsselungs-Proxy-Instanz. Verwenden Sie einen eindeutigen ProxyName, um bestimmte Proxy-Instanzen identifizieren zu können.
--instancehost	host	Der Hostname Ihrer ServiceNow-Instanz (z. B. mycompany.service-now.com).
-p	InstancePort	Der Port Ihrer Instanz. Bei Protokoll https ist der Port normalerweise 443.
--protocol	protocol	Das für den Zugriff auf Ihre ServiceNow-Instanz verwendete Protokoll (in der Regel https).

Hinweis:
Kopieren Sie keine Befehle aus dem Browser. Gelegentlich führen Kopier- / Einfügevorgänge dazu, dass unerwartete Zeichen auf dem Zielcomputer eingefügt werden und der Befehl falsch ausgeführt wird. Es ist am besten, den Befehl von Hand anhand der Dokumentation als Referenz einzugeben.

Um den Hilfebildschirm anzuzeigen, führen Sie diesen Befehl ohne Argumente aus: `java -jar edgeencryption-<version>-all.jar`

5. Beim Installieren auf einem Windows-Computer installieren Sie den Edge Encryption Proxy als Windows-Dienst.

   a. **Wahlweise:** Ändern Sie den Namen des Service, indem Sie die Datei conf/wrapper.conf auf dem neuen Proxy öffnen und die Eigenschaften in der folgenden Tabelle festlegen.

Eigenschaft	Beschreibung
wrapper.ntservice.name	Eindeutiger Name des Edge Encryption Proxy-Service.
wrapper.ntservice.displayname	Anzeigename des Edge Encryption Proxy-Service.
wrapper.ntservice.description (optional)	Beschreibung des Proxy-Server.

   Bei Nichtausführung dieses Schrittes wird der Edge Encryption Proxy-Service unter dem Namen **Edge Encryption** installiert.

   b. Speichern und schließen Sie die Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Öffnen Sie die Windows-Eingabeaufforderung und cd zu ServerName_port/bin.

d. Führen Sie edgeencryption.bat installieren aus.

Ergebnisse

Das Verzeichnis ProxyName_port wird im aktuellen Verzeichnis erstellt. Die Datei edgeencryption.properties wird mit den Host-, Port- und Protokollwerten über die Befehlszeile aktualisiert.

Das RSA-Schlüsselpaar für die digitale Signatur erstellen und konfigurieren

Erstellen Sie ein RSA-Schlüsselpaar, mit dem der Proxy-Server die digitale Signatur zum Signieren von Änderungen an den Verschlüsselungseigenschaften und der Konfiguration erstellen kann.

Vorbereitungen

Erforderliche Rolle: admin

Um die digitale Signatur zu erstellen und zu validieren, muss ein RSA-Schlüsselpaar generiert und im JCEKS Java KeyStore gespeichert werden, und jeder Proxy muss für die Verwendung dieses Schlüsselpaares konfiguriert sein. Generieren Sie ein Verschlüsselungsschlüsselpaar mit dem Befehl keytool.

Um das Dienstprogramm keytool mit einem auf SElinux installierten Proxy (CentOS) verwenden zu können, müssen Sie das Laden gemeinsam genutzter Bibliotheken aus dem Proxy-Java-Installationsverzeichnis aktivieren. Führen Sie dazu den folgenden Befehl als Root aus.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter <proxy install dir>java/jre/bin/keytool.

Prozedur

1. Wechseln Sie in das KeyStore-Verzeichnis im Proxy-Download-Verzeichnis.

2. Ändern Sie das Standardpasswort.

Das Standardpasswort lautet *changeme*.

```
keytool -keystore keystore.jceks -storetype jceks -storepasswd -new <newpassword>
```

3. Erstellen Sie ein Verschlüsselungsschlüsselpaar.

> **Hinweis:**
> Geben Sie kein Passwort für den Schlüssel ein, wenn das keytool-Dienstprogramm zur Eingabe auffordert.

Geben Sie diesen Befehl in einer einzigen Zeile ein.

```
keytool -genkeypair -alias <key alias> -keyalg rsa -keystore keystore.jceks
-storetype jceks -storepass <keystore password> -keysize 2048
```

4. Aktualisieren Sie die Eigenschaftsdatei des Verschlüsselungsproxys (edgeencryption.properties).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wechseln Sie in das Verzeichnis <installation directory>/conf/.

b. Öffnen Sie die Datei edgeencryption.properties.

c. Geben Sie die Eigenschaften für die Digitale Signatur ein.

Diese Eigenschaften müssen für alle Proxys gleich sein.

5. Speichern und schließen Sie die Datei edgeencryption.properties.

Das Zertifikat für eine sichere SSL-Verbindung importieren und konfigurieren

Um eine sichere SSL-Verbindung zu verwenden, importieren Sie ein Serverzertifikat und fügen es zum Java KeyStore hinzu.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen das Serverzertifikat und den passenden privaten Schlüssel abrufen, bevor Sie ihn dem Java KeyStore hinzufügen.

Prozedur

1. Generieren Sie eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) mit dem OpenSSL-Befehl.

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

2. Senden Sie Ihre CSR (im Beispiel oben MYCSR.csr) an Ihre Zertifizierungsstelle, um sie signieren zu lassen.
3. Erstellen Sie mit dem OpenSSL- Befehl einen P12-Schlüsselspeicher für den Import.

```
openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name shared >
 MY_SERVER.p12
```

4. Speichern Sie Ihr Zertifikat und Ihren privaten Schlüssel in einer jceks-Datei.

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -srckeystore
 MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```

Der Alias, im Beispiel als MYALIAS dargestellt, kann ein beliebiger Wert sein. Sie verwenden diesen Alias in der Eigenschaft „ edgeencryption.proxy.https.cert.alias “ in der Datei „edgeencryption.properties “ im<installation directory> Ordner /conf/

5. Halten Sie den Edge-Proxy an, und starten Sie ihn neu.

Hinweis:
Während eines Neustarts ist der Proxy-Server für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

Schlüsselspeicher und Verschlüsselungsschlüssel einrichten

Richten Sie den vom Edge Encryption Proxy Server verwendeten Schlüsselspeicher und die Verschlüsselungsschlüssel ein.

Vorbereitungen

Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Bestimmen Sie sorgfältig den geeigneten Keystore-Typ entsprechend den Anforderungen Ihres Unternehmens.

Unterstützter Keystore	Beschreibung
Dateispeicher	Die Schlüssel werden in einer Datei in einem Dateisystem gespeichert, auf das der Edge Encryption Proxy-Server zugreift. In einer Datei gespeicherte Verschlüsselungsschlüssel werden nicht verschlüsselt. Der Schutz dieser Dateien liegt daher in Ihrer Verantwortung.
Java KeyStore	Ein Java KeyStore: ○ Speichert Schlüssel in einem Java JCEKS KeyStore. ○ Ist passwortgeschützt und sicherer als das Speichern von Schlüsseln in einer Datei im Dateisystem. ○ Kann mehrere Schlüssel speichern. Ein Schlüsselalias repräsentiert jeden Schlüssel, was die Verwaltung mehrerer Schlüssel erleichtert. Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen keystore.jceks im Verzeichnis Schlüsselspeicher geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.
Enterprise Key Management (EKM)	**SafeNet KeySecure** Schlüssel werden mit der Schlüsselverwaltung von SafeNet KeySecure gespeichert und abgerufen. Sie müssen eine Lizenz von Gemalto erwerben, die Bibliotheken herunterladen und den SafeNet KeySecure-Schlüsselspeicher auf einem Host-Computer in Ihrem Netzwerk installieren, bevor Sie den Schlüsselspeicher auf dem Edge Encryption Proxy-Server konfigurieren. **Unbound Technology** Der base64-verschlüsselte Wrapped-Verschlüsselungsschlüssel wird als Textdatei auf dem Edge Encryption Proxy-Server gespeichert. Die Implementierung der Unbound Technology (zuvor Dyadic Security) behält die Kontrolle über den Wrapping-Schlüssel. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound-Technology-Client ausgeführt werden.

Hinweis:
Wenn Sie einen anderen Schlüsselspeicher als das Basissystem Java JCEKS KeyStore verwenden, müssen Sie den öffentlichen Schlüssel ServiceNow in Ihren Schlüsselspeicher importieren. Der Alias für den öffentlichen Schlüssel lautet `servicenow`.

2. Richten Sie den Schlüsselspeicher und die Verschlüsselungsschlüssel in Ihrem lokalen Netzwerk ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einen Java KeyStore-Schlüsselspeicher einrichten

Sie können einen Java KeyStore-Schlüsselspeicher zum Speichern von Verschlüsselungsschlüsseln verwenden.

Vorbereitungen
Erforderliche Rolle: admin

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter <proxy install dir>/java/jre/bin/keytool.

Warum und wann dieser Vorgang ausgeführt wird
Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen keystore.jceks im Verzeichnis Schlüsselspeicher geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.

Prozedur

1. Richten Sie die Keystore-Eigenschaften ein.
   a. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
   b. Öffnen Sie die Datei edgeencryption.properties.
   c. Geben Sie die Eigenschaften für den Java KeyStore ein.
2. Speichern und schließen Sie die Datei edgeencryption.properties.

Nächste Maßnahme
Nach dem Einrichten des Java KeyStore, Verschlüsselungsschlüssel mit dem Java KeyStore-Keytool erstellen.

Verschlüsselungsschlüssel mit dem Java KeyStore-Keytool erstellen

Sie können das mit der Verschlüsselungsproxy-Distribution mitgelieferte Keytool verwenden, um AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel zu erstellen.

Vorbereitungen
Erforderliche Rolle: admin

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter <proxy install dir>/java/jre/bin/keytool.

Weitere Informationen zum Keytool-Dienstprogramm finden Sie in der Java SE-Dokumentation .

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Der Java KeyStore erfordert, dass der Aliasname (Schlüsselname, Schlüsselalias) Kleinbuchstaben und Zahlen verwendet.

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/keystore/.
2. Führen Sie einen der folgenden Befehle aus, um den Verschlüsselungsschlüssel zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie diese Befehle aus einem anderen Verzeichnis als dem Keystore-Verzeichnis ausführen möchten, d. h. Sie haben den vorherigen Schritt übersprungen, müssen Sie die Option *-keystore* ändern, um den Pfad von Ihrem aktuellen Verzeichnis zum Keystore-Verzeichnis aufzunehmen. Wenn Sie sich beispielsweise im Verzeichnis <installation directory>\bin befinden, lautet die Option `-keystore ../keystore/keystore.jceks`.

Option	Bezeichnung
AES 128	`keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks`
AES 256	`keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks`

Der Alias wird in der Instanz hinzugefügt, wenn Sie Standardschlüssel zuweisen.

Hinweis:
Das Schlüsselpasswort muss mit dem Schlüsselspeicher-Passwort identisch sein.

Einen SafeNet KeySecure-Schlüsselspeicher einrichten

Wenn Sie einen SafeNet-Schlüsselspeicher verwenden, kopieren Sie einen Satz Bibliotheken in das Proxy-Distributionsverzeichnis.

Vorbereitungen
Erforderliche Rolle: admin

Sie müssen den SafeNet-Schlüsselspeicher installieren und einrichten, bevor Sie diesen Schritt ausführen. Sichern Sie sich eine Lizenz mit Thales, um die Bibliotheken herunterzuladen.

Hinweis:
Für IngrianNAE Version 8.12 müssen Sie auch die Datei `commons-collections.jar` herunterladen

Warum und wann dieser Vorgang ausgeführt wird
Hinweis:
Unter Linux verwenden Dateipfade einen Schrägstrich (/).

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/conf/ directory, und öffnen Sie die Datei edgeencryption.properties.
2. Geben Sie die Eigenschaften für den SafeNet-Schlüsselspeicher ein.

Hinweis:
Sie können den SafeNet-Schlüsselspeicher mit der Benutzername/Passwort-Authentifizierung oder der Client-Zertifikatauthentifizierung konfigurieren, aber nicht mit einer Kombination aus beidem.

Example

Ein Beispiel für einen SafeNet-Schlüsselspeicher mit Authentifizierung mit Benutzername und Passwort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
edgeencryption.nae.user = safenet_user
edgeencryption.nae.password = safenet_password
```

Example

Ein Beispiel für einen SafeNet-Schlüsselspeicher mit Client-Zertifikatsauthentifizierung. Durch diese Authentifizierungsmethode ist das Speichern von Benutzername und Passwort des SafeNet-Servers in der Eigenschaftendatei nicht erforderlich.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name
```

3. Hinzufügen oder Erstellen eines Schlüssels im SafeNet-Schlüsselspeicher.
   Der Schlüsselname (Alias) wird in der Instanz hinzugefügt, wenn Sie Standardschlüssel zuweisen.
4. Speichern und schließen Sie die Datei edgeencryption.properties.

Upgrade von Kingston oder niedriger auf London oder höher

Wenn Sie einen SafeNet NAE-Server für die Schlüsselspeicherung mit Edge verwenden, müssen Sie vor dem Upgrade des Proxys von Kingston oder niedriger auf London oder höher die JAR-Dateien der Gemalto SafeNet Client-ProtectApp kopieren und neue Eigenschaften hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Unter Linux verwenden Dateipfade einen Schrägstrich (/).

Prozedur

1. Kopieren Sie die folgenden Dateien aus<installation directory> /lib zum /nae-Verzeichnis:
   - commons-collections<version> .jar
   - ingrianlog4j-api-<version>.jar
   - ingrianlog4j-core-<version>.jar
   - ingrianNAE-<version>.jar
2. Aktualisieren Sie in der aktuellen Version (nicht aktualisiert) des Proxys<installation directory> /conf/edgeencryption.properties, indem Sie die folgenden zwei Eigenschaften hinzufügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *edgeencryption.ekm.provider.classname* = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
- *edgeencryption.thirdparty.vendor.library.path* =<directory path to the directory where you copied the jar files in step 1>

Hinweis:
edgeencryption.thirdparty.vendor.library.path für Java 11.

3. Speichern Sie die Änderungen.
4. Fahren Sie mit dem Upgrade auf London oder höher fort.

Unbound Technology-Schlüssel einrichten

Verwenden Sie Schlüssel von Unbound Technology (früher: dyadische Sicherheit) mit Edge Encryption, indem Sie den base64-codierten umschlossenen Verschlüsselungsschlüssel als Textdatei auf dem Proxy-Server Edge Encryption] speichern und den Schlüsselalias für die Umschließung angeben. Die Implementierung von Unbound Technology behält die Kontrolle über den Wrapping-Schlüssel.

Vorbereitungen

Erforderliche Rolle: security_admin

Identifizieren Sie in Ihrer Unbound Technology-Implementierung sowohl den Wrapping-Schlüssel als auch den Wrapped-Schlüssel. Verwenden Sie den RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING-Algorithmus für Umbruch und Auffüllung. Exportieren Sie den Wrapped-Schlüssel im base64-codierten Textformat. Speichern Sie die Datei mit dem Schlüsselalias als Namen ohne Dateierweiterung.

Hinweis:
Bei Verwendung der Unbound Technology-Verschlüsselungsschlüssel mit Edge Encryption installieren Sie den Proxy-Server mithilfe des Befehlszeileninstallationsprogramms auf dem Unbound-Client-Computer. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound Technology -Client ausgeführt werden.

Prozedur

1. Fügen Sie den Wrapped-Verschlüsselungsschlüssel im base64-codierten Textformat zum Verzeichnis <proxy-installation-directory>/keys hinzu.
   Der Name der Datei muss der Schlüsselalias ohne Dateierweiterung sein.
2. Aktualisieren Sie die Datei edgeencryption.properties.
   a. Wechseln Sie in das Verzeichnis <proxy-installation-directory>/conf.
   b. Öffnen Sie die Datei edgeencryption.properties.
   c. Geben Sie die Eigenschaften des Dateispeichers ein, und legen Sie den Wert von *edgeencryption.keyfile.directory* auf schlüsselfest.

      Diese Eigenschaft weist den Proxy-Server an, nach dem Verschlüsselungsschlüssel im Verzeichnis <Java-home-directory>/keys zu suchen.

      Weitere Informationen zu Edge Encryption Eigenschaften, siehe Eigenschaften des Proxy-Servers für die Edge Encryption.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Entfernen Sie den Kommentar für die Eigenschaften für die Konfiguration des dyadischen Providers, und legen Sie den Wert `edgeencryption.ekm.provider.rsa.wrapping.key.alias` auf den Schlüsselalias in Ihrer ungebundenen Implementierung fest.

e. Speichern und schließen Sie die Datei.

Nächste Maßnahme

Fügen Sie der Instanz den Aliasnamen der Verschlüsselung hinzu. Der Alias des Verschlüsselungsschlüssels ist der Dateiname des Wrapped-Verschlüsselungsschlüssels, der zum Verzeichnis <proxy-installation-directory>/keys hinzugefügt wurde. Wenn zum Beispiel die Datei im Verzeichnis myunboundkey heißt, fügen Sie diesen Namen zum Feld **Schlüsselalias** hinzu. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren.

Einen in einer Datei gespeicherten Verschlüsselungsschlüssel erstellen

Sie können eine einfache Textdatei als Schlüsselspeicher verwenden. Jede Datei enthält einen einzelnen Verschlüsselungsschlüssel.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Dieser Schritt erstellt sowohl den Schlüsselspeicher als auch den Verschlüsselungsschlüssel.

Hinweis:
Der Name der Schlüsseldatei muss mit dem in der Tabelle der Verschlüsselungsschlüssel der Instanz angegebenen Schlüsselalias übereinstimmen. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren.

Prozedur

1. Erstellen Sie eine Datei im Ordner /keys des Installationsverzeichnisses des Proxy-Servers.
2. Fügen Sie den Verschlüsselungsschlüssel zur Datei hinzu.

Option	Bezeichnung
AES 128	Platzieren Sie den Verschlüsselungsschlüssel (genau 16 Byte) in der Datei.
AES 256	Platzieren Sie den Verschlüsselungsschlüssel (genau 32 Byte) in der Datei.

3. Aktualisieren Sie die Datei edgeencryption.properties.
   a. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
   b. Öffnen Sie die Datei edgeencryption.properties.
   c. Geben Sie die Eigenschaften für den Dateispeicher ein.
   d. Speichern und schließen Sie die Datei.

Verschlüsselungsschlüssel für die Instanz konfigurieren

Edge Encryption bietet die Tools zum Verwalten von Verschlüsselungsschlüsseln, ohne den Proxy offline zu schalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: security_admin

Vor dem Einrichten neuer Verschlüsselungsschlüssel für die Instanz:

1. Erstellen Sie den Verschlüsselungsschlüssel.
2. Stellen Sie den neuen Schlüssel allen Verschlüsselungsproxys zur Verfügung. Kopieren Sie entweder die Datei oder die Java KeyStore-Datei auf jeden Proxy, oder stellen Sie sicher, dass jeder Proxy Zugriff auf das Java KeyStore- oder Enterprise Key Management(EKM)-Gerät hat.

Warum und wann dieser Vorgang ausgeführt wird

Schlüssel-Aliasse müssen eindeutig sein. Jeder Schlüsselalias muss auf jedem Proxy die gleiche Schlüsselgröße und den gleichen Typ haben, oder der Schlüssel kann nicht als Standard zugewiesen werden.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Schlüssel einrichten**.
2. Führen Sie im Abschnitt „Neue Schlüssel hinzufügen“ des Formulars die folgenden Schritte aus, um einen neuen Schlüssel hinzuzufügen.

Wichtig:
Bei Verwendung von mit SafeNet versionierten Schlüsseln wird eine zusätzliche Spalte für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** kann nicht bearbeitet werden. Klicken Sie auf den Link **Aktuelle Schlüsselversionen** abrufen unter Zugehörige Links, um die neueste Version jedes Schlüssels vom Edge-Proxy abzurufen.

Zeilen in der Liste mit einem **X** in der linken Spalte können gelöscht werden. Schlüssel, die als Standard verwendet wurden oder den **Status Verfügbar** haben, können nicht gelöscht werden.

a. Doppelklicken Sie in die Zeile mit der **Aufschrift Neue Zeile einfügen.**.

b. Geben Sie im Bearbeitungsfeld einen Namen für den Schlüssel ein, und klicken Sie dann auf das Häkchen.

Schlüsselaliasnamen bestehen aus Kleinbuchstaben und Zahlen. Großbuchstaben werden beim Klicken auf **Aktualisieren** in Kleinbuchstaben geändert. Schlüssel-Aliasse müssen eindeutig sein.

Hinweis:
Wenn Sie Unbound Technology-Schlüssel verwenden, fügen Sie den Alias für den Verschlüsselungsschlüssel hinzu. Der Alias des Verschlüsselungsschlüssels ist der Dateiname des Wrapped-Verschlüsselungsschlüssels, der zum Verzeichnis <proxy-installation-directory>/keys hinzugefügt wurde. Wenn zum Beispiel die Datei im Verzeichnis myunboundkey heißt, fügen Sie diesen Namen zum Feld **Schlüsselalias** hinzu.

c. Doppelklicken Sie in derselben Zeile auf die Spalte **Schlüsselgröße**.

d. Wählen Sie im Auswahlfeld eine Schlüsselgröße, entweder **128 Bit** oder **256 Bits** aus und klicken Sie dann auf das Häkchen.

e. Doppelklicken Sie in derselben Zeile auf die Spalte **Typ**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie im Auswahlfeld einen Schlüsseltyp, entweder **Datei**, **Keystore**, **SafeNet** oder **Unbound** aus und klicken Sie dann auf das Häkchen.

g. Wenn Sie mit dem Hinzufügen der Schlüssel fertig sind, klicken Sie auf **Nächster Schritt**.
Sie müssen für jeden Schlüssel einen Aliasnamen, eine Schlüsselgröße und einen Schlüsseltyp angeben, bevor Sie fortfahren.

3. Überprüfen Sie im Abschnitt „Schlüsselstatus“ des Formulars die Option **Status** des Schlüssels und stellen Sie sicher, dass **Verfügbar** eingestellt ist.
4. Wenn der Schlüssel **Verfügbar** ist, klicken Sie auf **Nächster Schritt**.
Dies kann einige Minuten dauern.

Hinweis:
Bei Verwendung von mit SafeNet versionierten Schlüsseln wird eine zusätzliche Spalte für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** kann nicht bearbeitet werden.

Die Instanz verfolgt den Status jedes für jeden Proxy verfügbaren Verschlüsselungsschlüssels. Wenn ein Schlüssel für alle Proxys verfügbar ist, ändert sich dessen Status zu **Verfügbar**. Wenn sich der Status nach einigen Minuten nicht ändert, überprüfen Sie, ob der Schlüssel für alle Proxys verfügbar ist. Wenn der Zustand **Nicht verfügbar** bestehen bleibt, hat einer oder haben mehrere Proxys den Schlüssel nicht.

Zustände der Verschlüsselungsschlüssel

Status	Beschreibung
Verfügbar	Alle Online-Proxys haben den Schlüssel.
Nicht verfügbar	Dies ist ein neuer Schlüssel, und die Proxys haben den Schlüssel noch nicht geladen, oder mindestens ein Proxy konnte den Schlüssel nicht laden.

5. Führen Sie im Abschnitt „Standardschlüssel ändern“ des Formulars einen der folgenden Schritte aus:
   - Geben Sie den Schlüsselalias ein.
   - Klicken Sie auf das Lupensymbol und wählen Sie einen Alias aus.

Hinweis:
Bei Verwendung von mit SafeNet versionierten Schlüsseln wird ein zusätzliches Feld für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** ist ausgegraut und kann nicht bearbeitet werden. Wählen Sie nur die neueste Schlüsselversion aus. Wenn Sie eine frühere Version auswählen, wird die folgende Meldung angezeigt, wenn Sie auf **Aktualisieren** oder **Nächster Schritt**klicken.

> One of the default keys chosen is not the latest version available for the key. Please use the latest version.

Wenn es sich bei den Standardschlüsseln nicht um die neuesten Versionen der SafeNet-Schlüssel handelt, wird unter Zugehörige Links ein Link **Standardschlüssel auf aktuelle Version** aktualisieren angezeigt. Klicken Sie auf den Link, um die Standardschlüssel zu aktualisieren und die neueste Version zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Planen Sie im Abschnitt „Schlüsselrotation planen“ des Formulars einen Massenschlüssel-Rotationsauftrag oder einen Einzelschlüssel-Rotationsauftrag, um vorhandene Daten mit dem neuen Verschlüsselungsschlüssel zu verschlüsseln.

   Wenn Sie keinen Massenschlüssel-Rotationsauftrag oder Einzelschlüssel-Rotationsauftrag ausführen, bleiben vorhandene Daten mit dem alten Schlüssel verschlüsselt, bis auf die Daten erneut zugegriffen wird.

Konfigurieren zusätzlicher Eigenschaften in der Edge Encryption-Eigenschaftendatei

Nach dem Installieren des Edge Encryption Proxy-Server in Ihrem Netzwerk und Einrichten des Schlüsselspeichers und der Schlüssel konfigurieren Sie die zusätzlichen Edge Encryption-Eigenschaften.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie die Datei <installation directory>/conf/edgeencryption.properties, und konfigurieren Sie die folgenden Edge Encryption Proxy-Server-Eigenschaften:
   - Zieleigenschaften (Instanz)
   - Benutzer-Account-Eigenschaften
   - Proxy-Eigenschaften
   - Konfigurieren Sie bei Verwendung von ordnungserhaltenden Verschlüsselungstypen oder Verschlüsselungsmustern die Proxy-Datenbankeigenschaften.
   - Klartext und statische IV-Eigenschaften
2. Speichern und schließen Sie die Datei.

Einen Web-Proxy konfigurieren

Wenn Ihr Netzwerk einen Web-Proxy verwendet, können Sie den Edge Encryption Proxy für die Verwendung für den Web-Proxy einrichten.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Ihr Netzwerk keinen Web-Proxy verwendet, belassen Sie die Web-Proxy-Eigenschaften in der Konfigurationsdatei auskommentiert.

Der Edge Encryption Proxy-Server unterstützt die HTTP-Verbindung mit dem Web-Proxy und die Basisauthentifizierung.

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
2. Öffnen Sie die Datei edgeencryption.properties.
3. Konfigurieren Sie die Web-Proxy-Eigenschaften.
4. Speichern und schließen Sie die Datei edgeencryption.properties.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wenn der Web-Proxy ein kundenspezifisches Serverzertifikat verwendet, fügen Sie dieses Zertifikat zur JVM hinzu, die vom Edge Encryption Proxy-Server verwendet wird, um eine Vertrauensstellung zwischen dem Web-Proxy und dem Edge Encryption Proxy-Server zu erstellen.
   a. Verwenden Sie den Befehl `cd`, um zu zu navigieren<Java home directory> /jre/lib/security/cacerts
   b. Führen Sie den Befehl aus: `keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile>`

Die anfängliche Speichergrenze des Proxy-Servers und die obere Grenze des Speicherbereichs festlegen

Legen Sie das anfängliche und das obere Speichergrenze fest, um festzulegen, wie viel Speicher der Proxy-Server verbrauchen kann. Legen Sie diese Grenzwerte fest, um Leistungsprobleme in Ihrer Edge Encryption Implementierung zu vermeiden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Legen Sie als Richtlinie sowohl die anfängliche Speichergrenze als auch die obere Speichergrenze auf denselben Wert fest. Weisen Sie dem Betriebssystem auf einem beliebigen Computer 2 GB des physischen Speichers zu. Weisen Sie dann den Rest des physischen Speichers dem Heap zu, indem Sie die Eigenschaften für die anfängliche Speichergrenze und die obere Speichergrenze verwenden. Weisen Sie beispielsweise auf einem Computer mit 8 GB Arbeitsspeicher dem Betriebssystem 2 GB zu, und weisen Sie die verbleibenden 6 GB (6144 MB) dem anfänglichen und dem oberen Speicher zu.

Wichtig:
Wenn der Edge Encryption Proxy-Server ausgeführt wird, müssen Sie den Proxy-Server nach der Aktualisierung dieser Eigenschaften anhalten und neu starten.

Prozedur

1. Öffnen Sie in Ihrem Proxy-Server-Verzeichnis <install dir>/conf/wrapper.conf.
2. Fügen Sie am Ende der Datei die folgende Zeile hinzu, um die anfängliche Speichergrenze festzulegen:

```
wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
```

   Legen Sie `<number>` auf die nächst verfügbare `<number>` in Reihenfolge der Eigenschaften von `wrapper.java.additional.<number>` fest, die in der Datei `wrapper.conf` definiert sind.

Example
Beispielsweise verfügen Sie über die folgende Liste von Eigenschaften `wrapper.java.additional.<number>`:

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Die höchste `<number>` in der obigen Liste ist **2**. Wenn Sie die Zeile `wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m` hinzufügen, setzen Sie `<number>` auf **3**, die nächst verfügbare Zahl.

Wichtig:
Lassen Sie keine Lücken in der Nummerierungsfolge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setzen Sie <min_memory_in_MB> auf die Anzahl der verbleibenden Megabytes des Arbeitsspeichers, nachdem dem Betriebssystem 2 GB Arbeitsspeicher zugewiesen wurde.

3. Legen Sie die obere Speichergrenze fest.
   Da im Basissystem keine Obergrenze für den Arbeitsspeicher festgelegt ist, kann der Proxy-Server den gesamten verfügbaren Arbeitsspeicher verwenden. Wenn auf dem Server andere Dienste ausgeführt werden, können Sie die obere Speichergrenze festlegen.

   Fügen Sie am Ende der Datei die folgende Zeile hinzu:

   wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m

   Legen Sie <number> auf die nächst verfügbare <number> in Reihenfolge der Eigenschaften von wrapper.java.additional.<number> fest, die in der Datei wrapper.conf definiert sind.

   Example
   Beispielsweise verfügen Sie über die folgende Liste von Eigenschaften wrapper.java.additional.<number>:

   ```
   wrapper.java.additional.1=
   wrapper.java.additional.2=
   ```

   Die höchste <number> in der obigen Liste ist **2**. Wenn Sie die Zeile wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m hinzufügen, setzen Sie <number> auf **3**, die nächst verfügbare Zahl.

   Hinweis:
   Lassen Sie keine Lücken in der Nummerierungsfolge.

   Setzen Sie <max_memory_in_MB> auf die Anzahl der verbleibenden Megabytes des Arbeitsspeichers, nachdem dem Betriebssystem 2 GB Arbeitsspeicher zugewiesen wurde.

4. Speichern und schließen Sie die Datei.

Example: Beispiel: Festlegen der anfänglichen und oberen Speichergrenzen des Proxy-Servers

```
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

Nächste Maßnahme
Edge Encryption Proxy starten.

Edge Encryption Proxy starten

Nach dem Installieren und Konfigurieren eines Edge Encryption Proxys kann der Proxy aus der Befehlszeile gestartet werden.

Vorbereitungen
Erforderliche Rolle: admin

Überprüfen Sie vor dem Starten des Verschlüsselungs-Proxys folgende Punkte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Plugin Edge Encryption ist in der Instanz aktiviert.
- Die Datei edgeencryption.properties wurde auf diesem Rechner konfiguriert.
- Bei Verwenden eines ordnungserhaltenden Verschlüsselungstyps oder Verschlüsselungsmusters wird die Proxy-Datenbank ausgeführt.

Hinweis:
Beim erstmaligen Einrichten der Datei edgeencryption.properties oder Ändern der Eigenschaften können Sie bei Bedarf die Eigenschaft für die Passwortverschlüsselung nicht festlegen. Nachdem Sie überprüft haben, dass alles funktioniert, können Sie die Passwortverschlüsselungseigenschaft festlegen, den Proxy herunterfahren und den Proxy erneut starten.

Prozedur

1. Führen Sie den Proxy-Server aus.

Option	Bezeichnung
Auf einem Linux-Rechner	**a.** CD zu ServerName_port **b.** Ausführen von ./startup.sh
Auf einem Windows-Rechner	Führen Sie die folgenden Schritte aus der Befehlszeile als Administrator aus: **a.** CD zu ServerName_port/bin **b.** Ausführen von edgeencryption.bat starten

2. Überprüfen Sie das Protokoll auf dem Proxy-Server, um sicherzustellen, dass der Proxy ausgeführt wird.

Passwörter in der Eigenschaftendatei verschleiern

Verschleiern Sie Passwörter in der Datei „ edgeencryption.properties “, um die Eigenschaftendatei freigeben zu können, ohne Klartextpasswörter offenzulegen.

Vorbereitungen
Erforderliche Rolle: admin

Stellen Sie sicher, dass der Edge Encryption Proxy-Server eingerichtet ist und erfolgreich ausgeführt wird, bevor Sie diese Eigenschaft festlegen. Bevor Sie diese Eigenschaft festlegen, Den Edge Encryption Proxy stoppen.

Warum und wann dieser Vorgang ausgeführt wird
Das Festlegen dieser Eigenschaft kann das Debuggen von Verbindungs- und Zugriffsproblemen beim ersten Start schwierig machen. Legen Sie diese Eigenschaft nur in Produktionsumgebungen fest, nachdem der Proxy erfolgreich eingerichtet und getestet wurde.

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
2. Erstellen Sie im Verzeichnis conf eine Textdatei, die eine komplexe Zeichenfolge oder einen Satz enthält, die als Passphrase verwendet werden kann, die der Proxy zum Verschleiern der Passwörter in der Datei edgeencryption.properties verwendet.
   Diese Passphrase sollte eine zufällige und komplexe Phrase sein, die sich nicht auf die Passwörter selbst bezieht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie die Datei edgeencryption.properties.
4. Legen Sie die Passwort-Verschlüsselungseigenschaft fest.
5. Speichern und schließen Sie die Datei edgeencryption.properties.

Nächste Maßnahme
Nachdem Sie diese Eigenschaft festgelegt haben, können Sie Edge Encryption Proxy starten.

Einen zusätzlichen Proxy manuell hinzufügen

Nachdem der erste Edge Encryption richtig konfiguriert und getestet wurde, können Sie zusätzliche Proxys auf einem Linux- oder Windows-Computer einrichten. Das Installieren mehrerer Proxys auf demselben Computer wird nicht empfohlen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Fügen Sie zusätzliche Proxy-Server auf zusätzlichen Computern hinzu, um eine optimale Umgebung sicherzustellen. Siehe Umgebungsgröße Ihrer Edge Encryption anpassen, um die Anzahl zusätzlich erforderlicher Proxys zu bestimmen.

Hinweis:
Stellen Sie sicher, dass alle Proxys die gleichen Verschlüsselungsschlüssel und dasselbe RSA-Schlüsselpaar haben, das zum digitalen Signieren von Konfigurations- und Verschlüsselungsregeln für die Verschlüsselung verwendet wird. Wenn eine Proxy-Datenbank als Teil der Installation eingerichtet wurde, müssen alle Proxys dieselbe Proxy-Datenbank verwenden.

Prozedur
1. Installieren Sie den Proxy mit dem entsprechenden Befehl.
   Weitere Informationen finden Sie unter Den Edge Encryption Proxy-Server (interaktives Installationsprogramm) installieren.
2. Kopieren Sie alle Verschlüsselungsschlüssel und die Datei edgeencryption.properties vom ersten Proxy zum neuen Proxy.
   Verschlüsselungsschlüssel befinden sich möglicherweise im Proxy-Schlüsselspeicher im Verzeichnis /Keys oder in einem SafeNet KeySecure-Schlüsselspeicher.
3. Öffnen Sie die Datei edgeencryption.properties auf dem neuen Proxy.
4. Ändern Sie die folgenden Eigenschaften:

Eigenschaft	Beschreibung
edgeencryption.proxy.name	Eindeutiger Name des Proxy-Servers
edgeencryption.proxy.host	Der Servername, die IP-Adresse oder der vollständig qualifizierte Domänenname des Computers, auf dem der Proxy ausgeführt wird.
edgeencryption.proxy.http.port	Port auf dem Proxy für die HTTP-Kommunikation. Muss für alle Prozesse auf der Maschine eindeutig sein.
edgeencryption.proxy.https.port	Port auf dem Proxy für die HTTPS-Kommunikation. Muss für alle Prozesse auf der Maschine eindeutig sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wenn Sie den Proxyserver auf einem Windows-Computer installieren, müssen Sie den Namen des Service ändern, indem Sie die Datei conf/wrapper.conf auf dem neuen Proxy öffnen und die in der folgenden Tabelle aufgeführten Eigenschaften hinzufügen.

   Hinweis:
   Sie müssen diesen Schritt ausführen, bevor Sie den Proxy-Server starten.

Eigenschaft	Beschreibung
wrapper.ntservice.name	Eindeutiger Name des Edge Encryption Proxy-Service.
wrapper.ntservice.displayname	Anzeigename des Edge Encryption Proxy-Service.
wrapper.ntservice.description (optional)	Beschreibung des Proxy-Servers.

6. Speichern und schließen Sie die Datei.
7. Starten Sie den Proxy mit dem entsprechenden Befehl.
   Weitere Informationen finden Sie unter Edge Encryption Proxy starten.

Einen Edge Encryption Proxy-Server authentifizieren

Legen Sie fest, dass ein Proxy-Server eine vertrauenswürdige Quelle ist, sodass Edge Encryption Anforderungen von diesem Proxy-Server verarbeiten kann.

Vorbereitungen

Wenn ein Proxy-Server nicht authentifiziert ist, enthält das Protokoll der Konsole folgende Meldung:

```
WARN This Edge Encryption proxy has not yet been authenticated by the instance.
Please navigate to the matching Proxy record on your ServiceNow instance and authenticate it.
```

Wenn Sie versuchen, auf den Proxy zuzugreifen, wird die folgende Meldung angezeigt: Diese Website ist nicht erreichbar.

Damit der Proxy während des Upgrade-Vorgangs betriebsbereit bleibt, wird die Authentifizierung erst erforderlich, wenn das Proxy-Update erfolgreich war.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Proxys**.
2. Wählen Sie den Proxy aus, und klicken Sie auf **Authentifizieren**.

Ergebnisse

Der Proxy wird von **„Nicht authentifiziert“** zu „ **Ausstehend** “ zu „ **Authentifiziert**“ verschoben. Der Status ändert sich von **Nicht** authentifiziert in **Ausstehend**, wenn Sie die Authentifizierung starten. Nach Abschluss der Authentifizierung ändert sich der Status von **Ausstehend** in **Authentifiziert**, und Sie können auf den Proxy zugreifen, und Edge Encryption kann Anforderungen vom Proxy akzeptieren.

Hinweis:
Wenn Sie den Proxy anhalten und neu starten, bleibt der Proxy **authentifiziert** und wird erfolgreich neu gestartet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den Edge Encryption Proxy stoppen

Sie können einen Edge Encryption Proxy aus der Befehlszeile stoppen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Den Proxy-Server stoppen.

Option	Bezeichnung
Auf einem Linux-Rechner	Ausführen von `./shutdown.sh`
Auf einem Windows-Rechner	Ausführen von `edgeencryption.bat stoppen` Um den Windows-Dienst zu entfernen, führen Sie `edgeencryption.bat entfernen` aus.

2. Überprüfen Sie das Protokoll auf dem Proxy-Server, um zu überprüfen, ob der Proxy angehalten wurde.

Den Edge Encryption Proxy unter Linux deinstallieren

Sie können den Edge Encryption Proxy deinstallieren. Wenn Sie den Proxy aktualisieren, ist es nicht notwendig, die aktuelle Version herunterzufahren und zu deinstallieren.

Vorbereitungen
Erforderliche Rolle: admin

Sie müssen Zugriff auf den Computer haben, auf dem der Edge Encryption Proxy ausgeführt wird.

Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie vor dem Herunterfahren des Edge Encryption Proxy sicher, dass keine Benutzer über den Proxy mit der Instanz verbunden sind.

Der unter Linux ausgeführte Verschlüsselungs-Proxy arbeitet als einzelner Prozess. Sie können diesen Prozess beenden, um Aufgaben wie das erneute Bereitstellen des Verschlüsselungsproxys auf einem anderen Host-Computer, das Aktualisieren der Proxyversion, das Aktualisieren der Java-Version oder das Ändern des eindeutigen Namens des Verschlüsselungsproxys bei der Bereitstellung des Verschlüsselungsproxys auf mehreren Proxy-Servern zu erledigen.

Prozedur

1. Sie können die Datei `edgeencryption.properties` speichern, bevor Sie das Verteilerverzeichnis löschen.
2. Führen Sie das Shell-Skript `shutdown.sh` aus.
3. Überprüfen Sie das Protokoll auf dem Proxy-Server, um sicherzustellen, dass der Proxy-Server heruntergefahren ist.
4. Löschen Sie die Dateien im Verteilerordner.

Den Edge Encryption Proxy unter Windows deinstallieren

Sie können den Edge Encryption Proxy deinstallieren. Wenn Sie den Proxy aktualisieren, ist es nicht notwendig, die aktuelle Version herunterzufahren und zu deinstallieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen Zugriff auf den Computer haben, auf dem der Edge Encryption Proxy ausgeführt wird.

Stellen Sie vor dem Herunterfahren des Edge Encryption Proxy sicher, dass keine Benutzer über den Proxy mit der Instanz verbunden sind.

Prozedur

1. Sie können die Datei edgeencryption.properties speichern, bevor Sie das Verteilerverzeichnis löschen.
2. Ausführen von `edgeencryption.bat stoppen`
3. Ausführen `edgeencryption.bat entfernen`
4. Überprüfen Sie das Protokoll auf dem Proxy-Server, um zu überprüfen, ob der Proxy-Server heruntergefahren ist.
5. Löschen Sie die Dateien im Verteilerordner.

SSO für mehrere Anbieter mit Edge Encryption einrichten

Richten Sie SSO für mehrere Anbieter ein, um die Anmeldung über die Edge Encryption Proxy-Server-URL oder Instanz-URL zu ermöglichen. Wenn Sie Single Sign-on (SSO) für mehrere Anbieter mit aktiviertem Edge Encryption implementieren, müssen sich einige Benutzer möglicherweise über den Proxy-Server Edge Encryption bei Ihrer Instanz anmelden, andere Benutzer hingegen nicht.

Vorbereitungen

- Aktivieren Sie das Plugin für die Installation des Single Sign-On-Installationsprogramms für mehrere Anbieter (com.snc.integration.sso.multi.installer).
- Aktivieren Sie das Plugin Edge Encryption (com.glide.edgeencryption) und stellen Sie sicher, dass ein oder mehrere Proxy-Server in Ihrem Netzwerk eingerichtet sind.
- Bestimmen Sie die URL für den Edge Encryption Proxy-Server, über den sich Benutzer mit SSO mehrerer Anbieter anmelden. Zum Ermitteln der URL eines Edge Encryption Proxy-Servers, siehe Edge Encryption wird installiert.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Der Benutzer, der sich anmeldet, muss die entsprechende URL verwenden, um sich anzumelden, entweder mit dem Edge-Proxy oder nicht mit dem Edge-Proxy.

- Wenn alle Benutzer über den Edge Encryption Proxy-Server geleitet werden, richten Sie Ihren Anbieter-Identifizierungsdatensatz ein und definieren Sie die Proxy-Server-URL in den Feldern **ServiceNow Homepage**, **Entitäts-ID/Aussteller** und **URI der Zielgruppe**.
- Um einige Benutzer über den Proxy-Server und einige Benutzer an die Instanz weiterzuleiten, erstellen Sie zwei Anbieter-Identifizierungsdatensätze. Beide Datensätze verwenden den gleichen Wert im Feld **URL des Identitätsanbieters**. Einer der Datensätze wird jedoch über den Proxy-Server geleitet, während der andere zur Instanz führt.
  - Melden Sie sich über den Instanznamen an: https:// <instance name> .service-now.com/ login_with_sso.do?glide_sso_id= <sys_id des IdP-Datensatzes für Nicht-Edge-Proxy
  - Melden Sie sich über den Edge-Proxy an: https:// <edge hostname> :<port> / login_with_sso.do?glide_sso_id= <sys_id des IdP-Datensatzes für den Edge-Proxy

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie die Duplizierung von Identitätsanbieter-URLs in Identitätsanbieter-Datensätzen.
   Eine eindeutige Einschränkung verhindert die Duplizierung der Identitätsanbieter-URL in zwei verschiedenen Identitätsanbieter-Datensätzen. Sie können die Duplizierung der URL des Identitätsanbieters in mehreren IdP-Datensätzen aktivieren, indem Sie ein Feld auf „false“ setzen.
   a. Navigieren zu **Systemdefinition** > **Lexikon**.
   b. Öffnen Sie Identitätsanbietertabelle [saml2_update1_properties] den Definitionsdatensatz für das Feld **idp**.
   c. Konfigurieren Sie das Formular, um das Feld **Eindeutig** hinzuzufügen.
   d. Stellen Sie sicher, dass der Wert im Feld **Eindeutig** auf **Falsch** gesetzt ist.
2. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
3. Erstellen Sie zwei Identitätsanbieter-Datensätze für denselben Identitätsanbieter: einen mit der Instanz-URL und einen mit der Edge Encryption Proxy-Server-URL.
   Informationen zum Erstellen eines Identitätsanbieter-Datensatzes finden Sie unter Externe Identitätsanbieter erstellen.
   a. Füllen Sie für die Edge Encryption Proxy-Server-URL das Formular mit diesen Werten aus.

Feld	Wert
URL des Identitätsanbieters	Importiert aus den IdP-Metadaten.
ServiceNow Homepage	Die URL für Ihre Proxy-Server-Startseite. Zum Beispiel: https://<proxy hostname>:<port>/navpage.do
Entitäts-ID/Aussteller	https://<proxy hostname>:<port>
Zielgruppen-URI	https://<proxy hostname>:<port>

   b. Klicken Sie auf **Absenden**.
   c. Füllen Sie für die Instanz-URL das Formular mit diesen Werten aus.

Feld	Wert
URL des Identitätsanbieters	Importiert aus den IdP-Metadaten.
ServiceNow Homepage	https://<instance>.service-now.com/navpage.do
Entitäts-ID/Aussteller	https://<instance>.service-now.com/navpage.do
Zielgruppen-URI	https://<instance>.service-now.com/navpage.do

   d. Klicken Sie auf **Absenden**.
4. **Wahlweise:** Wenn Sie mehrere Identitätsanbieter verwenden, ändern Sie den MultiSSO-Installations-Exit.
   a. Navigieren zu **Systemdefinition** > **Installationsausgänge**.
   Das System zeigt die aktuelle Liste der Installations-Exits an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Öffnen Sie **MultiSSO** Installations-Exit.

c. Lokalisieren Sie die folgende Anweisung im Feld **Skript**.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
      SSO_Helper.debug("IdP found based on SAML response: " +
idpRecord.getUniqueValue());
      return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
   }
}
```

d. Ersetzen Sie die Anweisung durch den folgenden Code.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
  /* // You have two profiles that use the same IdP entity id it cannot use
  // the IdP issuer / entity id from the response otherwise it may result in the
  // wrong IdP profile. IdP initiated login will not work
  var idpRecord = this.getIdPRecord(request);
  if (idpRecord) {
    SSO_Helper.debug("IdP found based on SAML response: " +
idpRecord.getUniqueValue());
    return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
    }*/
  return new SSO_Helper(null, true);
  }
```

Hinweis:
Die durch IdP initiierte Anmeldung funktioniert in dieser Konfiguration nicht.

e. Klicken Sie auf **Aktualisieren**.

5. **Wahlweise:** Wenn Sie mehr als ein Unternehmen verwenden, konfigurieren Sie Benutzer für Multi-Provider-SSO und aktualisieren Sie die sys_id des Identitätsanbieter-Datensatzes abhängig vom Benutzer.

   (Optional) Weitere Informationen finden Sie unter Benutzer für Mehrfachanbieter-SSO konfigurieren.

   - Um einen Benutzer für die Anmeldung über den Edge Encryption Proxy-Server zu konfigurieren, verwenden Sie die sys_id des Identitätsanbieter-Datensatzes, der die Edge Encryption Proxy-Server-URL verwendet.
   - Um einen Benutzer für die Anmeldung an der Instanz zu konfigurieren, verwenden Sie die sys_id des Identitätsanbieter-Datensatzes, der die Instanz-URL verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Login-URLs

URL	Login-Ziel
https://<proxy hostname>:<port>/login_with_sso.do?glide_sso_id=<sys_id of the IdP record for the proxy server URL>	Meldet sich über den Proxy-Server an.
https://<instance name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of IdP record for the instance URL>	Meldet sich über die Instanz an.

Eigenschaften des Edge Encryption Proxy-Servers

Die Konfigurationsdatei edgeencryption.properties im Ordner <installation directory>/conf/ enthält Eigenschaften zum Konfigurieren Ihrer Umgebung.

Sie müssen den Proxyserver neu starten, nachdem Sie Änderungen an den Eigenschaften des Proxyservers vorgenommen haben.

Klartext und statische IV-Eigenschaften

edgeencryption.customer.assigned.known.cleartext	Klartext, damit die Instanz überprüfen kann, ob alle Proxys die gleichen Schlüssel verwenden. Beim Start verschlüsselt der Proxy den Klartext und sendet den verschlüsselten Text an die Instanz. Die Instanz kennt weder den Klartext, noch werden an die Instanz Schlüssel gesendet. Diese Eigenschaft muss für alle Proxys gleich sein.
edgeencryption.encrypter.static.iv	Statischer IV (Initialisierungsvektor), der in der gleichstellungserhaltenden und ordnungserhaltenden Verschlüsselung verwendet wird. Diese Eigenschaft muss für alle Proxys gleich sein und genau 16 Byte (16 ASCII-Zeichen) betragen.

Eigenschaften der digitalen Signatur

edgeencryption.proxy.signature.keystore.path	Pfad und Name der Java KeyStore-Datei.
edgeencryption.proxy.signature.keystore.password	Passwort. Das Standardpasswort lautet <changeme>. Ändern Sie das Passwort nach der Installation des Java KeyStore.
edgeencryption.proxy.signature.keystore.keyalias	Das als Alias angegebene Argument -alias, wenn das RSA-Schlüsselpaar generiert wird.

Dateispeichereigenschaft

edgeencryption.keyfile.directory	Das Verzeichnis gibt an, wo Schlüsseldateien gespeichert werden. Wenn Sie den Java KeyStore oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Beispiel: `edgeencryption.keyfile.directory=keys` Wenn Sie Schlüssel für Unbound Technology verwenden, deaktivieren Sie diese Eigenschaft und setzen Sie den Wert auf das Schlüsselverzeichnis.

Allgemeine Konfigurationseigenschaften

edgeencryption.config.poll.interval	Abrufintervall in Sekunden. Die Standardeinstellung bedeutet, dass es 5 Sekunden dauert, bis der Proxy von Änderungen der Verschlüsselungskonfiguration erfährt. Größere Werte führen dazu, dass die Instanz länger braucht, um einen Offline-Proxy zu erkennen. **⚠ Warnung:** Diese Eigenschaft nicht ändern. Das Ändern der Standardeinstellung des Proxy-Abrufintervalls kann zu Erkennungsverzögerungen führen, wenn ein Proxy online geschaltet wird.
edgeencryption.rules.dir	Ordner, in dem die Verschlüsselungsregeln auf dem Proxy gespeichert sind.
edgeencryption.encryption.order_preserving.cache.enable	Die Einstellung bestimmt, ob Caching zur Unterstützung von ordnungserhaltenden Verschlüsselungstypen verwendet wird.
edgeencryption.encryption.order_preserving.cache.size	Maximale Cache-Größe, in Bytes.
edgeencryption.jobs.concurrency	Maximale Anzahl von Massenverschlüsselungsaufträgen, die gleichzeitig auf diesem Proxy ausgeführt werden können.
edgeencryption.jobs.requests_per_second	Anzahl der HTTP-Auftragsanforderungen pro Sekunde, die von diesem Proxy an die Instanz gesendet werden können.
edgeencryption.attachments.request.timeout.seconds	Zeitüberschreitung für das Hochladen von Anhängen in Sekunden.
edgeencryption.request.buffer.size	Größe einer Verschlüsselungsanforderung. Wenn eine Verschlüsselungsanforderung größer als diese Größe ist, wird der Überschuss auf der Festplatte gespeichert. **⚠ Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.httpclient.request.buffer.size	Größe der Client-Anforderung. Wenn die Client-Anforderung größer als diese Größe ist, wird der Überschuss auf der Festplatte gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	⚠ Warnung: Diese Eigenschaft nicht ändern.
„edgeencryption.httpclient.header.size“.	Größe des Anforderungs-/Antwort-Headers. • Mindestwert: 8.000 • Höchstwert: 32.000 **⚠ Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.proxy.idle.timeout	Zeit in Sekunden, nach der eine Transaktion abläuft. Standardwert: 300 (Sekunden)
edgeencryption.proxy.keepalive.interval	Zeit in Sekunden zwischen den vom Proxy an die Instanz ausgegebenen Pings. Pings werden regelmäßig ausgegeben, um die Verbindung zwischen dem Proxy und der Instanz zu überprüfen. • Standardwert: 10 (Sekunden) • Mindestwert: 5 (Sekunden)
edgeencryption.register.retry.count	Maximale Anzahl, wie oft der Proxy die Instanz pingt, um zu versuchen, sich zu registrieren. Standardwert: 0 (kein Grenzwert)
edgeencryption.tokenization.exclusion.list	Verschlüsselungsmuster können in diesen Feldern gefundene Zeichenfolgen nicht tokenisieren.

Java KeyStore-Eigenschaften

edgeencryption.keystore.path	Pfad zum Java KeyStore. Wenn Sie einen Dateispeicher oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert. Beispiel: `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	Passwort, das der Proxy für die Verbindung zum Java KeyStore verwendet. Wenn Sie einen Dateispeicher oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert.

Protokollierungseigenschaften

Protokollierungseigenschaften befinden sich in der Datei lo4gj2.properties im<installation directory> Verzeichnis /conf/ Diese Eigenschaften werden nur zur Problembehandlung oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf Anweisung des ServiceNow -Supports geändert. Weitere Informationen finden Sie unter So erhöhen Sie die Debug-Protokollierung für den Edge Encryption-Proxy .

NAE-Geräteschlüsselspeicher-Eigenschaften

edgeencryption.nae.retries	Anzahl der Wiederholungsversuche.
edgeencryption.nae.enabled	Die Einstellung zeigt an, ob ein NAE-Gerät verfügbar ist.
edgeencryption.nae.server	Name des NAE-Servers
edgeencryption.nae.port	Vom NAE-Server verwendeter Port.
edgeencryption.nae.protocol	Vom NAE-Server verwendetes Protokoll.
edgeencryption.nae.keystore.path	Pfad zum Keystore auf dem NAE-Server.
edgeencryption.nae.keystore.password	NAE-Schlüsselspeicherpasswort.
edgeencryption.nae.username	Benutzername, der zur Authentifizierung beim NAE-Gerät verwendet werden soll.
edgeencryption.nae.password	Passwort zur Authentifizierung beim NAE-Gerät.
edgeencryption.nae.client.certificate	Das Zertifikat, das sich im Keystore des NAE-Servers befindet. Legen Sie diese Eigenschaft für die Authentifizierung mithilfe eines Zertifikats anstelle von Benutzername und Passwort fest.

Passworteigenschaft

edgeencryption.encrypter.properties.password	Name der Datei im Ordner conf, der eine Zeichenfolge enthält, die innerhalb eines sicheren Prozesses zum Verschleiern von Passwörtern in der Datei edgeencryption.properties verwendet wird. **Hinweis:** Name der Datei im Ordner conf, der eine Zeichenfolge enthält, die innerhalb eines sicheren Prozesses zum Verschleiern von Passwörtern in der Datei edgeencryption.properties verwendet wird.

Proxy-Eigenschaften

edgeencryption.proxy.host	Servername, IP-Adresse oder vollständig qualifizierter Domänenname des Computers, auf dem der Proxy ausgeführt wird. Zusammen mit dem Port definiert diese Eigenschaft die URL, die der Client für den Zugriff auf den Proxy-Server verwendet.
edgeencryption.proxy.name	Proxy-Name Muss für jeden Proxy eindeutig sein.
edgeencryption.proxy.http.port	Port auf dem Proxy für die HTTP-Kommunikation.
edgeencryption.proxy.https.port	Port auf dem Proxy für die HTTPS-Kommunikation.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft für gesperrte Proxy-Konfiguration

edgeencryption.proxy.locked	Bei „Wahr“ akzeptiert der Proxy keine Konfigurationsänderungen der Verschlüsselung oder Änderungen der Verschlüsselungsregel von der Instanz. Legen Sie diese Eigenschaft für die Produktionsinstanz fest, nachdem alle Verschlüsselungskonfigurationen und Regeln abgeschlossen sind.

Proxy-Datenbankeigenschaften

edgeencryption.db.url	Proxy-Datenbankspeicherort Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.user	Benutzername für den Zugriff auf die Proxy-Datenbank. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.password	Passwort für den Zugriff auf die Proxy-Datenbank. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.name	Proxy-Datenbankname. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Der Standardwert für diese Eigenschaft ist „edgeencryption“.
edgeencryption.db.bootstrap.file	Bootstrap-Datei für die Proxy-Datenbank. Die Datei ist relativ zum Verzeichnis sql/. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. **⚠ Warnung:** Ändern Sie diesen Parameter unter normalen Umständen nicht.

Proxy-Server-Performance-Eigenschaften

Proxy-Server-Performance-Eigenschaften sind standardmäßig nicht in der Konfigurationsdatei vorhanden. Um die Standardwerte zu ändern, müssen Sie die Eigenschaften hinzufügen und den Proxy-Server neu starten. Weitere Informationen finden Sie unter Diagnose und Leistung der Edge Encryption.

edgeencryption.stat.collection.enabled	Aktiviert die Erfassung von Statistiken, die vom Edge Encryption Proxy-Server-Performance-Dashboard verwendet werden. Standardwert: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Fügen Sie diese Eigenschaft hinzu, und setzen Sie den Wert auf „false“, um die Sammlung von Statistiken zu deaktivieren, die vom Edge Encryption Proxy-Server-Performance-Dashboard verwendet werden.
edgeencryption.stat.collection.interval	Intervallzeit in Sekunden, in der der Edge Encryption Proxy-Server Statistiken erfasst. Der Wert darf nicht unter 30 Sekunden liegen. Standardwert: 30 (Sekunden)

SSL-Zertifikateigenschaften

Starten Sie Ihren Proxy neu, wenn Sie den Wert einer SSL-Zertifikateigenschaft ändern. Das System verwendet beim Start das HTTPS-Schlüsselpaar zum Herstellen der Proxy-Server-Verbindung sowie zum Bestimmen, wie der Proxy Client-Anforderungen beantwortet.

edgeencryption.proxy.https.cert.alias	Alias des Zertifikats, das vom Proxy-Server für die Verbindung von Clients bereitgestellt wird.
edgeencryption.proxy.https.keystore.path	Pfad zum Schlüsselspeicher, der das HTTPS-Zertifikat enthält.
edgeencryption.proxy.https.keystore.password	Passwort für den Schlüsselspeicher, der das HTTPS-Zertifikat enthält.

Zieleigenschaften (Instanz)

edgeencryption.target.host	Hostname für die Instanz. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird. Zum Beispiel instancename.servicenow.com
edgeencryption.target.port	Instanzport. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird.
edgeencryption.target.protocol	Instanzprotokoll. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird. Verfügbare Optionen: • http • https

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften für nicht Unbound Technology-Anbieter

edgeencryption.ekm.provider.classname	Interner Klassenname für die Implementierung. **⚠ Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.thirdparty.vendor.library.path	Pfad zur Unbound API-JAR-Datei auf dem Unbound-Client-Computer.
edgeencryption.ekm.provider.rsa.wrapping.key.alias	Wrapping-Schlüsselalias in der Implementierung der Unbound Technology. Muss für alle Proxys gleich sein.

Benutzer-Account-Eigenschaften

edgeencryption.target.username	Benutzername, mit dem sich der Proxy bei der Instanz anmeldet. Der Benutzer muss über die Rolle „edge_encryption“ verfügen. Weitere Informationen finden Sie unter Benutzerkonto für die Edge Encryption einrichten.
edgeencryption.target.password	Passwort, mit dem sich der Proxy bei der Instanz anmeldet.

Web-Proxy-Eigenschaften

edgeencryption.webproxy.host	Webproxy-Name oder IP-Adresse
edgeencryption.webproxy.port	Port auf dem Web-Proxy.
edgeencryption.webproxy.user	Benutzername, der zum Herstellen einer Verbindung zum Web-Proxy verwendet wird. Wenn Ihr Web-Proxy keine Authentifizierung verwendet, lassen Sie diese Eigenschaft auskommentiert.
edgeencryption.webproxy.password	Passwort für die Verbindung zum Web-Proxy. Wenn Ihr Web-Proxy keine Authentifizierung verwendet, lassen Sie diese Eigenschaft auskommentiert.

Veraltete Proxy-Verschlüsselungseigenschaften

edgeencryption.encrypter.default.key128

Gibt den Namen des aktuellen AES 128-Schlüssels an. Ein AES 128-Schlüssel muss verfügbar sein, auch wenn er nicht verwendet wird. Muss für alle Proxys gleich sein.

Führen Sie eine Wartung dieser Schlüssel für die Instanz durch.

edgeencryption.encrypter.default.key256

Gibt den Namen des aktuellen AES 256-Schlüssels an. Muss für alle Proxys gleich sein.

Führen Sie eine Wartung dieser Schlüssel für die Instanz durch.

edgeencryption.encrypter.key

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gibt den Schlüsselnamen für jeden Schlüssel an und wird verwendet, um die Standardschlüssel anzugeben. Dies ist der Schlüsselalias, der in die Metadaten integriert ist, die in jedem verschlüsselten Element enthalten sind und daher in der Instanz gespeichert werden. Der Schlüsselname muss aus Kleinbuchstaben bestehen.

edgeencryption.encrypter.type

Gibt den Typ des Verschlüsselungs-Schlüsselspeichersystems an.

edgeencryption.encrypter.file

Gibt den Pfad und den Dateinamen der dem Schlüssel zugeordneten Textdatei an.

edgeencryption.encrypter.password

Gibt das Passwort für den Zugriff auf den Schlüsselspeicher an.

CyberArk-Integration mit dem Edge-Proxy-Server

Verwenden Sie CyberArk, um Passwörter in einem zentralen und sicheren digitalen Tresor zu speichern, um Passwörter zu sichern, die zuvor im Klartext gespeichert und durch Dateizugriff gesichert wurden oder zuvor über eine zweite Datei verschlüsselt wurden.

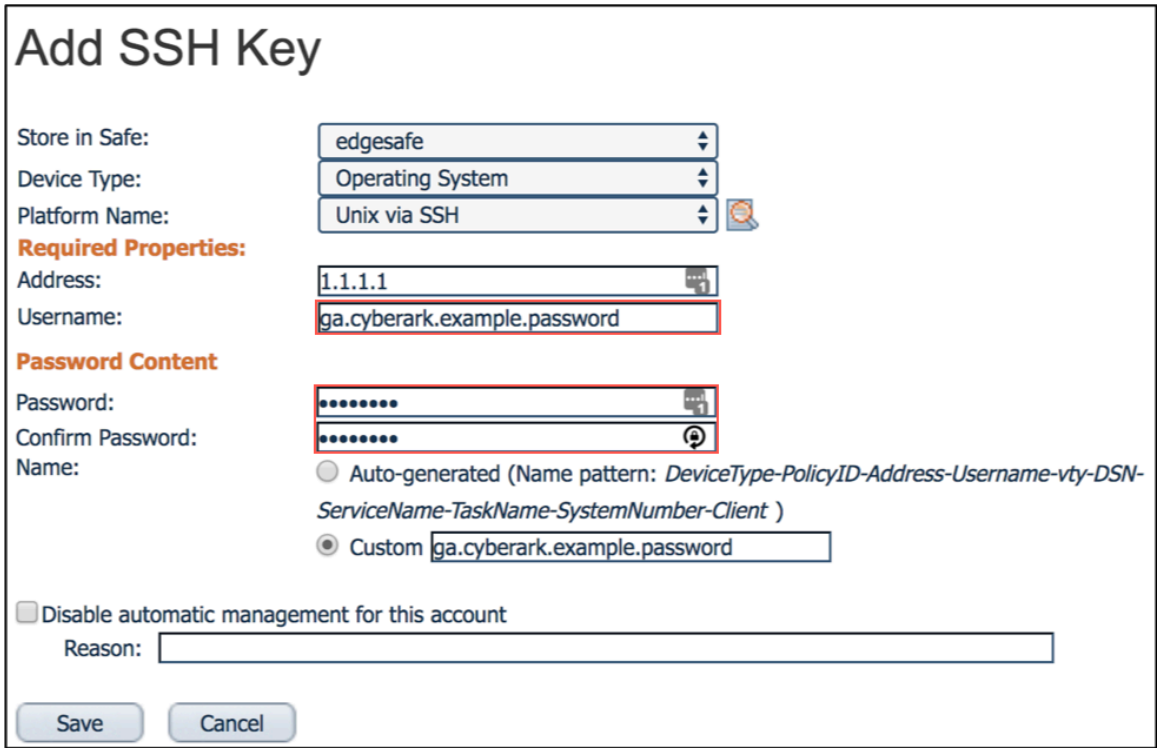
CyberArk AIM (Application Identity Management) verhindert unautorisierten Zugriff, indem hartcodierte und sichtbare Passwörter entfernt werden. AIM speichert Passwörter in einem digitalen Tresor auf einem unabhängigen gehärteten Server, wobei die Passwörter als digitale Anmeldeinformationen dargestellt werden. Die AIM-Clients (die Edge-Proxy-Server) verwenden die digitalen Anmeldeinformationen von CyberArk und greifen auf den unabhängigen Server zu, um die gesicherten Passwörter abzurufen. Auf den Edge-Proxy-Servern oder in der Instanz werden keine Passwörter gespeichert.

CyberArk-Anmeldeinformationen für digitale Tresore

Sie müssen CyberArk erwerben und konfigurieren, bevor Sie die CyberArk-Integration mit dem Edge-Proxy-Server einrichten können.

Legen Sie zum Hinzufügen eines Berechtigungsnachweises für CyberArk (der vom Edge-Proxy gelesen wird) den **Plattformnamen** der Anmeldeinformation auf **Unix über SSH** fest und stellen Sie sicher, dass Sie entweder einen **benutzerorientierten** Anmeldeinformations**namen** generieren oder den **Automatisch generierten** Ausweis**namen** notieren. Wenn Sie den Edge-Proxy für die Verwendung dieser Anmeldeinformation konfigurieren, stimmt der Proxy-Server mit dem **Namen** dieser Anmeldeinformation zur Einstellung im Proxy überein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



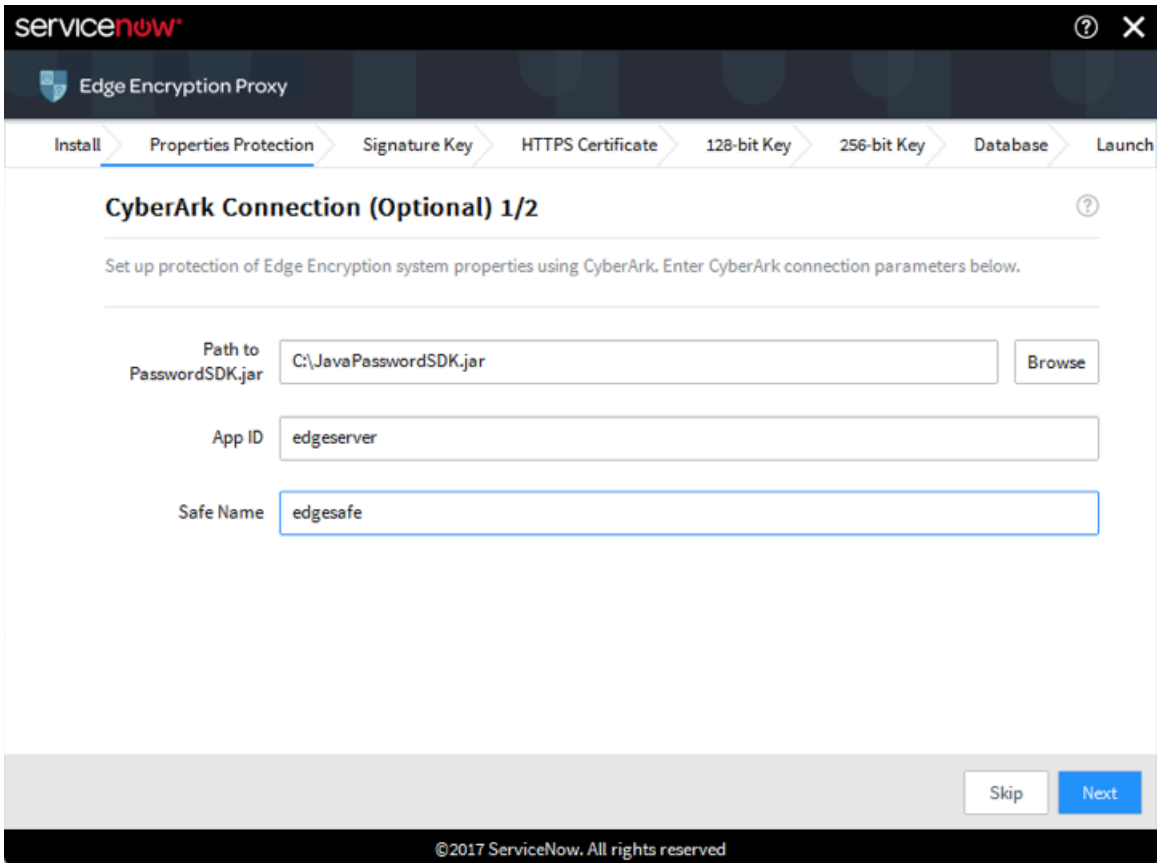
Jeder Anmeldeinformationseintrag enthält ein **Passwort**, das gespeichert wird, sowie einen **Namen** für die Anmeldeinformation, der von einer Anwendung für den Zugriff auf dieses Passwort verwendet wird.

Hinweis:
CyberArk-Anmeldeinformationen sind keine Verschlüsselungsschlüssel.

Hinzufügen von CyberArk während der Installation eines Edge-Proxys

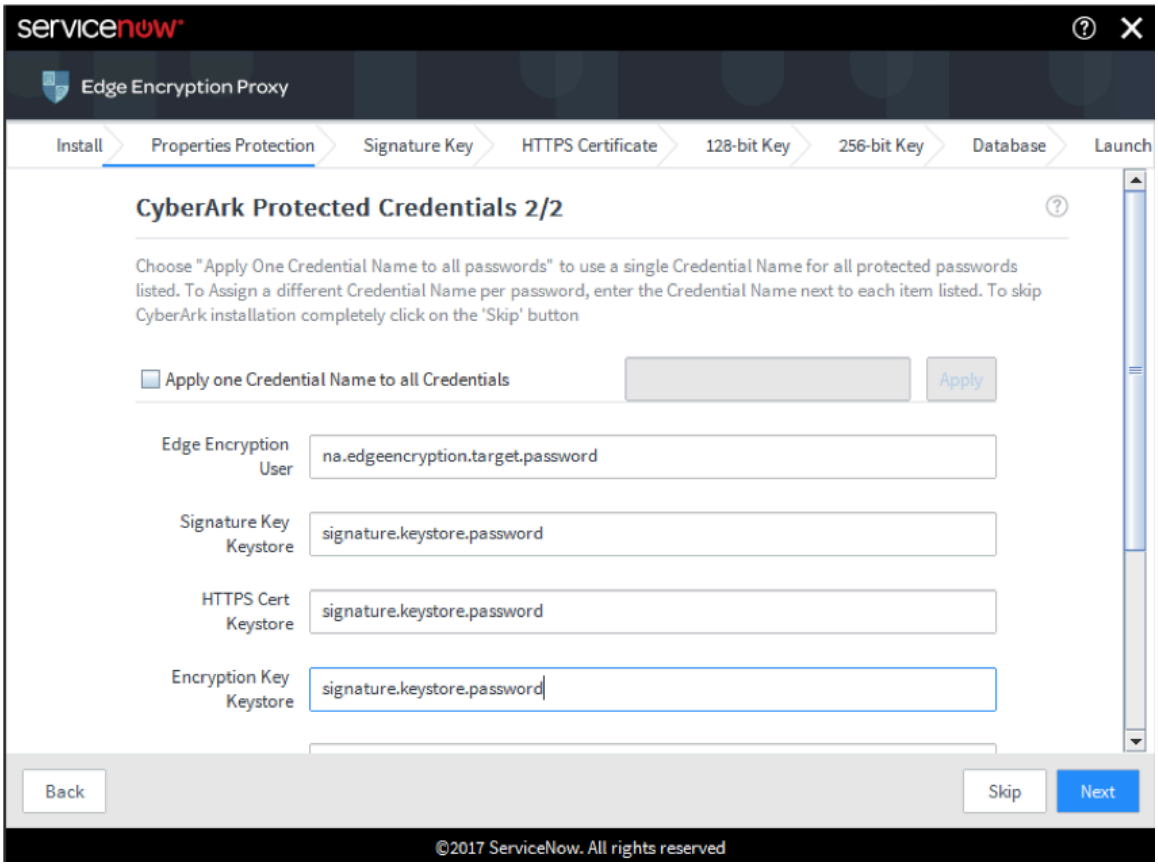
Das Proxy-Installationsprogramm enthält eine neue Konfigurationsseite für eine CyberArk-Integration. Diese Seite ist optional, wenn Sie CyberArk bei der Installation Ihres Proxy mit dem Proxy-Installationsprogramm nicht einschließen möchten. Sie können die CyberArk-Integration auch manuell in der Konfigurationsdatei einrichten und konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Proxy-Installationsprogramm enthält auch eine neue Seite für CyberArk-geschützte Anmeldeinformationen. Auf dieser Seite können verschiedene Eigenschaften mit einem oder mehreren Namen für die Anmeldeinformationen konfiguriert werden. Diese Seite ist optional, wenn Sie CyberArk bei der Installation Ihres Proxy mit dem Proxy-Installationsprogramm nicht einschließen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CyberArk-Passwortschutz

Jedes Passwortfeld im Edge-Proxy-Installationsprogramm, für das eine CyberArk-Anmeldeinformation im CyberArk-Tresor konfiguriert und auf der Seite mit den geschützten Anmeldeinformationen von CyberArk des Installationsprogramms angegeben ist, ist grau und enthält die Nachricht Von CyberArk geschützt.

Einen Load Balancer mit dem Edge-Proxy-Server verwenden

Sie können einen Load Balancer verwenden, um die Last auf den Proxy-Servern in Ihrem Edge Encryption Proxy-Setup auszugleichen. Wenn der Load Balancer und die Proxy-Server unterschiedliche Ports verwenden, geben Sie den Hostnamen und den HTTPS-Port des Load Balancer an, damit Benutzer die Antworten in ihrem Browser anzeigen können.

Wichtig:
Alle Produktionsumgebungen sollten aus Gründen der Redundanz mindestens zwei Edge Encryption Proxy-Server enthalten.

Edge-Anforderungsverarbeitung ohne Load Balancer

Wenn Sie keinen Load Balancer verwenden, wird eine Anforderung wie im Folgenden beschrieben verarbeitet.

1. Der Benutzer gibt eine Anforderung von einem Browser aus.
2. Der Browser sendet die Anforderung an den Edge-Proxy-Server.
3. Der Proxy-Server sendet die Anforderung an die ServiceNow-Instanz.
4. Die ServiceNow-Instanz gibt die Antwort an den Proxy-Server zurück.
5. Der Proxy-Server fügt in der Antwortkopfzeile seine eigene Portnummer hinzu, bevor er die Antwort an den Browser des Benutzers zurücksendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anforderung wurde erfolgreich abgeschlossen, da der Benutzer die Antwort des Proxy-Servers unter der in der Antwortkopfzeile angegebenen Anschlussnummer anzeigen kann.

Edge-Anforderungsverarbeitung mit einem Load Balancer

Wenn Sie jedoch einen Load Balancer verwenden, kommuniziert der Browser des Benutzers direkt mit dem Load Balancer, nicht mit dem Proxy-Server. Eine Anforderung wird wie im Folgenden beschrieben verarbeitet.

Hinweis:
Das folgende Beispiel verwendet 1025 als Portnummer des Proxy-Servers.

1. Der Benutzer gibt eine Anforderung von einem Browser aus.
2. Der Browser sendet die Anforderung an eine virtuelle IP (VIP) des Load Balancers, die auch als virtueller Server bezeichnet wird.
3. Der VIP ist so konfiguriert, dass er auf den Proxy-Server verweist (z. B. 10.2.200.148:1025). Somit leitet der Load Balancer die Anforderung an den Proxy-Server weiter.
4. Der Proxy-Server sendet die Anforderung an die ServiceNow-Instanz.
5. Die ServiceNow-Instanz gibt die Antwort an den Proxy-Server zurück.
6. Der Proxy-Server schreibt die Location-Kopfzeile in der Antwort mit Werten um, die in den Eigenschaften von risk-servicenow.dev.echonet:1025 konfiguriert sind.
   - **Host**: edgencryption.proxy.host
   - **HTTP-Port**: edgeencryption.proxy.http.port
   - **HTTPS-Port**: edgeencryption.proxy.https.port
7. Der Proxy-Server leitet die Antwort an den Load Balancer weiter, wobei die Location-Kopfzeile auf den Port des Proxy-Servers verweist.

Das Ergebnis hängt davon ab, ob Load Balancer und Proxy-Server denselben Port verwenden.

- Wenn Load Balancer und Proxy-Server denselben Port verwenden, ist die Anforderung erfolgreich, da der Benutzer die Antwort vom selben Port empfängt, der in der Antwort-Kopfzeile angegeben ist.
- Wenn Load Balancer und Proxy-Server unterschiedliche Ports verwenden, schlägt die Anforderung fehl, da der Browser des Benutzers nur mit dem Load Balancer kommuniziert, die Antwort sich jedoch auf dem Proxy-Server befindet.

Lösung

Sie können das Problem beheben, indem Sie einfach den Load Balancer und alle Edge-Proxy-Server am selben Port verwenden. Dies ist jedoch keine ideale Lösung. Eine bessere Lösung besteht darin, das System wissen zu lassen, welchen Port der Load Balancer verwendet.

Die folgenden Eigenschaften ermöglichen es, dass der Edge-Proxy-Server Antwortnachrichten an den Load Balancer weiterleiten kann, wenn Proxy-Server und Load Balancer unterschiedliche Ports verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *edgeencryption.proxy.rewrite.location.host* gibt den Hostnamen an, der für den Zugriff auf ServiceNow über den Load Balancer verwendet wird.
- *edgeencryption.proxy.rewrite.location.https.port* gibt den HTTPS-Port an, der für den Zugriff auf ServiceNow über den Load Balancer verwendet wird.

Den Load Balancer konfigurieren

Wenn der Load Balancer und die Proxy-Server unterschiedliche Ports verwenden, geben Sie den Hostnamen und den HTTPS-Port des Load Balancer an, damit Benutzer die Antworten in ihrem Browser anzeigen können.

Vorbereitungen

Erforderliche Rollen:

- Lokaler oder Domänenadministrator auf einem Windows-Host
- Service-Benutzer mit vollem Dateisystemzugriff auf einem Linux-Host

Prozedur

1. Melden Sie sich als Administrator, Domänenadministrator oder Service-Benutzer beim Proxy-Server-Host an.
2. Navigieren Sie zum Installationsverzeichnis für den Edge-Proxy und wählen Sie `conf/edgeencryption.properties`.
3. Setzen Sie die folgenden Eigenschaften:

Eigenschaft	Beschreibung
edgeencryption.proxy.rewrite.location.host	Wenn Ihre Edge-Konfiguration einen Load Balancer enthält, um die Last zwischen Proxy-Servern auszugleichen, werden die Antworten auf den Load Balancer neu geschrieben, so dass Anfragen abgeschlossen werden können. ○ Wenn im Proxy-Setup ein Load Balancer vorhanden ist, geben Sie den Hostnamen an, mit dem Sie über den Load Balancer auf ServiceNow zugreifen. ○ Optional: Wenn im Proxy-Setup kein Lastenausgleichsmodul vorhanden ist, können Sie diesen Wert auf den vom Proxy-Server verwendeten Hostnamen festlegen.
edgeencryption.proxy.rewrite.location.https.port	Wenn Ihre Edge-Konfiguration einen Load Balancer zum Ausgleich der Last zwischen Proxy-Servern enthält, geben Sie den HTTPS-Port an, über den auf ServiceNow über den Load Balancer zugegriffen wird. ○ Wenn in der Konfiguration ein Load Balancer vorhanden ist, geben Sie den HTTPS-Port an, über den der Zugriff auf ServiceNow über den Load Balancer erfolgt. ○ Optional: Wenn in der Konfiguration kein Lastenausgleichsmodul vorhanden ist,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	können Sie diesen Wert auf den vom Proxy-Server verwendeten HTTPS-Port festlegen.

4. Speichern Sie die Datei.

Ergebnisse

Anforderungen können abgeschlossen werden, da Benutzer jetzt Antworten in ihrem Browser anzeigen können.

Edge Encryption wird aktualisiert

Sowohl Instanz-Upgrades als auch Proxy-Server-Upgrades erfordern in einer Edge Encryption-Umgebung eine besondere Berücksichtigung.

Instanz-Upgrades

Instanz-Upgrades in einer Edge-Encryption-Umgebung erfordern Vorsicht, um sicherzustellen, dass die Edge-Steuerelemente nach dem Instanz-Upgrade ordnungsgemäß funktionieren.

Während eines Instanz-Upgrades sollten Sie Folgendes nicht hinzufügen, bearbeiten oder löschen:

- Edge Encryption-Konfigurationen
- Edge Encryption-Regeln
- Edge Encryption-Tokenisierungsmuster
- Geplante Aufträge für die Edge Encryption
- Edge Encryption-Schlüsselkonfigurationen
- Geplante Upgrades für die Edge Encryption
- Edge Encryption IP-Konfigurationen auf Deny-Liste

Ein geplanter Auftrag, der während des Instanz-Upgrades ausgeführt wird, wird nicht abgeschlossen. Um den unterbrochenen Auftrag abzuschließen, führen Sie den Auftrag nach dem Instanz-Upgrade erneut aus. Wenn Sie den Auftrag neu einplanen, geht die Verarbeitung, die vor dem Instanz-Upgrade stattgefunden hat, nicht verloren, und der Auftrag verarbeitet weiterhin nur die Daten, die noch nicht verarbeitet wurden.

Proxy-Server-Upgrades

Planen Sie ein Proxy-Upgrade, damit die Instanz den Edge Encryption Proxy-Server aktualisieren oder den Proxy-Server jederzeit manuell aktualisieren kann.

⚠ Warnung:
Bei einem Upgrade unter Windows können Probleme mit der Dateisperre auftreten, und das Upgrade schlägt möglicherweise fehl. Damit das Upgrade erfolgreich ist, dürfen im Installationsverzeichnis keine Dateien geöffnet sein. Außerdem darf im Installationsverzeichnis keine Shell vorhanden sein. Insbesondere wenn Sie den Proxy über die Befehlszeile (über `bin\edgeencryption.bat install/start`) starten, während Sie sich im Installationsverzeichnis befinden, sollten Sie diese Shell schließen oder sie anschließend aus dem Installationsverzeichnis verschieben. Unter dem Installationsverzeichnis dürfen keine Dateien von einem Editor oder einer anderen Anwendung geöffnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bibliotheken von Drittparteien

Bibliotheken von Drittanbietern wie Gemalto gehen bei Instanz- und Proxy-Server-Upgrades verloren, wenn sie im selben Verzeichnis aufbewahrt werden. Sie können Folgendes tun, um den Verlust von Bibliotheken von Drittanbietern während Upgrades zu verhindern:

1. Fügen Sie die folgende Eigenschaft manuell zu „edgeencryption.properties“ hinzu:

   „edgeencryption.ekm.provider.classname“ = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider

2. Fügen Sie die Eigenschaft *edgeencryption.thirdparty.vendor.library.path* Lieferantenbibliothekstandort hinzu, und legen Sie sie auf /path/to/jarsfest.

   Beispiel:

   Edge-Verschlüsselung.Drittpartei.Vendor.Bibliothek.Pfad = /app/servicenow/libs

3. Kopieren Sie die SafeNet-JAR-Dateien in diesen Pfad.

Nachdem Sie die Bibliotheken von Drittanbietern außerhalb der Installation Edge Encryption installiert haben, gehen sie bei Upgrades nicht mehr verloren.

Geplante Upgrades

Wichtig:
Aktualisieren Sie während ServiceNow Instanz-Upgrades auch Ihre Proxy-Server-Version, um sie an Ihre Instanzversion anzupassen und die Wahrscheinlichkeit von Kompatibilitätsproblemen zu verringern.

Planen Sie ein Upgrade, damit die Instanz den Proxy-Server zum geplanten Zeitpunkt aktualisieren kann. Diese Funktionalität ist nach dem Upgrade standardmäßig verfügbar. Ein geplantes Upgrade umfasst folgende Events:

1. Der Proxy-Server überprüft bei der Instanz, ob eine neue Version für das Upgrade verfügbar ist. Neue Versionen werden im Allgemeinen verfügbar, wenn die Instanz aktualisiert wird.
2. Der Administrator erhält beim Anmelden eine Benachrichtigung, wenn eine neue Version des Proxy-Servers verfügbar ist.
3. Der Administrator kann für jeden Proxy-Server Ein Upgrade des Edge Encryption Proxy-Servers planen.

   Hinweis:
   Nur Benutzer mit der Rolle „security_admin“ können einen Upgrade-Zeitplan über den Proxy-Server erstellen.

4. Sobald das Upgrade geplant ist, wird der Proxy-Server automatisch zum geplanten Zeitpunkt aktualisiert. Während des Upgrades ist der Proxy-Server nur für kurze Zeit offline.

   Hinweis:
   Da der Proxy-Server während des Upgrades neu startet, ist er für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

5. Während des geplanten Upgrades wird ein neues Proxy-Verzeichnis erstellt und Ihre Konfigurationsdateien werden in das neue Verzeichnis kopiert. Neue Eigenschaften werden in Ihre vorhandene Eigenschaftendatei geschrieben. Die folgenden Dateien oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verzeichnisse in Ihrem alten Proxy-Verzeichnis werden in das neue Proxy-Verzeichnis kopiert.

- Das Verzeichnis /conf
- Das Verzeichnis /keys
- Das Verzeichnis /keystore
- Die Datei java/jre/lib/security/cacerts

Dadurch bleiben Ihre Schlüssel, Schlüsselspeicher, Einstellungen und Zertifikate erhalten.

Hinweis:
Nur die oben genannten Dateien werden in das neue Proxy-Verzeichnis kopiert. Andere angepasste Dateien im Proxy-Server-Verzeichnis werden während eines geplanten Upgrades nicht beibehalten. Die Upgrade-Protokolldatei befindet sich im ursprünglichen Proxy-Verzeichnis im folgenden Ordner: <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Voraussetzungen für geplante Upgrades

Stellen Sie vor dem Planen eines Upgrades für einen Edge Encryption Proxy Folgendes sicher:

1. Die Umgebungsvariable *JAVA_HOME* verweist auf eine Java-Installation auf dem Computer, der sich außerhalb der Verzeichnisstruktur des Edge Encryption Proxys befindet.
2. Die Umgebungsvariable *JAVA_HOME* verweist auf eine Java-Installation mit Version 1.8_u144 oder höher.
3. Der Parameter *-Djava.io.tmpdir* in der Datei wrapper.conf des Edge Encryption Proxy zeigt auf ein Verzeichnis außerhalb der Verzeichnisstruktur des Edge Encryption Proxys. Der Proxy verfügt über Lese-/Schreib-/Ausführungsberechtigungen für das Verzeichnis. Optional können Sie den Parameter vollständig auskommentieren, sodass Java seinen Standard-TMP-Speicherort verwendet.

Manuelle Upgrades

Anstatt einen Aktualisierungszeitplan zu erstellen, können Sie jeden Proxy-Server über die Befehlszeile manuell aktualisieren. Siehe Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren oder Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren.

Proxy-Build-Status

Sie können leicht feststellen, ob ein Proxy-Server veraltet ist, indem Sie zu navigieren **Konfiguration der Edge Encryption** > **Proxys** > **Alle**. Der Status Ihres Proxy-Builds wird in der Spalte **Proxy Build** mit den folgenden Farben dargestellt:

Grün

Ihr Proxy-Server ist auf dem neuesten Stand.

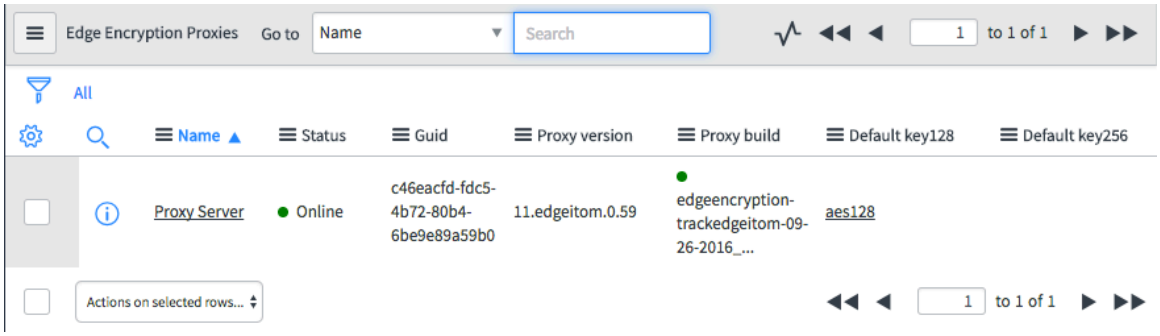
Gelb

Ihr Proxy-Server ist veraltet und ein Upgrade ist erforderlich.

Orange

Upgrade fehlgeschlagen. Ihr Proxy-Server wird auf die alte Version zurückgesetzt, um sicherzustellen, dass keine Ausfallzeiten auftreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Problembehandlung bei einem fehlgeschlagenen geplanten Proxy-Upgrade

Wenn ein geplantes Proxy-Upgrade fehlschlägt, wird der Proxy-Server auf die Version zurückgesetzt, von der Sie ein Upgrade durchführen. Alle Originaldaten, Schlüssel und Konfigurationsdateien bleiben erhalten. Dieser Vorgang kann mehrere Minuten dauern. Kontaktieren Sie Kundenservice und Support, um ein erfolgreiches Upgrade sicherzustellen.

Um den Grund für den Fehler zu ermitteln, können Sie **Fehlergrund** im Upgrade-Zeitplan überprüfen. Darüber hinaus wird das Installationsverzeichnis für das fehlgeschlagene Upgrade beibehalten, sodass Protokolldateien für die Problembehandlung verfügbar sind.

Hinweis:
Überprüfen Sie vor dem Löschen zusätzlicher Proxy-Verzeichnisse immer, welches Verzeichnis aktuell ist, indem Sie die Protokolldateien überprüfen. Wenn die Protokolldateien eine aktuelle Aktivität aufweisen, ist der Proxy möglicherweise mit Ihrer Instanz verbunden.

Wenn ein geplantes Proxy-Upgrade wiederholt fehlschlägt, können Sie Ihren Proxy-Server manuell aktualisieren. Weitere Informationen finden Sie unter Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren und Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren.

Java-Mindestanforderungen

Der Hostcomputer, auf dem der Proxyserver Edge Encryption installiert oder ausgeführt wird, muss eine unterstützte Version von Java enthalten. Derzeit unterstützte Versionen sind Java 11.0.6 oder höher in der 11.x-Versionsreihe

Hinweis:
Java 8 wird ab Release Utah nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit dem Proxy Edge Encryption auf Java 11, bevor Sie versuchen, die Version Edge Encryption des Proxys [Utah zu installieren.

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Umgebungen mit gemischten Proxy-Versionen

Obwohl eine Umgebung, in der alte Versionen des Proxy-Servers mit aktuellen Versionen des Proxy-Servers ausgeführt werden, nicht empfehlenswert ist, wird sie unterstützt, wenn sich alle Proxy-Server in der gleichen Versionsfamilie wie Ihre Instanz befinden. Wenn Sie beispielsweise eine Instanz im Washington DC Release haben, unterstützt Ihre Umgebung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proxy-Server von jedem Washington DC Patch oder Hotfix. Es gelten jedoch die folgenden Einschränkungen.

- Wenn ein Proxy-Server Funktionen unterstützt, die ein anderer Proxy nicht unterstützt, tritt ein inkonsistentes Verhalten auf, je nachdem, welcher Proxy-Server verwendet wird.
- Wenn ein Proxy-Server nicht mehr aktuell ist, enthält er möglicherweise keine aktuellen Sicherheitsverbesserungen.

Wenn ein Proxy-Server aus einer früheren Version mit einer neueren Version der Instanz registriert wird, erhalten Sie regelmäßig Benachrichtigungen, dass der Proxy-Server nicht mehr aktuell ist. Um eine optimale und sichere Umgebung zu gewährleisten, empfiehlt ServiceNow, den Proxy-Server stets auf die neueste Version der von Ihrer Instanz unterstützten Software zu aktualisieren.

Ein Upgrade für den Edge Encryption Proxy-Server planen

Erstellen Sie einen Upgrade-Zeitplan, damit die Instanz einen veralteten Proxy-Server aktualisieren kann.

Vorbereitungen

Um ein Upgrade zu planen, müssen Sie über den Proxy-Server bei Ihrer Instanz angemeldet sein.
Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Sobald das Upgrade geplant ist, wird der Proxy-Server automatisch zum geplanten Zeitpunkt aktualisiert. Während des Upgrades ist der Proxy-Server nur für kurze Zeit offline.

Hinweis:
Da der Proxy-Server während des Upgrades neu startet, ist er für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

Während des geplanten Upgrades wird ein neues Proxy-Verzeichnis erstellt und Ihre Konfigurationsdateien werden in das neue Verzeichnis kopiert. Neue Eigenschaften werden in Ihre vorhandene Eigenschaftendatei geschrieben. Die folgenden Dateien oder Verzeichnisse in Ihrem alten Proxy-Verzeichnis werden in das neue Proxy-Verzeichnis kopiert.

- Das Verzeichnis /conf
- Das Verzeichnis /keys
- Das Verzeichnis /keystore
- Die Datei java/jre/lib/security/cacerts

Dadurch bleiben Ihre Schlüssel, Schlüsselspeicher, Einstellungen und Zertifikate erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Nur die oben genannten Dateien werden in das neue Proxy-Verzeichnis kopiert. Andere angepasste Dateien im Proxy-Server-Verzeichnis werden während eines geplanten Upgrades nicht beibehalten. Die Upgrade-Protokolldatei befindet sich im ursprünglichen Proxy-Verzeichnis im folgenden Ordner: <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Wenn mehrere Proxy-Server nicht mehr aktuell sind, muss für jeden Proxy-Server ein Upgrade individuell geplant werden.

Hinweis:
Vermeiden Sie das Hosten mehrerer Proxy-Server auf demselben Computer. Wenn Ihre Umgebung diese Konfiguration enthält, sollten Sie jedoch nicht gleichzeitig Upgrades für mehrere Proxys auf demselben Computer planen.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Proxys** > **Upgrade-Zeitpläne**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus.

Formular für den Zeitplan für die Aktualisierung des Edge Encryption Proxy

Feld	Beschreibung
Proxy-Server	Proxy-Server wird aktualisiert.
Zielversion	Version, auf die Sie Ihren Proxy-Server aktualisieren. Dieser Wert ist schreibgeschützt und auf die aktuellste für Ihre Instanz verfügbare Proxy-Version festgelegt.
Geplante Startzeit	Datum und Uhrzeit, zu der das Upgrade gestartet werden soll.
Aktiv	Gibt an, ob das geplante Upgrade aktiv ist. Wenn dieses Feld nicht ausgewählt ist, wird das Upgrade nicht zum geplanten Datum und zur geplanten Uhrzeit ausgeführt.
Status	Der Upgrade-Status. Dieser Wert ist schreibgeschützt. Mögliche Status sind: ○ Ausstehend ○ Wird ausgeführt ○ Abgeschlossen ○ Fehlgeschlagen

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Die typische Zeit für ein Upgrade beträgt weniger als 15 Minuten. Nachdem ein Upgrade ausgeführt wurde, können Sie die Upgrade-Details überprüfen, um mehr darüber zu erfahren. Wenn Ihr Upgrade fehlgeschlagen ist, überprüfen Sie **Fehlergrund**, um die nächsten Schritte festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade-Details

Feld	Beschreibung
Ab Version	Die Version, von der der Server aktualisiert wurde.
Zur Version	Die Version, auf die der Server aktualisiert wurde.
Tatsächliche Startzeit	Zeit, zu der das Upgrade begann.
Endzeit	Uhrzeit, zu der das Upgrade beendet wurde.
Fehlergrund	Grund für das Fehlschlagen des Upgrades.

Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren

Einen Proxy aktualisieren, der unter Linux ausgeführt wird.

Vorbereitungen

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Erforderliche Rolle: security_admin oder lokaler Administrator auf dem Hostcomputer

Prozedur

1. Laden Sie die Edge Encryption Proxy-Update-Archivdatei in das Installationsverzeichnis herunter.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**
   b. Klicken Sie auf den Link **Befehlszeilen-Installationsprogramm herunterladen**.
   c. Wenn der Download beginnt, wählen Sie Ihr Installationsverzeichnis als Download-Speicherort aus.
2. Wechseln Sie in das Installationsverzeichnis.
3. Führen Sie den folgenden Befehl aus:

```
java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade -c <proxy directory>
```

Option	Beschreibung
Proxy-Verzeichnis	Das Verzeichnis im Installationsverzeichnis, in dem der Proxy ursprünglich installiert wurde. Dieses Verzeichnis wird von der Installation erstellt.

Wenn Sie den Hilfebildschirm anzeigen möchten, führen Sie diesen Befehl ohne Argumente aus: `java -jar edgeencryption-dist-<version>-linux-x86-64.jar`

Ein neues Proxy-Verzeichnis wird mit einem aktuellen Zeitstempel erstellt. Eine Sicherung des alten Proxy-Verzeichnisses wird als „backup.dist-upgrade_timestamp“ im neuen Proxy-Installationsverzeichnis verwaltet. Der alte Proxy wird heruntergefahren und der neue Proxy gestartet. Alle offenen Verbindungen/Transaktionen auf dem alten Proxy-Server werden beendet.

4. Überprüfen Sie das Proxy-Protokoll im neuen Verzeichnis und in der Instanz, um sicherzustellen, dass der neue Proxy ausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren

Einen Proxy aktualisieren, der unter Windows ausgeführt wird.

Vorbereitungen

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Erforderliche Rolle: security_admin oder lokaler Administrator auf dem Hostcomputer

Prozedur

1. Laden Sie die Edge Encryption Proxy-Update-Archivdatei in das Installationsverzeichnis herunter.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**
   b. Klicken Sie auf den Link **Befehlszeilen-Installationsprogramm herunterladen**.
   c. Wenn der Download beginnt, wählen Sie Ihr Installationsverzeichnis als Download-Speicherort aus.
2. Starten Sie das Windows-CMD-Terminalprogramm mit Administratorrechten.
3. Wechseln Sie in das Installationsverzeichnis.
4. Führen Sie den folgenden Befehl aus:

   ```
   java -jar-Edge-Encryption-Dist-<version> -all.jar -m dist-upgrade -c<proxy directory>
   ```

Option	Beschreibung
Proxy-Verzeichnis	Das Verzeichnis im Installationsverzeichnis, in dem der Proxy ursprünglich installiert wurde. Dieses Verzeichnis wird von der Installation erstellt.

   Wenn Sie den Hilfebildschirm anzeigen möchten, führen Sie diesen Befehl ohne Argumente aus: `java -jar Edge-Verschlüsselung-Dist-<version> -all.jar`

   Ein neues Proxy-Verzeichnis wird mit einem aktuellen Zeitstempel erstellt. Eine Sicherung des alten Proxy-Verzeichnisses wird als „backup.dist-upgrade_timestamp“ im neuen Proxy-Installationsverzeichnis verwaltet. Der alte Proxy wird heruntergefahren und der neue Proxy gestartet. Alle offenen Verbindungen/Transaktionen auf dem alten Proxy-Server werden beendet.
5. Überprüfen Sie das Proxy-Protokoll im neuen Verzeichnis und in der Instanz, um zu überprüfen, ob der Proxy aktualisiert wurde und ausgeführt wird.

Ein Upgrade des Edge Encryption Proxy-Servers rückgängig machen

Wenn ein Proxy-Upgrade nicht erfolgreich ist, können Sie zur vorherigen Version zurückkehren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein Upgrade bei Verwendung der geplanten Upgrade-Funktion in der Version Washington DC fehlschlägt, wird der Proxy-Server automatisch auf die alte Version zurückgesetzt. Der alte Proxy-Server wird unverändert in einem Sicherungsverzeichnis gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie ein manuelles Upgrade rückgängig machen möchten, können Sie diese Schritte ausführen.

Prozedur

1. Fahren Sie den Proxy herunter.
2. Löschen Sie das neue Proxy-Verzeichnis.
3. Benennen Sie das Sicherungsverzeichnis in den Proxy-Namen um.
   Das Sicherungsverzeichnis befindet sich im Proxy-Installationsverzeichnis mit dem Namen <proxy name>_backup
4. Starten Sie den Proxy.
5. Überprüfen Sie das Proxy-Protokoll und die Instanz, um sicherzustellen, dass der Proxy online ist.

Edge Encryption konfigurieren

Nachdem der Edge Encryption Proxy-Server installiert ist und ausgeführt wird, verwalten Sie Edge Encryption über den Proxy-Server.

Sie müssen alle Schritte unter Edge Encryption wird installiert ausführen, bevor Sie Verschlüsselungskonfigurationen und Verschlüsselungsmuster auf der Instanz erstellen.

Hinweis:
Um auf die Konfiguration von Edge Encryption zugreifen zu können, müssen Sie sich über den Proxy-Server anmelden und zur Rolle security_admin wechseln.

Rotation von Verschlüsselungsschlüsseln

Führen Sie die Rotation von Verschlüsselungsschlüsseln aus der Instanz aus. Fügen Sie einen neuen Schlüssel hinzu, ändern Sie die Standardschlüsselzuordnung, und planen Sie dann einen Massenschlüssel-Rotationsauftrag oder eine Einzelschlüsselrotation.

Bevor Sie einen Verschlüsselungsschlüssel als Standardschlüssel festlegen, stellen Sie den Schlüssel für jeden Proxy zur Verfügung. Dadurch wird sichergestellt, dass die Proxys den Schlüssel zur Verschlüsselung von Daten haben, wenn der Schlüssel als Standardschlüssel zugewiesen wird. Alle Proxys müssen Zugriff auf einen Schlüssel haben, bevor dieser Schlüssel als Standardschlüssel zugewiesen werden kann.

Warnung:
Bevor Sie einen Schlüssel aus dem Proxy löschen, müssen Sie einen Massenschlüssel-Rotationsauftrag einrichten und ausführen, um sicherzustellen, dass keine Daten in der Instanz den Schlüssel verwenden. Wenn noch Daten mit diesem Schlüssel verschlüsselt sind, können Sie die Informationen nicht mehr entschlüsseln, nachdem der Schlüssel gelöscht wurde.

Edge-Filterung und Sortierverhalten

Stellen Sie jedes Mal, wenn Sie Standardschlüssel ändern, sicher, dass Sie eine Schlüsselrotation (Massen- oder Einzelschlüsselrotation) durchführen. Andernfalls erhalten Sie unter Umständen unerwartete Ergebnisse beim Sortieren und Filtern von Datensätzen. Stellen Sie sich zum Beispiel das folgende Szenario vor:

1. Sie erstellen mit einem einzigen Verschlüsselungsschlüssel verschlüsselte Datensätze.
2. Sie erstellen einen neuen Schlüssel und legen diesen als Standard fest.
3. Sie erstellen mit dem neuen Verschlüsselungsschlüssel einen neuen Satz verschlüsselter Datensätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie nach einem beliebigen verschlüsselten Feld filtern, während eine Verbindung über den Edge-Proxy hergestellt ist, werden möglicherweise nicht alle Datensätze richtig herausgefiltert, oder es werden gegebenenfalls Datensätze unerwarteterweise angezeigt. Der Filter funktioniert nur für Datensätze, die mit dem aktuellen Standardschlüssel verschlüsselt sind. Die Datensätze, die mit dem vorherigen Standardschlüssel verschlüsselt wurden, werden weiterhin in der Listenansicht angezeigt.

Wenn Sie nach einem beliebigen verschlüsselten Feld sortieren, während eine Verbindung über den Edge-Proxy hergestellt ist, werden zwei Gruppen von Datensätzen mit demselben visuell lesbaren Text im verschlüsselten Feld angezeigt.

Einen Einzelschlüssel-Rotationsauftrag planen

Planen Sie einen Auftrag, um Daten zu finden, die mit einem bestimmten Schlüsselalias verschlüsselt sind, und verschlüsseln Sie die Daten dann erneut mit dem aktuellen Standardverschlüsselungsschlüssel. Die Daten werden entschlüsselt, bevor sie mit dem Standardschlüssel erneut verschlüsselt werden.

Vorbereitungen

Erforderliche Rolle: security_admin

Aktualisieren Sie vor der Planung dieser Aufgabe den Standardschlüssel in **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Standardschlüssel festlegen**.

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Reserviert** > **Einzelschlüsselrotation planen**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Einzelschlüsselrotation**.
Schlüssel	Geben Sie den Schlüssel ein, der stillgelegt werden soll. Vergewissern Sie sich, dass dieser Schlüssel nicht mehr der Standardschlüssel in ist **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Standardschlüssel festlegen**.
Anzahl der Datensätze schätzen	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Nicht verfügbar, wenn eine Einzelschlüsselrotation ausgeführt wird.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Dieses Feld ist schreibgeschützt und aktiv. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl der Audit-Datensätze, die verarbeitet werden sollen. Nicht verfügbar, wenn eine Einzelschlüsselrotation ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
Anzahl der Datensätze schätzen wird bei der Verarbeitung geprüfter Felder nicht unterstützt.

Einen Massenschlüssel-Rotationsauftrag planen

Planen Sie einen Auftrag, um nach mit einem vorherigen Schlüssel verschlüsselten Daten zu suchen, und verschlüsseln Sie die Daten anschließend erneut mit den aktuellen Standard-Verschlüsselungsschlüsseln. Die Daten werden entschlüsselt, bevor sie mit dem aktuellen Standardschlüssel erneut verschlüsselt werden.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Schlüsselmassenrotation planen**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Massenschlüsselrotation**.
Schätzen Sie die Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Nicht verfügbar, wenn eine Massenrotation ausgeführt wird.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Dieses Feld ist schreibgeschützt und aktiv. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl der Audit-Datensätze, die verarbeitet werden sollen. Nicht verfügbar, wenn eine Massenrotation ausgeführt wird.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, um diesen Auftrag zu deaktivieren.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
   Anzahl der Datensätze schätzen wird bei der Verarbeitung geprüfter Felder nicht unterstützt.

Einen Rotationsauftrag für einen Anhangsschlüssel planen

Planen Sie einen Auftrag, um mit einem bestimmten Schlüsselalias verschlüsselte Anhänge zu finden, und verschlüsseln Sie die Anhänge dann erneut mit dem aktuellen Standardverschlüsselungsschlüssel. Der Anhang wird entschlüsselt, bevor er mit dem Standardschlüssel erneut verschlüsselt wird.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Anhangsschlüsselrotation planen**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Anhangsschlüsselrotation**.
Aktiv	Deaktivieren Sie das Häkchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Geschätzte Datensatzanzahl**.
5. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Felder mit Verschlüsselungskonfigurationen verschlüsseln

Verschlüsseln Sie Felder, indem Sie Verschlüsselungskonfigurationen erstellen.

Um Edge Encryption zu konfigurieren, müssen Sie über den Proxy mit der Instanz verbunden sein. Testen Sie alle Änderungen in einer Nicht-Produktionsinstanz, bevor Sie sie auf die Produktionsinstanz anwenden.

Verschlüsselungsschlüssel definieren

Nachdem ein oder mehrere Proxys eingerichtet und ein Standardverschlüsselungsschlüssel konfiguriert wurde, überprüft die Instanz, ob die Schlüssel für alle Proxys verfügbar sind. Sie können einen Verschlüsselungsschlüssel nicht als Standardschlüssel festlegen, es sei denn, alle Proxys haben den Schlüssel. Nachdem ein Standardschlüssel definiert wurde, können Sie Verschlüsselungskonfigurationen erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zu verschlüsselnde Felder und Anlagen zuweisen

Die Zuweisung von zu verschlüsselnden Feldern und Anhängen bedeutet, dem Feld oder der Anlage einen Verschlüsselungstyp zuzuordnen. Bevor Sie ein Feld als verschlüsselt markieren, bewerten Sie diese Vorfälle.

- Bestimmen Sie, welche Systemfunktionen betroffen sein könnten.
- Überprüfen Sie alle Skripts auf die Verwendung des Felds.
- Nehmen Sie die gewünschten Änderungen an der Feldgröße vor. Nachdem ein Feld für die Verschlüsselung konfiguriert wurde, kann die Feldgröße nicht mehr geändert werden.

Durch Markieren eines zu verschlüsselnden Felds wird die Feldgröße zum Speichern der verschlüsselten Daten erweitert. Das Erweitern der Feldgröße kann je nach Anzahl der Datensätze in der Tabelle lange dauern.

API-Unterstützung

Die Verschlüsselung auf Spaltenebene aktualisiert die APIs `setDisplayValue()` und `setValue()`, sodass sie verschlüsselte Daten für verschlüsselte Felder einfügen können. Außerdem können `getDisplayValue()` und `getValue()` Klartextwerte zurückgeben.

Das folgende Skript veranschaulicht diese API-Änderungen, wenn die Kurzbeschreibung des Incidents verschlüsselt wird:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Wenn Sie `getValue()` verwenden, um verschlüsselten Text abzurufen, gibt Ihr Skript den Geheimtext nicht mehr zurück. Ihr Skript gibt den Nur-Text zurück, vorausgesetzt, der Benutzer hat Zugriff auf das kryptografische Modul. `getValue()` gibt den Geheimtext zurück, wenn der Benutzer keinen Zugriff auf das kryptografische Modul hat.

Erstellen Sie eine Feldverschlüsselungskonfiguration

Wählen Sie die zu verschlüsselnden Felder aus und geben Sie den Verschlüsselungstyp an.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Neu erstellen**.
2. Füllen Sie das Formular aus.

Feld	Beschreibung
Tabelle	Die Tabelle, die das zu verschlüsselnde Feld enthält.
Typ	Ob eine Tabellenspalte oder Anhänge für die Tabelle verschlüsselt werden sollen. Wählen Sie **Spalte**.
Spalte	Das zu verschlüsselnde Feld. Wird nur angezeigt, wenn der **Typ** **Spalte** ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Nur Felder vom Typ Zeichenfolge, Datum, Datum/Uhrzeit, Journal, Journaleingabe und URL werden unterstützt. ○ **Felder vom Typ Zeichenfolge und URL**: Sie können eine Verschlüsselungskonfiguration einer übergeordneten Tabelle oder einer untergeordneten Tabelle hinzufügen. ○ **Felder vom Typ Datum und Datum/Uhrzeit**: Sie können eine Verschlüsselungskonfiguration nur einer übergeordneten Tabelle hinzufügen. Sie können eine neue Verschlüsselungskonfiguration nicht einer untergeordneten Tabelle hinzufügen. **Hinweis:** Je nach Anzahl der Datensätze, die von den Datum- und Datum/Uhrzeit-Feldern, die Sie verschlüsseln, betroffen sind, kann es einige Minuten dauern, die Verschlüsselungskonfiguration zu erstellen. Stellen Sie sicher, dass Sie die Verschlüsselungskonfiguration für die Felder vom Typ Datum und Datum/Uhrzeit erstellen, wenn das Transaktionsvolumen in der Instanz gering ist.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp.

Hinweis:
Eine bestimmte Tabellen- und Feldkombination kann jeweils nur eine aktive Konfiguration haben.

3. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Nachdem Sie den Verschlüsselungskonfigurationsdatensatz hinzugefügt haben, können Sie einen Verschlüsselungsauftrag erstellen, um vorhandene Daten zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag ausführen, werden die vorhandenen Daten bei der nächsten Änderung der Daten von Edge verschlüsselt. Details finden Sie unter Einen Verschlüsselungsauftrag planen.

Erstellen Sie eine Konfiguration für die variable Verschlüsselung

Wählen Sie die zu verschlüsselnden Servicekatalogvariablen aus, und geben Sie den Verschlüsselungstyp an.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur
1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung**.
2. Klicken Sie in der Liste „ **Edge Encryption-Variablenkonfigurationen“** auf **Neu**.
3. Füllen Sie das Formular aus.

Feld	Beschreibung
Variable	Die zu verschlüsselnde Variable.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Nachdem Sie den Verschlüsselungskonfigurationsdatensatz hinzugefügt haben, können Sie einen Verschlüsselungsauftrag erstellen, um vorhandene Daten zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag ausführen, werden die vorhandenen Daten bei der nächsten Änderung der Daten von Edge verschlüsselt. Details finden Sie unter Einen Verschlüsselungsauftrag planen.

Eine Verschlüsselungskonfiguration deaktivieren

Nachdem Sie ein Feld oder die Anhänge einer Tabelle für die Verschlüsselung konfiguriert haben, können Sie die Verschlüsselung beenden, indem Sie die Verschlüsselungskonfiguration deaktivieren. Nach dem Deaktivieren der Verschlüsselung können Sie einen Entschlüsselungsauftrag für Felder oder einen Entschlüsselungsauftrag für Anhänge ausführen, um die verschlüsselten Daten aus der Instanz zu entfernen.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

⚠ Warnung:
Durch das Deaktivieren einer Verschlüsselungskonfiguration wird der Verschlüsselungsdatensatz nicht gelöscht, und der Verschlüsselungstyp kann nicht geändert werden.

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Konfigurationen der Edge Encryption** > **Alle**.
   Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.
2. Klicken Sie auf die zu deaktivierende Verschlüsselungskonfiguration.
   Das Formular **Edge Encryption-Konfiguration** wird angezeigt.
3. Klicken Sie auf das Feld **Aktiv**.
   Das Feld **Aktiv** ist leer.
4. Klicken Sie auf **Aktualisieren**.
   Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.

Nächste Maßnahme

Sie können einen Entschlüsselungs- oder Anlagenentschlüsselungsauftrag ausführen, um Daten in der Instanz zu entschlüsseln. Wenn Sie keinen Auftrag ausführen, werden die verschlüsselten Daten bei der nächsten Änderung entschlüsselt.

Einen Verschlüsselungsauftrag planen

Sie können einen Auftrag zum Auffinden und Verschlüsseln aller unverschlüsselten Daten in einem bestimmten Feld mit dem für das Feld konfigurierten Standardverschlüsselungsschlüssel planen. Wenn Sie nach dem Konfigurieren eines Felds für die Verschlüsselung keinen Verschlüsselungsauftrag erstellen, werden nur neue Werte verschlüsselt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle** , um einen Auftrag für ein Feld oder zu erstellen **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung** , um einen Job für eine Variable zu erstellen.
2. Klicken Sie auf das Feld, für das Sie einen Verschlüsselungsauftrag planen möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenverschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für alle vorherigen Auftragsausführungen angezeigt.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Auftragsart	Wählen Sie **Verschlüsselung**.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Geschätzte Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl geprüfter Datensätze, die verarbeitet werden sollen. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt. Dieses Feld ist nur sichtbar wenn **Historische Aufzeichnungen verarbeiten** ausgewählt ist. **Hinweis:** Die Schätzung kann größer sein als die tatsächliche Anzahl der verarbeiteten Datensätze.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Einen Entschlüsselungsauftrag planen

Sie können einen Auftrag zum Entschlüsseln von Daten in einem verschlüsselten Feld einplanen, um klare Daten in der Instanz zu speichern.

Vorbereitungen

Hinweis:
Sie müssen den Verschlüsselungsdatensatz für das Feld als inaktiv markieren (deaktivieren Sie das Feld **Aktiv**), um den Entschlüsselungsauftrag auszuführen.

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle** , um einen Auftrag für ein Feld oder zu erstellen **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung** , um einen Job für eine Variable zu erstellen.
2. Klicken Sie auf das Feld, das Sie entschlüsseln möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenentschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Entschlüsselung**.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Geschätzte Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale	Geschätzte maximale Anzahl geprüfter Datensätze, die verarbeitet werden sollen. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt. Dieses Feld ist nur sichtbar wenn **Historische Aufzeichnungen verarbeiten** ausgewählt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Anzahl der Audit-Datensätze	**Hinweis:** Die Schätzung kann größer sein als die tatsächliche Anzahl der verarbeiteten Datensätze.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Anhänge mithilfe der Standardverschlüsselung verschlüsseln

Sie können Anhänge für bestimmte Tabellen verschlüsseln.

Alle Anhänge für eine Tabelle verwenden denselben Verschlüsselungstyp. Verschlüsselte Anhänge werden bei der Textsuche nicht durchsucht. Für Anhänge sind nur die Standardverschlüsselungstypen zulässig. Die ordnungs- und gleichstellungserhaltenden Verschlüsselungstypen sind nicht zulässig.

Für eine Sitzung unter Umgehung des Edge Encryption Proxy:

- Auf einem Datensatz mit aktivierter Anhangsverschlüsselung:
  - Der Benutzer kann Anhänge und die Namen der Anhänge sehen.
  - Der Benutzer kann keine neuen Anhänge hinzufügen.
- Auf einem Datensatz ohne aktivierte Anhangsverschlüsselung:
  - Der Benutzer kann vorhandene Anhänge öffnen und herunterladen.
  - Der Benutzer kann neue Anhänge hinzufügen.

Für eine Sitzung, die den Verschlüsselungsproxy verwendet, kann der Benutzer bestehende Anhänge öffnen und herunterladen sowie neue Anhänge hinzufügen.

Die Anhangsverschlüsselung konfigurieren

Wählen Sie die Tabellen aus, deren Anhänge verschlüsselt werden sollen, und geben Sie den Verschlüsselungstyp an.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfigurationen der Edge Encryption** > **Neu erstellen**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration der Edge Encryption

Feld	Beschreibung
Tabelle	Wählen Sie eine Tabelle aus, deren Anhänge verschlüsselt werden sollen.
Typ	Ob eine Tabellenspalte oder Anhänge für die Tabelle verschlüsselt werden sollen. Wählen Sie **Anhang**.
Spalte	Das zu verschlüsselnde Tabellenfeld. Dieses Feld wird angezeigt, wenn der **Typ Spalte** und nicht **Typ Anhang** ist.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp. Für Anhänge sind nur Standard AES128 und Standard AES256 zulässig.

3. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Nachdem der Verschlüsselungsdatensatz hinzugefügt wurde, können Sie einen Anhangsverschlüsselungsauftrag erstellen, um vorhandene Anhänge zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag für Anhänge ausführen, verschlüsselt das System neue Anhänge, wenn Sie sie anhängen.

Hinweis:
Wenn Sie das `Attribut „edge_encryption_clear_attachment_allowed“` im Dictionary-Eintrag der Tabelle als „ **True** “ markieren, werden unverschlüsselte Anhänge einer Tabelle mithilfe von Edge Encryption hinzugefügt, um Anhänge zu verschlüsseln. Wenn Sie dieses Attribut aktivieren, sollten Sie einen Verschlüsselungsauftrag für Anhänge einrichten, damit alle hinzugefügten unverschlüsselten Anhänge verschlüsselt werden.

Einen Anhangsverschlüsselungsauftrag planen

Sie können einen Auftrag so planen, um unverschlüsselte Anhänge für eine angegebene Tabelle zu suchen und zu verschlüsseln. Verwenden Sie dazu den für die Tabelle konfigurierten Standard-Verschlüsselungsschlüssel.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**.
2. Klicken Sie auf die Tabelle, für die Sie einen Verschlüsselungsauftrag planen möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenverschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Auftragsart	Wählen Sie **Anhangsverschlüsselung**.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Einen Anhangsentschlüsselungsauftrag planen

Sie können einen Auftrag planen, um alle verschlüsselten Anhänge für eine bestimmte Tabelle zu entschlüsseln und klare Anhänge in der Instanz zu speichern.

Vorbereitungen

Hinweis:
Sie müssen den Verschlüsselungsdatensatz für die Tabelle als inaktiv markieren (deaktivieren Sie das Feld **Aktiv**), um den Entschlüsselungsauftrag auszuführen, da ansonsten nichts passieren wird.

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**.
2. Klicken Sie auf die Tabelle mit den Anlagen, die Sie entschlüsseln möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Anhangsmassenentschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Anhangsentschlüsselung**.
Aktiv	Deaktivieren Sie das Häkchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Den Verschlüsselungstyp eines Felds oder Anhangs ändern

Sie können den Verschlüsselungstyp eines Felds oder eines Anhangs ändern, indem Sie im vorhandenen Verschlüsselungskonfigurationssatz einen neuen Verschlüsselungstyp auswählen. Eine bestimmte Tabellen- und Feldkombination kann jeweils nur eine aktive Konfiguration haben.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**. Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.
2. Öffnen Sie den Datensatz für die zu ändernde Verschlüsselungskonfiguration.
3. Klicken Sie auf die Dropdown-Liste **Verschlüsselungstyp** und wählen Sie einen neuen Verschlüsselungstyp.

   Hinweis:
   Für Anhänge sind nur Standard AES128 und Standard AES256 zulässig.

4. Führen Sie, falls erforderlich, einen Auftrag zur Verschlüsselung oder Anhangsverschlüsselung aus.
   Es ist nicht notwendig, einen Verschlüsselungsauftrag auszuführen. Wenn Sie keinen Verschlüsselungsauftrag ausführen, wird das Feld oder der Anhang bei der nächsten Änderung des Felds oder des Anhangs mit dem neuen Verschlüsselungstyp verschlüsselt.

Zeichenketten mithilfe von Verschlüsselungsmustern tokenisieren

Sie können Zeichenkettenmuster durch Token ersetzen, bevor sie an die Instanz gesendet und dort gespeichert werden.

Vorbereitungen

Um Verschlüsselungsmuster verwenden zu können, müssen Sie eine MySQL-Datenbank in Ihrem Netzwerk installieren und einrichten. Dies ist die gleiche Datenbank, die für die ordnungserhaltende Verschlüsselung verwendet wird. Um Verschlüsselungsmuster erstellen oder bearbeiten zu können, müssen Sie über den Proxy mit der Instanz verbunden sein.

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Basissystemmuster verwenden oder eigene Muster erstellen. Basissystemmuster sind erweiterte Muster. Verschlüsselungsmuster enthalten die folgenden Einschränkungen.

- Ein Muster aller Alpha-Zeichen ist nicht zulässig.
- Die minimale Mustergröße beträgt fünf Zeichen. Sie können diese Einstellung mithilfe einer Systemeigenschaft ändern.
- Die Quantifizierer * und + sind in Verschlüsselungsmustern nicht zulässig.
- Verschlüsselungsmuster stimmen mit vollständigen Wörtern überein, nicht mit Teilen von Zeichenfolgen, die in eine größere Zeichenfolge eingebettet sind. Wörter werden durch Leerzeichen und Zeichen definiert, die nicht in ein Muster eingefügt werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn dieselbe Zeichenfolge mehrmals an die Instanz gesendet wird, wird sie durch das gleiche Token ersetzt.
- Die Textsuche nach exakten Übereinstimmungen wird unterstützt. Die Abfragezeichenfolge wird mit einem Token ausgetauscht, wenn sie an die Instanz gesendet wird, die Suche nach Token durchgeführt wird und wenn die Suchergebnisse an den Proxy-Server zurückgegeben werden, werden die Token durch den Klartext ersetzt. Features wie Stemming werden nicht unterstützt.

Bei der Verwendung von Mustern verlässt der Klartext niemals Ihr Netzwerk. Wenn der Proxy-Server mit einem Muster in einer Anforderung übereinstimmt, die an die Instanz gerichtet ist, ersetzt der Proxy die Zeichenfolge durch ein Token derselben Größe. Das Token wird anstelle der Klartextzeichenfolge an die Instanz gesendet. Wenn die Antwort von der Instanz an den Proxy-Server gesendet wird, ersetzt der Proxy das Token durch die Zeichenfolge. Bei Anzeige über den Proxy-Server wird die Zeichenfolge als Klartext angezeigt.

Hinweis:
Verschlüsselte Felder werden nicht auf Verschlüsselungsmuster geprüft.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Verschlüsselungsmuster** > **Neu erstellen**.
   Alternativ können Sie zu **Erweiterte Muster** navigieren, um ein vorkonfiguriertes Muster zu aktivieren oder zu bearbeiten.
2. Geben Sie den Musternamen ein.
3. Definieren Sie den **Eingabetyp für Edge-Muster**.

Option	Bezeichnung
Basis	Eine Reihe von Zeichentypen. Klicken Sie in der Registerkarte **Eingabe Basismuster** auf die Registerkarte **Hinzufügen** und wählen Sie einen Zeichentyp. Das **Beispielmuster** zeigt das Muster an, wenn Zeichen hinzugefügt werden. Klicken Sie auf **Neuer Block**, um das nächste Zeichen in die nächste Zeile zu verschieben. Auf diese Weise können Sie Zeichen in einem langen Muster gruppieren. Klicken Sie auf **X**, um das letzte Zeichen im Muster zu löschen.
Erweitert	Ein Java-RegEx-Ausdruck. Wenn „Erweitert“ ausgewählt ist, können Sie den Eingabetyp nicht wieder in „Basis“ ändern. Geben Sie im Feld **Beispielmuster** ein Muster ein, um den RegEx-Ausdruck zu testen. Geben Sie im Feld **Muster** einen Java-RegEx-Ausdruck ein. Klicken Sie auf **Bestäti**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	gen, um zu überprüfen, ob der Ausdruck mit dem Muster übereinstimmt.

Der Eingabetyp legt fest, wie Sie das Muster eingeben. Die Verwendung des Musters wird dadurch nicht beeinflusst.

4. Klicken Sie auf **Absenden**.

Ordnungserhaltend verschlüsselte Daten reparieren oder wiederherstellen

Wenn Sie die Rolle Security-Admin haben, können Sie vom Edge Encryption Proxy ausgeführte Aufträge planen, um Felder zu reparieren oder wiederherzustellen, die ordnungserhaltende Verschlüsselung verwenden.

Aufgaben planen für:

- Auftragstoken zu reparieren
- Die Proxy-Datenbank neu zu erstellen.

Das Ausführen dieser Jobs kann ein zeitaufwändiger Vorgang sein, der sich auf die Leistung des Edge Encryption -Proxy auswirken kann. Planen Sie diese Jobs zu einem Zeitpunkt ein, zu dem keine Benutzer oder eine minimale Anzahl von Benutzern das System nutzen, z. B. am Wochenende um Mitternacht.

Einen Reparaturauftrag für ein Auftragstoken planen

Sie können einen Auftrag planen, um Felder zu finden und zu reparieren, in denen das Auftragstoken fehlt.

Vorbereitungen
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie diese Aufträge, um einzelne Felder in einer Tabelle zu reparieren oder um alle Felder unter Verwendung der ordnungserhaltenden Verschlüsselung zu reparieren. Führen Sie diesen Auftrag aus, wenn die Proxy-Datenbank während der Ausführung der Instanz offline war. Dies führt zu ordnungserhaltenden Feldern, deren Auftragstoken fehlen.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Plantafel Tokenreparatur**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Reparatur von Reihenfolge-Token**.
Alle Felder	Aktivieren Sie dieses Kontrollkästchen, um alle Tabellen zu reparieren.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Geschätzte Datensatzanzahl**.

Einen Proxy-Datenbank-Wiederherstellungsauftrag planen

Führen Sie diesen Auftrag aus, wenn die Proxy-Datenbank Daten verloren hat. Dieser Auftrag findet alle Datensätze, die mit einem Token verschlüsselt wurden (ordnungserhaltender Verschlüsselungstyp), und sendet sie an den Proxy, damit die Proxy-Datenbank neu erstellt werden kann.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Datenbankwiederherstellung planen**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen für diesen Auftrag ein.
Auftragsart	Wählen Sie **Datenbankwiederherstellung**.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der dieser Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.

Konfigurieren Sie die Deny-Liste für IP-Adressen

Verhindern Sie, dass eine IP-Adresse in Ihrem Netzwerk Anforderungen an Ihre Instanz sendet

Vorbereitungen

Erforderliche Rolle: security_admin

Da sich der Edge Encryption Proxy-Server in Ihrem Netzwerk befindet, kann er Schwachstellen-Scans durch Ihre Netzwerksoftware unterzogen werden. Um zu verhindern, dass IP-Scanner- oder andere Anforderungen an Ihre ServiceNow -Instanz weitergeleitet werden, können Sie IP-Adressen, IP-Bereiche oder Netzwerkmasken zu einer Deny-Liste hinzufügen. Jede Verbindung mit dem Proxyserver von einer Deny-Listenadresse wird beendet und nicht an Ihre Instanz weitergeleitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine IP-Adresse auf eine Deny-Liste zu setzen, müssen Sie über den Proxy-Server bei Ihrer Instanz angemeldet sein.

Wichtig:
Stellen Sie sicher, dass Sie Ihre Netzwerktopologie verstehen, bevor Sie IP-Adressen in Ihrem Netzwerk zu einer Deny-Liste hinzufügen. Wenn der Deny-Liste eine IP-Adresse hinzugefügt wird, wird jeder Benutzer mit dieser IP-Adresse für den Zugriff auf den Proxy-Server Edge Encryption gesperrt.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **IP-Adressen auf Deny-Liste**.
   Die Listenansicht „Encryption Proxy IP Denylists“ [edge_encryption_ip_blacklist] wird geöffnet.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus.

Feld	Beschreibung
Proxy-Server	Der Edge Encryption -Proxy-Server, der von der Weiterleitung von Anforderungen von Adressen in der Deny-Liste abgehalten wird.
IP, IP-Bereich oder Netzwerkmaske	Anfragen von dieser IP-Adresse, diesem Bereich oder dieser Netzwerkmaske werden nicht an Ihre ServiceNow-Instanz weitergeleitet. Beispielwerte sind: ○ IP-Adresse: 10.10.10.5 ○ IP-Bereich: 10.10.10.1-15 ○ Netzwerkmaske: 10.10.10.0/24 **Hinweis:** Sie können entweder IPv4- oder IPv6-Adressen verwenden
Aktiv	Ob der Datensatz aktiv ist Nur IP-Adressen aus aktiven Datensätzen können keine Anfragen an die Instanz senden.
Beschreibung	Beschreibung des Deny-Listen-Datensatzes.

4. Klicken Sie auf **Absenden**.
5. Wiederholen Sie diese Schritte für alle anderen Proxys, für die eine IP-Adresse verweigert werden soll.

Ergebnisse
Der Proxyserver Edge Encryption beendet alle Verbindungen von IP-Adressen, Bereichen oder Netzwerkmasken in der Deny-Liste und kann die Anforderung nicht an die Instanz weiterleiten.

Daten von einem Datensatzersteller verschlüsseln

Konfigurieren Sie Ihren Edge Encryption -Proxy-Server so, dass Einfügungen von einem Datensatzersteller zugelassen werden, indem Sie Verschlüsselungsregeln aus dem Datensatz des Datensatzerstellers erstellen.

Vorbereitungen
Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatzersteller ermöglichen Endbenutzern das Erstellen von aufgabenbasierten Datensätzen, z. B. Servicekatalog und Serviceportal. Wenn ein Datensatzersteller versucht, Daten in ein für die Verschlüsselung markiertes Feld einzufügen, wird eine ungültige Einfügemeldung angezeigt und die Daten werden nicht im Feld gespeichert.

Das Verschlüsseln von Daten von einem Datensatzersteller erfordert eine für das Zielfeld definierte Verschlüsselungskonfiguration. Stellen Sie sicher, dass Sie eine Verschlüsselungskonfiguration für das Zielfeld und die Zieltabelle erstellt haben, bevor Sie eine Verschlüsselungsregel von einem Datensatzersteller erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Feldverschlüsselungskonfiguration. Um Anhänge eines Datensatzerstellers zu verschlüsseln, Die Anhangsverschlüsselung konfigurieren.

Prozedur

1. Melden Sie sich über den Edge Encryption Proxy-Server bei der Instanz an.
2. Navigieren zu **Servicekatalog** > **Katalogdefinitionen** > **Datensatzersteller**.
3. Erstellen Sie einen Datensatzersteller -Datensatz, oder öffnen Sie einen vorhandenen Datensatzersteller-Datensatz.
4. Wählen Sie unter **Zugehörige Links Eine Edge Encryption-Regel erstellen**.
   Es werden automatisch zwei inaktive Verschlüsselungsregeln erstellt, um Daten zu verschlüsseln, die vom Datensatzersteller an das für die Verschlüsselung markierte Feld gesendet werden.

Verschlüsselungsregel	Beschreibung
<RecordProducerName>	Regel erstellt, um POST-Parameter von Servicekatalog zu verarbeiten und Variablen den Feldern in der Instanz zuzuordnen.
<RecordProducerName>Json	Regel, die erstellt wurde, um eine JSON-Nutzlast von Serviceportal zu verarbeiten und Variablen den Feldern in der Instanz zuzuordnen.

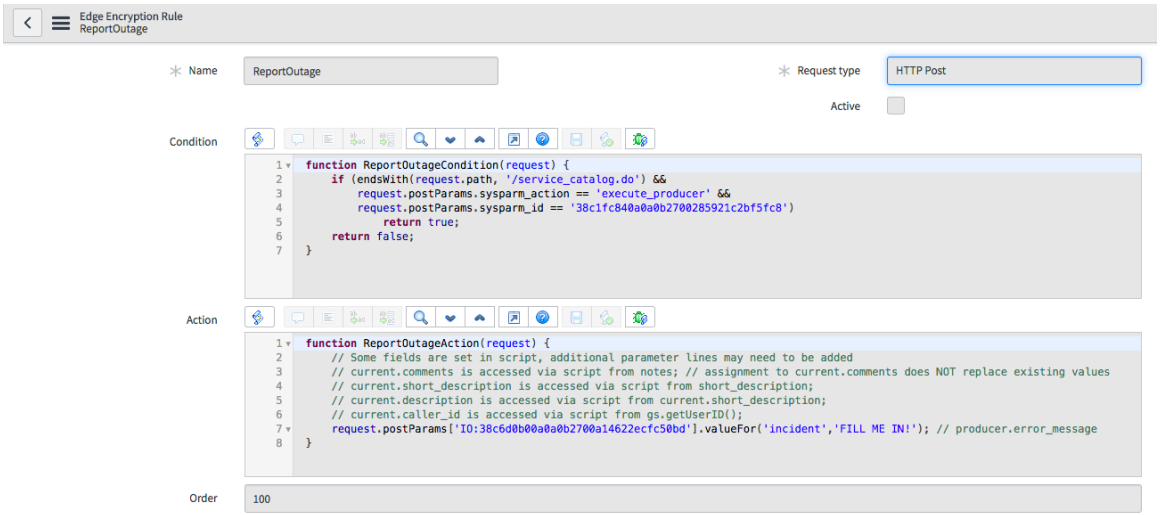
5. Aktivieren Sie die erforderlichen Verschlüsselungsregeln, die vom Datensatzersteller erstellt wurden.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Regeln** > **Alle**.
   b. Öffnen Sie je nach Verwendungsort des Datensatzerstellers die zugehörige vom Datensatzersteller erstellte Verschlüsselungsregel und wählen Sie die Option **Aktiv**.
   Bei Verwendung des Datensatzerstellers im Servicekatalog aktivieren Sie die Verschlüsselungsregel <RecordProducerName>. Bei Verwendung des Datensatzerstellers im Serviceportal aktivieren Sie die Verschlüsselungsregel <RecordProducerName>Json.
6. **Wahlweise:** Untersuchen Sie das **Aktion** der Verschlüsselungsregel und fügen Sie die erforderlichen Feldnamen oder Anweisungen hinzu.

   (Optional) Wenn ein Datensatzersteller eine Variable direkt einem Feld in einer Tabelle zuordnet, ordnet die Verschlüsselungsregel die Variable automatisch dem richtigen Feld zu. Wenn eine Variable jedoch indirekt durch verschiedene Skripts auf der Plattform zugeordnet wird, müssen Sie möglicherweise die Regeln aktualisieren, um jede Variable dem richtigen Feld zuzuordnen.

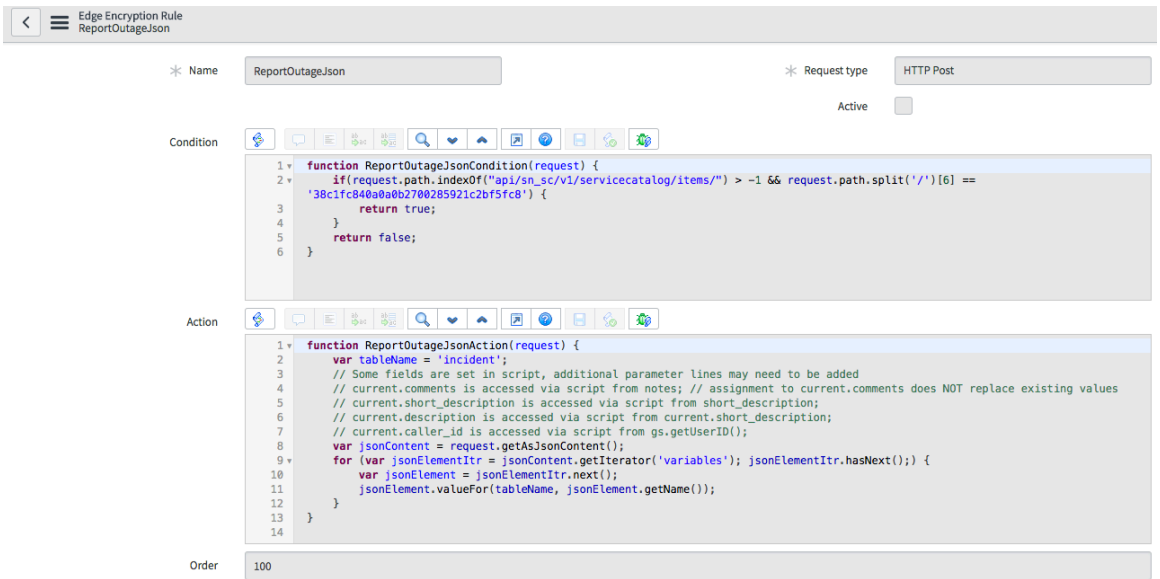
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example

(Optional) Die folgende Verschlüsselungsregel wurde aus dem Datensatzersteller „Report Outage“ erstellt und verarbeitet die POST-Parameter von Servicekatalog, um Variablen den Feldern in der Instanz zuzuordnen. Ersetzen Sie „FÜLL MICH AUS“ mit dem Zielfeld.



Die folgende Verschlüsselungsregel wurde aus dem Datensatzersteller „Report Outage“ erstellt und verarbeitet die JSON-Payload von Serviceportal, um Variablen den Feldern in der Instanz zuzuordnen. Fügen Sie zusätzliche Anweisungen hinzu, um alle Skriptvariablen den Zielfeldern zuzuordnen.



Wenn die Nutzdaten des Datensatzerstellers geprüft werden, enthält das Element error_message den Wert für das Feld short_description. Durch Hinzufügen der folgenden Anweisung können Sie die Skriptvariable error_message dem Feld short_description zuordnen.

```
if (jsonElement.getName() == 'error_message')
    jsonElement.valueFor(tableName, 'short_description');
```

Der Wert des Feldes **Aktion** ändert sich zu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
function ReportOutageJsonAction(request) {
 var tableName = 'incident';
 // Some fields are set in script, additional parameter lines may need to be added
 // current.comments is accessed via script from notes; // assignment to current.comments
 does NOT replace existing values
 // current.short_description is accessed via script from short_description;
 // current.description is accessed via script from current.short_description;
 // current.caller_id is accessed via script from gs.getUserID();
 var jsonContent = request.getAsJsonContent();
 for (var jsonElementItr = jsonContent.getIterator('variables'); jsonElementItr.hasNext();) {
  var jsonElement = jsonElementItr.next();
  if (jsonElement.getName() == 'error_message')
   jsonElement.valueFor(tableName, 'short_description');
            } else {
         jsonElement.valueFor(tableName, jsonElement.getName());
 }
}
```

Ergebnisse
Die beiden Verschlüsselungsregeln ermöglichen es dem Datensatzersteller, Werte in Felder einzufügen, die entweder vom Servicekatalog oder von Serviceportal zur Verschlüsselung markiert sind.

Eine benutzerdefinierte Verschlüsselungsregel definieren

Es kann notwendig sein, sensible Informationen in HTTP-Anforderungen auf dem Weg zu Ihrer Instanz zu identifizieren und zu verschlüsseln. Sie können Verschlüsselungsregeln schreiben, um Daten in solchen Anforderungen zu identifizieren, zu interpretieren und zu verschlüsseln, und Felder in der Anforderung zu Tabellenfeldnamen in Ihrer Instanz zuordnen.

Was ist eine Verschlüsselungsregel?

Verschlüsselungsregeln sind Skripts, die auf dem Edge Encryption Proxy-Server ausgeführt werden, um Felder in einer Anforderung Feldern in einer Tabelle in Ihrer ServiceNow-Instanz zuzuordnen. Eine Verschlüsselungsregel weist den Edge Encryption Proxy-Server an, wie Daten in benutzerdefinierten Payloads verschlüsselt werden.

Hinweis:
Verschlüsselungsregeln unterstützen nur ECMAScript 3 und niedriger.

Wann werden benutzerdefinierte Regeln verwendet?

Ein Satz von Verschlüsselungsregeln ist im Edge Encryption Plugin enthalten. Diese Regeln behandeln viele Anwendungsfälle der Kernplattform, z. B.:

- Bearbeiten eines Felds aus dem Listenbearbeitungsformular
- Aktualisieren eines Datensatzes aus dem Datensatzformular
- Direkten Webservice verwalten
- Daten aus der REST-Anwendungsprogrammschnittstelle (API) verarbeiten

Anwendungen, die mit Standardformularen und -listen erstellt wurden, sollten ohne benutzerdefinierte Verschlüsselungsregeln funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Skripts entwickeln, die Daten enthalten, die verschlüsselt werden sollen, erstellen Sie Verschlüsselungsregeln, um diese Daten zu finden und den Glide-Tabellenfeldnamen zuzuordnen. Beispiel:

- Geskriptete Prozessoren
- Geskriptete Webservices
- Scripted REST APIs, UIs oder Ajax-Skripts

Format einer Verschlüsselungsregel

Regeln bestehen aus drei Teilen:

- **Bedingung**: Gibt die Art der Anforderung an.
- **Aktion**: Ordnet Felder in der Anforderung Feldern in einer Tabelle zu und verschlüsselt Werte, die Feldern mit definierten Verschlüsselungskonfigurationen zugeordnet sind.
- **Reihenfolge**: Priorität der Regel. Die Regel mit der niedrigsten Priorität mit einer erfüllten Bedingung ist die einzige ausgeführte Regel. Wie Business Rules laufen die Regeln vom niedrigsten zum höchsten.

Mit Ausnahme von Anhanganforderungen werden HTTP-Anforderungen vom Proxy-Server Edge Encryption ausgewertet. Der Edge Encryption -Proxy-Server wertet alle Verschlüsselungsregelbedingungen in der Prioritätsreihenfolge aus, bis entweder alle Bedingungen „falsch“ oder eine Bedingung „wahr“ zurückgibt. Wenn eine Bedingung „true“ zurückgibt, wird die Aktion für die Anforderung ausgeführt und das Ergebnis an die Instanz weitergeleitet. Andere Bedingungen werden nicht bewertet. Daher sollten die Bedingungen für die Verschlüsselungsregeln so genau wie möglich sein. Eine generische Regel kann für eine Anforderung, die von einer anderen Regel verarbeitet werden soll, als „Wahr“ bewertet werden, was dazu führt, dass die Anforderung durch die falsche Aktion verarbeitet wird. Wenn eine generische Bedingung unvermeidbar ist, sollte die Regel mit einem Wert höherer Ordnung markiert werden, damit spezifischere Regeln zuerst ausgewertet werden.

Richtlinien zum Erstellen von Verschlüsselungsregeln

Durch das Erstellen effizienter, optimierter Verschlüsselungsregeln kann die Verarbeitungszeit für die Skriptvalidierung reduziert werden.

Allgemeine Richtlinie: Wenn Regeln lang werden, versuchen Sie, die Anzahl der Blöcke so gering wie möglich zu halten und die Regeln nach Möglichkeit aufzuschlüsseln. Im Idealfall sollten benutzerdefinierte Regeln für bestimmte Anwendungsfälle gelten, anstatt mehrere Fälle zu umfassen, mit den Anweisungen Falls oder „Switch“ im Aktionsskript.

1. Teilen Sie die Regeln, wann immer möglich. Beispiel:
   - Erstellen Sie unterschiedliche Regeln für verschiedene Tabellen und stellen Sie sicher, dass jede Regel nur für die jeweilige Tabelle ausgeführt wird.
   - Erstellen Sie unterschiedliche Regeln für jeden Datensatzersteller, auf den Sie abzielen, oder zumindest für jede Teilmenge von Datensatzerstellern. Anstelle einer Regel, die auf Dutzende von sys_ids abzielt, können Sie mehrere verschiedene Regeln erstellen, die auf kleinere Teilmengen von Datensatzerstellern abzielen, oder sogar eine Regel pro sys_id erstellen.

> **Hinweis:**
> Das Erstellen mehrerer Regeln erfordert mehr Wartung. Der Nachteil ist, dass mehrere, einfachere Regeln effizienter validiert werden können als längere, komplexere Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Minimieren Sie die Anzahl der Blöcke. Da das Verarbeitungsmodul jeden Block während der Auswertung von Skripts durchsucht, führt eine große Anzahl von Blöcken zu Verzögerungen bei der Validierung. Beispiel:
   - Ersetzen Sie alle `Falls`-Blöcke durch ein Array-Lookup, und ersetzen Sie alle Blöcke im Array-Lookup durch nur einen `Falls`-Block.
   - Kombinieren Sie `if` -Blöcke, wann immer es möglich ist, sie zu gruppieren.

Verschlüsselungsregel-APIs

Verschlüsselungsregeln werden in JavaScript geschrieben und verwenden Edge Encryption APIs zum Auffinden und Verschlüsseln sensibler Informationen im Hauptteil einer Anforderung. Die API verwendet ähnliche Ausdrücke wie xPath, um durch JSON- und XML-Inhalte zu navigieren.

Edge Encryption APIs verarbeiten die Anforderung aus dem Stream, während sie in den Ausgabestream geschrieben wird. Durch die Streamanalyse können Verschlüsselungsregeln netzwerkleistungsfähig sein. Das mehrmalige Abrufen und Analysieren von Inhalten aus dem Körper kann jedoch zu unerwarteten Ergebnissen führen. Um dieses potenzielle Problem zu vermeiden, sollten Anforderungen von der Aktion in einem einzigen Schritt verarbeitet werden.

Beim Erstellen von Verschlüsselungsregeln können Sie keine Glide-APIs, Skripteinbindungen, Business Rules oder globale Parameter wie `current`verwenden. Da die Regeln für HTTP-Objekte erstellt werden, ist ein globales Objekt `Anforderung` verfügbar.

Beim Erstellen von Verschlüsselungsregeln können Sie keine APIs aus dem Allow-Listen-Manager oder bereichsbezogene Anwendungen verwenden.

Fehlerbehandlung

Wenn eine Bedingung oder Aktion einer Verschlüsselungsregel eine Ausnahmebedingung auslöst, überprüfen Sie das Proxy-Protokoll auf Informationen zur Problembehandlung.

Die Client-Anforderung überprüfen

Bevor Sie eine benutzerdefinierte Verschlüsselungsregel erstellen, müssen Sie das Format der Client-Anforderung festlegen, die auf dem Edge Encryption Proxy-Server eingegeben wird.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Da Verschlüsselungsregeln Client-Anforderungen durchlaufen und bestimmen, was ggf. verschlüsselt werden muss, müssen Sie den Typ der Anforderung kennen, für die Sie eine Regel erstellen. Das Format der Client-Anforderung bestimmt die Struktur Ihrer Verschlüsselungsregel und die zur Verwendung in der Regel verfügbaren APIs.

Prozedur

1. Überprüfen Sie die Client-Anforderung.

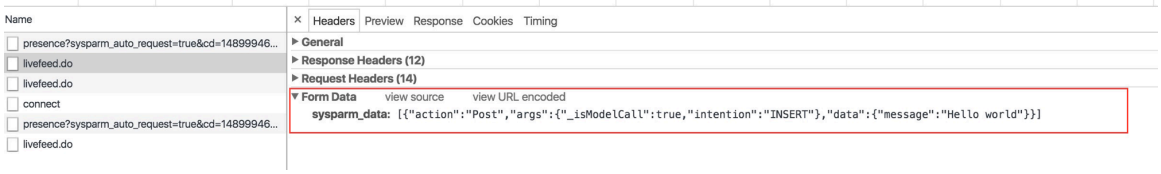
   Abhängig von der Quelle der Anforderung stehen die folgenden Tools zur Verfügung, um die Anforderung zu überprüfen und das Format zu bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelle der Anforderung	Verfügbare Tools
Client-Browser	Verwenden Sie die Entwicklerkonsole in Ihrem Browser, um die Client-Anforderung zu überprüfen. Zu den nützlichen Tools gehören: ○ Firefox Netzwerkmonitor ○ Chrome Netzwerkbereich
Drittanbieter/externe Quelle	Verwenden Sie ein HTTP-Protokollanalysegerät, um die Anforderung zu überprüfen. Zu den nützlichen Tools gehören: ○ Wireshark ○ HTTP Scoop Alternativ können Sie häufig Dokumentation für die externe Quelle verwenden, um das Format der Anforderung zu bestimmen.

2. Überprüfen Sie das Paket in der Client-Anforderung und stellen Sie Folgendes fest:
   - Die Methode der Client-Anforderung
   - Der URL-Pfad der Anforderung
   - Die URL-Parameter
   - Die POST-Parameter, falls vorhanden
   - Das Format des Anforderungstextes, falls vorhanden

Example



Ergebnisse

Durch Überprüfen der Anforderung erhalten Sie Informationen zu den Feldern, die Sie in Ihrer Verschlüsselungsregel filtern und iterieren müssen. Hinweise zum besseren Verständnis der Felder im Objekt *`Anforderung`* finden Sie unter Anforderung.

Eine Verschlüsselungsregel erstellen

Der Proxy verwendet Verschlüsselungsregeln, um Inhalte in HTTP-Anforderungen zu finden, die verschlüsselt werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: security_admin

Bevor Sie eine Verschlüsselungsregel erstellen, müssen Sie Die Client-Anforderung überprüfen, um das Format zu bestimmen.

Warum und wann dieser Vorgang ausgeführt wird

Um Verschlüsselungsregeln erstellen oder bearbeiten zu können, müssen Sie über einen Verschlüsselungs-Proxy mit der Instanz verbunden sein.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Regeln** > **Neu erstellen**.
2. Geben Sie im Feld **Name** einen Namen ein.
3. Wählen Sie unter **Anfragetyp** eine HTTP-Methode aus.
   - **HTTP Post**
   - **HTTP Get**
   - **HTTP Put**
   - **HTTP Patch**
   - **HTTP Delete**

   Hinweis:
   Instanzen vorJakarta erlauben nur **HTTP-Methoden „Get** “ und „ **HTTP Post** “.
4. Geben Sie im Feld **Bedingung** eine JavaScript-Anweisung ein, die festlegt, wann die Regel ausgeführt werden soll.
5. Geben Sie im Feld **Aktion** eine JavaScript-Funktion ein, die ausgeführt werden soll, wenn die Bedingung erfüllt ist.
6. Geben Sie im Feld **Auftrag** die relative Priorität der Regel ein.
7. Klicken Sie auf **Absenden** oder speichern Sie das Formular.

Bedingungen für Verschlüsselungsregeln

Die Bedingungen für die Verschlüsselungsregeln bestimmen, ob die Regel ausgeführt werden soll.

Eine Bedingung für eine Verschlüsselungsregel muss „Wahr“ zurückgeben, wenn die Regel die HTTP-Anfrage behandeln soll; andernfalls muss sie „Falsch“ zurückgeben.

Beachten Sie beim Erstellen Ihrer Bedingung, dass pro Anforderung nur eine Regel ausgeführt wird. Daher muss die Bedingung so allgemein oder spezifisch sein, dass sie unter den vorgesehenen Umständen ausgeführt werden kann.

Hinweis:
Seien Sie vorsichtig, wenn Sie Überprüfungen des Inhalts in der Bedingung durchführen. Übermäßige Überprüfungen können für den Proxy-Server teuer sein und zu einer erhöhten Latenzzeit bei der Bearbeitung komplexer Anfragen führen.

Die Bedingung kann den Methodentyp, den Inhaltstyp, den URL-Pfad oder beliebige URL-Abfragezeichenfolgeparameter verwenden, um zu bestimmen, ob die Regel die Anforderung verarbeiten soll. Die Bedingung hat auf diese Felder über das Objekt Anforderung Zugriff. Stellen Sie sicher, dass Sie vor dem Erstellen einer Verschlüsselungsregel die Client-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderung überprüft haben und die für das Auslösen der Regel erforderlichen Bedingungen kennen.

Hinweis:
Um effiziente Regeln zu erstellen, sollten Sie einfache Möglichkeiten berücksichtigen, Anforderungen auszuschließen, die nicht von einer Regel ausgewertet werden sollen. Erstellen Sie Ihre Bedingung, um zuerst für diese Anforderungen „Falsch“ zurückzugeben. Diese Methode erhöht die Leistung und leitet die Anforderung schneller an die richtige Regel weiter.

Verschlüsselungsregelobjekte und APIs sind für Verschlüsselungsregelbedingungen verfügbar.

Beispiel mit Pfad und Postparametern

```
/*This condition checks if the request coming in has a path ending in
"/sample_processor.do" and if a post parameter exists in that request called myPostParam */

function SampleCondition(request) {
  if (endsWith(request.path, "/sample_processor.do") && request.postParams.myPostParam) {
     return true;
  }
  return false;
}
```

Beispiel mit urlParams und contentType

```
/* This condition checks if a url parameter exists in the query called
myUrlParam and if the content type contains 'xml'
(if so, you can expect the body to be an XML payload).
Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
  if (request.urlParams.myUrlParam && request.contentType.indexOf('xml') > -1 &&
 request.xmlContains('myXmlTag')) {
     return true;
  }
 return false;
}
```

Aktionen für Verschlüsselungsregeln

Eine Verschlüsselungsregel ordnet Felder in einer Client-Anforderung Feldern in einer Tabelle in Ihrer Instanz zu und identifiziert Felder, die für die Verschlüsselung markiert sind.

Eine Verschlüsselungsregelaktion wird nur ausgeführt, wenn die Bedingung der Verschlüsselungsregel „Wahr“ zurückgibt. Eine Verschlüsselungsregel gibt die Daten an, die in Ihrer Anforderungs-Payload verschlüsselt werden sollen. Da die Regel den Inhalt im Anforderungsobjekt durchläuft, müssen Sie die Form und Struktur Ihres Anforderungstexts verstehen und bestimmen, was in der Anforderung verschlüsselt werden muss. Die zu verschlüsselnden Daten befinden sich möglicherweise in:

- einem POST- oder URL-Parameter,
- einem JSON- oder XML-Inhalt in einem POST- oder URL-Parameter,
- einer JSON-Payload,
- einer XML-Payload.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie vor dem Schreiben einer Verschlüsselungsregelaktion Folgendes sicher:

- Die Client-Anforderung überprüfen.
- Stellen Sie fest, wo sich die sensiblen Daten im Objekt Anforderung befinden.
- Bestimmen Sie das Feld und den Tabellennamen, in das Daten eingefügt werden sollen, oder verstehen Sie, wie man dies dynamisch aus der Anforderung entnimmt.

Verschlüsselungsregelobjekte und APIs stehen für Verschlüsselungsregelaktionen und -bedingungen zur Verfügung.

Verschlüsselungsregelobjekte und APIs

Verwenden Sie Verschlüsselungsregel-APIs, um Werte in Anforderungen zu analysieren und zu verschlüsseln, die sich durch den Edge Encryption Proxy-Server zur Instanz bewegen.

Die für Ihre Verschlüsselungsregel verfügbaren APIs hängen vom Format des Anforderungsobjekts ab. Wenn der contentType-Parameter des Anforderungsobjekts beispielsweise XML ist, können Sie XML-APIs verwenden, um Werte in der Payload zu analysieren und zu verschlüsseln. Nachdem Sie den Objekttyp in Ihrer Anforderung ermittelt haben, können Sie eine Verschlüsselungsregel mit den verfügbaren APIs erstellen.

Verschlüsselungsregel-APIs sind sowohl in den Bedingungen für Verschlüsselungsregeln als auch in Aktionsskripts verfügbar.

Anforderung

Das Objekt `Anforderung` ist ein globales Objekt, das in Edge Encryption Regelaktionen und Bedingungsskripts verfügbar ist.

Das Objekt `Anforderung` ist ein JavaScript-Objekt, das die Client-Anforderung darstellt, die an den Edge Encryption Proxy-Server gesendet wird. Sie müssen Ihre Verschlüsselungsregel erstellen, um das Objekt `Anforderung` zu analysieren, die Objektwerte `Anforderung` Feldern in einer Tabelle in der Instanz zuordnen und alle sensiblen Daten im Objekt `Anforderung` verschlüsseln.

Das Objekt `Anforderung` enthält die folgenden Attribute und Daten aus der Client-Anforderung:

Anforderungsobjektfelder

Feld	Beschreibung
Pfad	Der Pfadbestandteil der URL.
requestMethod	GET, POST, PUT, PATCH, DELETE.
contentType	Das Kopfzeilenfeld „Content-Type“.
urlParams	Die Parameter in der Abfragezeichenfolge. Dies kann auch als String ausgewertet werden.
postParams	Wenn es sich um einen Formular-Post handelt, enthält dieser die Post-Parameter.

Anforderung – getAsJsonContent()

Gibt die Anforderung als iterierbares Objekt vom Typ `JsonNode` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige JSON-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald die Anforderung als `JsonNode`-Objekt zurückgegeben wird, können Sie mit Hilfe von JSON-APIs über das Objekt iterieren und Felder verschlüsseln.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Die Anforderung als iterierbarer `JsonNode`.

Anforderung – getAsXmlContent()

Gibt den Anforderungsinhalt als iterierbares Objekt vom Typ `XMLContent` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige XML-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

Sobald die Anfrage als `XMLContent`-Objekt zurückgegeben wird, können Sie mit Hilfe von XML-APIs über die Objekt- und Verschlüsselungsfelder iterieren.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLContent	Die Anforderung als iterierbares Objekt vom Typ `XMLContent`.

Anforderung – XMLContains (Zeichenfolgenpfad)

Gibt „Wahr“ zurück, wenn der angegebene Pfad im XML DOM vorhanden ist.

Diese Methode ist nur verfügbar, wenn der Anforderungstext eine gültige XML-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

Parameter

Name	Typ	Beschreibung
Pfad	Zeichenfolge	XPath-Anweisung, nach der Sie suchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
Boolean	Gibt an, ob der angegebene Pfad im XML DOM vorhanden ist.

POST- und URL-Parameter-APIs

POST- und URL-Parameter können als Eigenschaften des Objekts *Anforderung* über request.postParams und request.urlParams aufgerufen werden.

Auf jeden einzelnen Parameter kann als Eigenschaft der übergeordneten Objekte *postParams* und *urlParams* durch Aufrufen von request.postParams.myParam zugegriffen werden. Jeder Parameter, auf den auf diese Weise zugegriffen wird, ist ein Objekt der zugrunde liegenden Klasse *ParameterValue*. Alle APIs in dieser Klasse können für jeden Parameter aufgerufen werden.

Nach dem Überprüfen der Client-Anforderung kann es notwendig sein, auf Parameterwerte aus dem Objekt *Anforderung* zuzugreifen und diese zu verschlüsseln. Abhängig von den Daten in der Clientanforderung können Sie Werte auf mehrere Arten verschlüsseln und sie Feldern in der Instanz zuordnen.

Den Wert einer bekannten Tabelle und eines Felds verschlüsseln

Wenn Sie den Namen der Instanztabelle und des Felds kennen, in dem die verschlüsselten Daten gespeichert werden sollen, können Sie sie explizit in der Verschlüsselungsregel definieren. Möglicherweise wissen Sie beispielsweise, dass die Anforderung in der Instanz verarbeitet wird, um einen Incident zu erstellen, und Sie möchten den Parameter **Text** im Beschreibungsfeld verschlüsseln. In diesem Fall können Sie die folgende Aktion erstellen.

```
function SampleAction1() {
   request.postParams.text.valueFor('incident', 'description');
}
```

Den Wert einer dynamisch definierten Tabelle und eines Felds verschlüsseln

Wenn Sie andererseits den Namen des Feldes nicht kennen, das die verschlüsselten Daten füllen sollen, können Sie sie mit **tableName** und **fieldName** dynamisch definieren.

Im folgenden Beispiel wird eine generische Anforderung verarbeitet, in der möglicherweise Daten in verschiedenen Aufgabentabellen (z. B. Incident, Problem und Change_request) in der Instanz gespeichert werden.

```
function SampleAction2() {
   var tableName = request.urlParams.table;
   for (var parameter in request.postParams) {
      var currentParam = request.postParams[parameter];
      var fieldName = currentParam.toString();
      if (fieldName == 'text') {
         currentParam.valueFor(tableName, 'description')
      } else {
         currentParam.valueFor(tableName, fieldName);
      }
   }
}
```

Diese Aktion:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ruft die Zieltabelle aus den URL-Parametern ab.
- Iteriert über die URL-Parameter.
- Fordert den Edge Encryption Proxy-Server auf, jeden URL-Parameter mit einem Namen zu verschlüsseln, der einem für die Verschlüsselung markierten Feld entspricht.
- Sucht nach einem bestimmten Parameter namens *Text* und fordert den Edge Encryption Proxy auf, den Wert basierend auf der Verschlüsselungskonfiguration für das Beschreibungsfeld in der Incident-Tabelle zu verschlüsseln.

In diesem Beispiel führt die Methode valueFor() eigentlich keine Verschlüsselung durch. Vielmehr fordert das Verfahren den Edge Encryption Proxy-Server auf, zu prüfen, ob das Tabellen-/Feldpaar im Anforderungsobjekt mit einer Verschlüsselungskonfiguration zur Verschlüsselung vorgemerkt ist, und gegebenenfalls zu verschlüsseln.

JSON oder XML innerhalb eines Parameters verschlüsseln

Ein POST- oder URL-Parameter kann JSON- oder XML-Inhalte enthalten. In diesem Fall können Sie den Inhalt innerhalb des Parameters verarbeiten, die Werte durchlaufen und die erforderlichen Felder verschlüsseln. In diesem Beispiel wird weiterhin über einen POST-Parameter auf **tableName** zugegriffen, aber der Wert des Feldes ist das JSON-Objekt **Daten**.

```
function SampleAction3() {
   var tableName = request.postParams.table;
   var data = request.postParams.data;
   var dataIterator = data.getAsJsonContent().iterator();
   while (dataIterator.hasNext()) {
      var jsonElement = dataIterator.next();
      var fieldName = jsonElement.getName();
      if (fieldName == 'text') {
         jsonElement.valueFor(tableName, 'description');
      } else {
         jsonElement.valueFor(tableName, fieldName);
      }
   }
}
```

Ein Beispiel für eine Verschlüsselungsregelaktion, die XML innerhalb eines POST-Parameters verarbeitet.

```
function SampleAction4() {
   var tableName = request.postParams.table;
   var data = request.postParams.data;
   var dataIterator = data.getAsXmlContent().getIteratorOverAllChildren();
   while (dataIterator.hasNext()) {
      var jsonElement = dataIterator.next();
      var fieldName = jsonElement.getName();
      if (fieldName == 'text') {
         jsonElement.valueFor(tableName, 'description');
      } else {
         jsonElement.valueFor(tableName, fieldName);
      }
   }
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Anforderung verschlüsseln

In einer Client-Anforderung, die vertrauliche Daten enthält, tritt möglicherweise eine verschlüsselte Abfrage in einem Parameter auf. Um ein Feld in einer Abfrage einem verschlüsselten Wert in der Instanzdatenbank zuzuordnen, müssen Sie eine Verschlüsselungsregel erstellen, die den Proxy-Server auffordert, zu prüfen, ob ein Feld in der Abfrage für die Verschlüsselung markiert ist. Die Methode encodedQueryFor() analysiert eine verschlüsselte Abfrage für eine bestimmte Tabelle und prüft, ob Felder in der Abfrage Verschlüsselungskonfigurationen enthalten.

In diesem Beispiel durchläuft die Regel die Parameter und sucht den Parameter **Filter**, der voraussichtlich eine Glide-codierte Abfrage ist.

```
function SampleAction5() {
   var tableName = request.urlParams.table;
   for (var parameter in request.postParams) {
      var currentParam = request.postParams[parameter];
      var fieldName = currentParam.toString();
      if (fieldName == 'filter') {
         currentParam.encodedQueryFor(tableName);
      } else {
         currentParam.valueFor(tableName, fieldName);
      }
   }
}
```

Wenn beispielsweise der Wert von **Filter** `short_description=My sensitive information^number=INC000056^category=Outage` ist, würde die Abfrage in der Instanz zu `short_description=<Encrypted(My sensitive information)>^number=INC000056^category=Outage` werden.

ParameterValue - toString()

Konvertiert den POST- oder URL-Parameterwert in eine Zeichenfolge.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Parameterwert als Zeichenfolge.

ParameterValue - getAsJsonContent()

Gibt die Anforderung als iterierbares Objekt vom Typ *`JsonNode`* zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige JSON-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt *`Anforderung`*.

Sobald die Anforderung als *`JsonNode`*-Objekt zurückgegeben wird, können Sie mit Hilfe von JSON-APIs über das Objekt iterieren und Felder verschlüsseln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Die Anforderung als iterierbarer `JsonNode`.

ParameterValue - getAsXmlContent()

Gibt den Anforderungsinhalt als iterierbares Objekt vom Typ `XMLContent` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar Diese Methode setzt voraus, dass der Anforderungstext eine gültige XML-Payload ist. Sie können den contentType überprüfen, um sicherzustellen, dass dies der Fall ist.

Sobald die Anfrage als `XMLContent`-Objekt zurückgegeben wird, können Sie mit Hilfe von XML-APIs über die Objekt- und Verschlüsselungsfelder iterieren.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLContent	Die Anforderung als iterierbares Objekt vom Typ `XMLContent`.

ParameterValue - encodedQueryFor(String tableName)

Gibt an, dass der Wert des Elements eine codierte Abfrage für die angegebene Tabelle ist.

Durch Aufrufen dieser Funktion für einen Parameter wird dem Proxy mitgeteilt, dass der Wert des Parameters eine codierte Abfragezeichenfolge für die angegebene Tabelle ist. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

Ergebnisse

Typ	Beschreibung
void	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ParameterValue - valueFor(String tableName, String fieldName)

Gibt an, dass der Wert des Elements dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für einen Elementwert wird dem Proxy mitgeteilt, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

XML-APIs

XML-APIs können nach dem Aufrufen von `getAsXmlContent()` entweder über das Objekt `Anforderung` oder eine Eigenschaft `ParameterValue` verwendet werden.

Wenn Sie XML-APIs zum Schreiben Ihrer Verschlüsselungsregel verwenden, können Sie ein allgemeines Format verwenden:

1. Aufrufen von `getAsXmlContent()` über das Objekt `Anforderung` oder die Eigenschaft `ParameterValue`. Dies gibt ein iterierbares Objekt der zugrunde liegenden Klasse `XMLContent` zurück.
2. Aufrufen von `getIterator()` oder `getIterator(String xPath)` im Objekt `XMLContent`. Dies gibt ein Objekt `XMLElementIterator` zurück, das zum Iterieren von XML-Elementen verwendet werden kann.
3. Aufrufen der Methode `hasNext()` im Objekt `XMLElementIterator`, um zu bestimmen, ob ein anderes Element verfügbar ist.
4. Aufrufen von `next()` im Objekt `XMLElementIterator`, um das nächste XML-Element zurückzugeben. Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.
5. Aufruf von `valueFor(String tableName, String fieldName)` auf dem XML-Element. Diese Methode teilt dem Proxy mit, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

> **Hinweis:**
> Um festzustellen, ob Sie `valueFor(String tableName, String fieldName)` auf einem XML-Element aufrufen möchten, können Sie die Methode `getName()` verwenden, um den Namen des Elements zurückzugeben.

Zu einem bekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die XML-Payload auf der Instanz verarbeitet, um Datensätze in die Incident-Tabelle einzufügen. Das Beschreibungsfeld füllt den Incident mit short_description aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<data>
   <record>
      <name>'Test Record 1'</name>
      <description>'Test Record 1 Description'</description>
      <tag>critical</tag>
   </record>
   <record>
      <name>'Test Record 2'</name>
      <description>'Test Record 2 Description'</description>
      <tag>security</tag>
   </record>
</data>
```

Die folgende Verschlüsselungsregelaktion kann angewendet werden:

```
function sampleXmlAction1() {
   var xmlContent = request.getAsXmlContent();
   // This loop iterates over all description tags that match the given path
   var xmlElementIterator = xmlContent.getIterator('data/record/description');
   while (xmlElementIterator.hasNext()) {
      var xmlElement = xmlElementIterator.next();
      xmlElement.valueFor('incident', 'short_decription');
   }
}
```

Diese Aktion iteriert das Tag **Beschreibung** und fordert den Proxy-Server auf, die Werte zu verschlüsseln und sie in der Instanz in instance.short_description einzufügen.

Hinweis:
Diese Regel findet alle Tags **Beschreibung** in allen Tags **Datensatz** in der XML-Payload. Wenn es nur ein einziges Vorkommen eines zu verschlüsselnden Tags gibt, verwendet die Regel weiterhin die xPath- und Iteratorstruktur. Es iteriert jedoch nur einmal in der Schleife.

Zu einem unbekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel iteriert die Regel die Tags **Datensatz**, weiß jedoch nicht, welche Tags innerhalb des Tags **Datensatz** zu erwarten sind. Es ist nur bekannt, dass die Tags innerhalb der Tags **Datensatz** mit den Namen der in der Tabelle „URL-Parameter“ angegebenen Spalten übereinstimmen.

Die Regel legt außerdem fest, dass bei Vorliegen einer Incident-Tabelle, die Daten im Tag **Beschreibung** verschlüsselt und im Feld short_description der Instanz gespeichert werden sollen.

```
function sampleXmlAction2() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
      encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //Then, iterate over all tags representing fields in the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
   while (fieldIterator.hasNext()) {
      var field = fieldIterator.next();
      var fieldName = childElement.getName();
      //if table is incident, then description is encrypted for the short_description field
      if (tableName == 'incident' && fieldName == 'description') {
         field.valueFor(tableName, 'short_description');
      } else {
         //if table is not incident, ask the proxy to check if the given field is encrypted for the
 given table
         field.valueFor(tableName, fieldName);
      }
   }
}
```

In der Funktion *`encryptFieldsInRecord()`* wird die Methode *`valueFor()`* für eine Tabelle und ein Feld aufgerufen, die aufgrund der Anforderung dynamisch zugewiesen werden. Obwohl sich die Tabellen- und Feldnamen ändern können, fordert die Regel den Proxy auf, zu prüfen, ob das Feld in der Tabelle aufgrund der definierten Verschlüsselungskonfigurationen verschlüsselt werden muss.

Wenn das Feld nicht für die Verschlüsselung konfiguriert ist oder das Tag nicht mit einem Feld in der Tabelle übereinstimmt, überspringt der Proxy dieses Tag. Wenn das Tag mit einem für die Verschlüsselung markierten Feld übereinstimmt, verschlüsselt der Edge Encryption Proxy-Server den Wert.

Eine verschlüsselte Abfrage verwenden

In diesem Beispiel haben alle Tags das Attribut **Filter**, das angibt, ob das Tag eine verschlüsselte Abfrage enthält.

```
<data>
   <record>
      <name filter="false">'Test Record 1'</name>
      <description filter="false">'Test Record 1 Description'</description>
      <query filter="true">category=1^name=edge</query>
   </record>
   <record>
      <name filter="false">'Test Record 2'</name>
      <description filter="false">'Test Record 2 Description'</description>
      <query filter="true">category=2^severity=3</query>
  </record>
</data>
```

Die folgende Verschlüsselungsregelaktion kann angewendet werden:

```
function sampleXmlAction3() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
      encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //this time we want to iterate over all tags representing fields in the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  while (fieldIterator.hasNext()) {
     var field = fieldIterator.next();
     var fieldname = childElement.getName();
     //let's look at the filter attribute, if true, then encrypt as encoded query
     if (field.getAttributeValue('filter') == 'true') {
        field.encodedQueryFor(tableName);
     } else {
        //if it is false then check if the field should be encrypted
        field.valueFor(tableName, fieldName);
     }
  }
}
```

Wenn das Attribut **Filter** „Wahr“ ist, fordert die Regel den Proxy-Server auf, die Werte in der verschlüsselten Abfrage zu verschlüsseln. Bei „falsch“ fordert die Regel den Proxy auf, zu prüfen, ob das Feld verschlüsselt werden soll.

XMLContent

Ein globales Objekt, das Methoden zum Iterieren des XML-Inhalts bereitstellt.

Sie können auf ein Objekt `XMLContent` zugreifen, indem Sie getAsXmlContent() auf einem Objekt `Anforderung` aufrufen.

Sie greifen auf XML-Daten in einem POST- oder URL-Parameter zu, indem Sie request.postParams.<parameter name>.getAsXmlContent() oder request.urlParams.<parameter name>.getAsXmlContent() aufrufen.

XMLContent - getIterator()

Gibt ein Objekt `XMLElementIterator` für den XML-Inhalt zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, das zum Iterieren von Elementen im Objekt `XMLContent` verwendet werden kann.

XMLContent - getIterator(String xPath)

Gibt ein Objekt `XMLElementIterator` für den XML-Inhalt basierend auf dem angegebenen Parameter zurück.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-ähnlicher Ausdruck, der angibt, wo im Objekt `XMLContent` begonnen werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, das zum Iterieren von Elementen im Objekt `XMLContent` verwendet werden kann.

XMLElementIterator

Stellt Methoden zum Iterieren von XML-Elementen bereit.

Sie erhalten ein Objekt `XMLElementIterator`, indem Sie die Methode `getIterator()` in der Klasse `XMLContent` aufrufen.

XMLElementIterator - hasNext()

Bestimmt, ob ein anderes Element verfügbar ist.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Boolean	„Wahr“, wenn ein anderes Element verfügbar ist.

XMLElementIterator - next()

Gibt das nächste Element im Iterator zurück.

Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElement	Das nächste XML-Element.

XMLElement

Stellt Methoden zum Iterieren von XML-Elementen und zum Zuordnen von Werten zu Feldern in einer Tabelle bereit.

Sie erhalten ein Objekt `XMLElement`, indem Sie die Methode `next()` eines Objekts `XMLElementIterator` aufrufen.

XMLElement - getIterator(String xPath)

Gibt ein Objekt `XMLElementIterator` für das XML-Element basierend auf dem angegebenen Parameter zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-ähnlicher Ausdruck, der angibt, wo im Objekt `XMLElement` begonnen werden soll.

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, mit dem über Elemente im Objekt `XMLElement` iteriert werden kann.

XMLElement - getIteratorOverAllChildren()

Gibt ein Objekt `XMLElementIterator` zurück, das alle Unterelemente des XML-Elements basierend auf dem angegebenen Parameter enthält.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, mit dem über Elemente im Objekt `XMLElement` iteriert werden kann.

XMLElement - valueFor(String tableName, String fieldName)

Gibt an, dass der Wert des Elements dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für einen Elementwert wird dem Proxy mitgeteilt, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss. Wenn die Tabellen- und Feldnamen unbekannt sind, können Sie die Methode `valueFor()` auf einer Tabelle und einem Feld mit der Bezeichnung Dynamisch zugeordnet basierend auf der Anfrage aufrufen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

XMLElement - encodedQueryFor(String tableName)

Gibt an, dass der Wert des Elements eine codierte Abfrage für die angegebene Tabelle ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch Aufrufen dieser Funktion für ein Element wird dem Proxy mitgeteilt, dass der Wert des Elements eine codierte Abfragezeichenfolge für die angegebene Tabelle ist. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

Ergebnisse

Typ	Beschreibung
void	

XMLElement - getName()

Gibt den Elementnamen zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Elementname.

XMLElement - getAttributeValue(String attribute)

Gibt den Wert des angegebenen Attributs zurück.

Parameter

Name	Typ	Beschreibung
Attribut	Zeichenfolge	Der Attributname.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Attributwert.

JSON-APIs

JSON-APIs können nach dem Aufrufen von `getAsJsonContent()` entweder über das Objekt `Anforderung` oder eine Eigenschaft `ParameterValue` verwendet werden.

Wenn Sie JSON-APIs zum Schreiben Ihrer Verschlüsselungsregel verwenden, können Sie ein allgemeines Format verwenden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aufrufen von `getAsJsonContent()` im Objekt `Anforderung`. Dies gibt ein iterierbares Objekt der zugrunde liegende Klasse `JsonNode` zurück.
2. Rufen Sie iterator `()` oder `getIterator(String xPath)` für das `JsonNode-` Objekt auf. Dies gibt ein Objekt `JsonNodeIterator` zurück, das zum Iterieren von Knoten im JSON-Objekt verwendet werden kann.
3. Aufrufen der Methode `hasNext()` im Objekt `JsonNodeIterator`, um zu bestimmen, ob ein anderes Element verfügbar ist.
4. Aufrufen von `next()` im Objekt `JsonNodeIterator`, um das nächste JSON-Element zurückzugeben. Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.
5. Aufrufen von `valueFor(String tableName, String Feldname)` auf dem JSON-Element. Diese Methode teilt dem Proxy mit, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

Hinweis:
Um festzustellen, ob Sie `valueFor(String tableName, String fieldName)` auf einem JSON-Element aufrufen möchten, können Sie die Methode `getName()` verwenden, um den Namen des Elements zurückzugeben.

Zu einem bekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die JSON-Payload auf der Instanz verarbeitet, um Datensätze in die Incident-Tabelle einzufügen. Das Beschreibungsfeld füllt den Incident mit short_description aus.

```
{
   data: {
      records: [
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         },
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         }],
      "query": "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
   },
   "source": "10.11.13.14"
}
```

Die folgende Regel kann gelten:

```
function sampleJsonAction1() {
   var jsonContent = request.getAsJsonContent();
   // This loop iterates over all description elements in the records array
   var jsonNodeIterator = jsonContent.getIterator('/data/records/description');
   while (jsonNodeIterator.hasNext()) {
      var jsonNode = jsonNodeIterator.next();
      jsonNode.valueFor('incident', 'short_decription');
   }
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Aktion iteriert die Knoten **Beschreibung** und fordert den Proxy-Server auf, die Werte zu verschlüsseln und sie in instance.short_description auf der Instanz einzufügen.

Hinweis:
Diese Regel findet alle Knoten **Beschreibung** innerhalb der JSON-Payload. Wenn nur ein Knoten zu verschlüsseln ist, verwendet die Regel weiterhin die xPath- und Iterator-Struktur. Es iteriert jedoch nur einmal in der Schleife.

Zu einem unbekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die Regel **Datensätze** iteriert. Es ist jedoch nicht bekannt, welche Knoten zu erwarten sind. Es ist nur bekannt, dass für jedes Objekt innerhalb von **Datensätze** die Knoten mit den Namen der im URL-Parameter der Tabelle angegebenen Spalten übereinstimmen.

Die Regel legt außerdem fest, dass bei Vorliegen einer Incident-Tabelle, die Daten im Knoten **Beschreibung** verschlüsselt und im Feld short_description der Instanz gespeichert werden sollen.

```
function sampleJsonAction2() {
   var jsonContent = request.getAsJsonContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var jsonNodeIterator = jsonContent.getIterator('data/records');
   while (jsonNodeIterator.hasNext()) {
         encryptFieldsInRecord(jsonNodeIterator.next());
   }
}
function encryptFieldsInRecord(jsonNode) {
   //this time we want to iterate over all nodes
   var fieldIterator = jsonNode.iterator();
   while (fieldIterator.hasNext()) {
         var field = fieldIterator.next();
         var fieldname = childElement.getName();
         if (fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
         } else {
            field.valueFor(tableName, fieldName);
         }
   }
}
```

In der Funktion *`encryptFieldsInRecord()`* wird die Methode *`valueFor()`* für eine Tabelle und ein Feld aufgerufen, die aufgrund der Anforderung dynamisch zugewiesen werden. Obwohl sich die Tabellen- und Feldnamen ändern können, fordert die Regel den Proxy auf, zu prüfen, ob das Feld in der Tabelle aufgrund der definierten Verschlüsselungskonfigurationen verschlüsselt werden muss.

Wenn das Feld nicht für die Verschlüsselung konfiguriert ist oder der Knotenname nicht mit einem Feld in der Tabelle übereinstimmt, überspringt der Proxy diesen Knoten. Wenn der Knotenname mit einem für die Verschlüsselung markierten Feld übereinstimmt, verschlüsselt der Proxy den Wert.

Eine verschlüsselte Abfrage verwenden

```
function sampleJsonAction3() {
   var jsonContent = request.getAsJsonContent();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecors(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    //we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            field.valueFor(tableName, fieldName);
    }
}
```

In diesem Beispiel wird die Regel **Daten** iteriert. Mit Auffinden von **Datensätzen** wird die gleiche Logik wie im zweiten Beispiel ausgeführt, wobei die Felder in jedem Knoten iteriert werden. Nach Auffinden des Knotens **Abfrage** wird `encodedQueryFor()` aufgerufen, um Werte verschlüsseln, die in der Abfrage verschlüsselt werden sollen.

JsonNode

Ein globales Objekt, das Methoden zum Durchlaufen des JSON-Inhalts bereitstellt.

Sie können auf ein Objekt `JsonNode` zugreifen, indem Sie getAsJsonContent() in einem Objekt `Anforderung` aufrufen.

Sie haben Zugriff auf JSON-Inhalte von einem POST- oder URL-Parameter, indem Sie request.postParms.<parameter name>.getAsJsonContent() oder request.urlParms.<parameter name>.getAsJsonContent() aufrufen.

JsonNode - getIterator(String xPath)

Gibt ein Objekt `JsonNodeIterator` für den JSON-Inhalt zurück.

Diese Methode kann nur für den Stammknoten verwendet werden, kann jedoch auch verwendet werden, um tief in das JSON-Objekt zu gelangen. Nachfolgende Traversen müssen die Methode `Iterator()` verwenden.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-Ausdruck.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
JsonNodeIterator	Ein Objekt, das Knoten im JSON-Objekt iterieren kann.

JsonNode - iterator()

Gibt ein Objekt `JsonNodeIterator` zurück, das alle untergeordneten Knoten des aktuellen Knotens iteriert.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNodeIterator	Ein Objekt, das Knoten im JSON-Objekt iterieren kann.

JsonNode - getAsString()

Gibt den aktuellen Knotenwert als Zeichenfolge zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der aktuelle Knotenwert.

JsonNode - getAsString(String propertyName)

Gibt den Zeichenfolgenwert der angegebenen Eigenschaft zurück.

Parameter

Name	Typ	Beschreibung
propertyName	Zeichenfolge	Der Name der Eigenschaft.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Eigenschaftswert.

JsonNode - getName()

Gibt den Namen des aktuellen JSON-Knotens zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Name des aktuellen JSON-Knotens.

JsonNode - valueFor(String tableName, String fieldName)

Gibt an, dass die JSON-Eigenschaft dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für eine JSON-Eigenschaft wird dem Proxy mitgeteilt, dass der Wert für diese Eigenschaft dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy entscheidet dann, ob das Feld verschlüsselt werden muss. Wenn die Tabellen- und Feldnamen unbekannt sind, können Sie die Methode `valueFor()` auf einer Tabelle und einem Feld mit der Bezeichnung Dynamisch zugeordnet basierend auf der Anfrage aufrufen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

JsonNode - encodedQueryFor(String tableName)

Gibt an, dass der Wert der JSON-Eigenschaft eine codierte Abfrage für die angegebene Tabelle ist.

Durch Aufrufen dieser Funktion auf einem JSON-Knoten wird dem Proxy mitgeteilt, dass der Wert eine codierte Abfragezeichenfolge für die angegebene Tabelle ist. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Werte für Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
void	

JsonNodeIterator

Sie erhalten ein Objekt `JsonNodeIterator`, indem Sie die Methoden `getIterator()` oder `iterator()` der Klasse `JsonNode` aufrufen.

JsonNodeIterator - hasNext()

Bestimmt, ob eine andere Eigenschaft verfügbar ist.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Boolean	„Wahr“, wenn eine andere Eigenschaft verfügbar ist.

JsonNodeIterator - next()

Gibt die nächste Eigenschaft im Iterator zurück.

Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Der nächste `JsonNode`.

print(String message)

Gibt eine Nachricht an die Wrapper-Protokolldatei aus: <proxy server directory>/logs/wrapper_<date>.log.

Diese Methode ist nur in einem Edge Encryption-Regelaktionsskript verfügbar

Parameter

Name	Typ	Beschreibung
Nachricht	Zeichenfolge	Die Nachricht, die in die Wrapper-Protokolldatei geschrieben werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
void	

Nicht zulässige Schlüsselwörter

Der Edge Encryption Proxy überprüft Verschlüsselungsregelskripts, bevor die Regel gespeichert wird. Viele JavaScript-Stichwörter sind in Skripts für Verschlüsselungsregeln nicht zulässig.

Nicht zulässige Schlüsselwörter

Stichwort
__DIR__
__FILE__
__LINE__
__parent__
__proto__
Fehler
Ausw
getClass
getPrototypeOf
Java
javax
javafx
JavaImporter
laden
loadWithNewGlobal
neu
Pakete
Objekt
Prototyp
RegExp
setPrototypeOf
diese
werfen

Attribute für das Edge-Encryption-Dictionary

Fügen Sie Wörterbuchattribute zu Tabellen und Feldern hinzu, um zu steuern, wie sie mit Edge Encryption funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um ein Wörterbuchattribut auf „true“ zu setzen, müssen Sie `attribute=true` in das Feld **Attribute** eingeben. Informationen zum Hinzufügen eines Wörterbuchattributs zu einem Datensatz finden Sie unter Wörterbuchattribute .

Edge Encryption ausgeschlossen [edge_encryption_excluded]

Bestimmt, ob das Feld von der Verschlüsselung ausgeschlossen wird.

Bei Festlegung auf `true`kann das Feld oder die Tabelle nicht verschlüsselt werden. Bei `false`kann das Feld verschlüsselt werden.

- Wert: true/false
- Zielelement: Feld oder Tabelle
- Standardwert: false

Edge Encryption aktiviert [edge_encryption_enabled]

Bestimmt, ob das Feld für die Verschlüsselung durch eine Verschlüsselungskonfiguration geeignet ist.

Bei Festlegung auf `true`ist das Feld für die Verschlüsselung geeignet. Bei „ `false`“ist das Feld nicht für die Verschlüsselung geeignet. Da dieses Attribut vom System verwendet wird und nicht geändert werden kann, wird es dem Benutzer nicht angezeigt.

Hinweis:
Dieses Attribut gibt nicht an, dass ein Feld verschlüsselt ist, und löst keine Verschlüsselungslogik für das Feld aus. Das Attribut bestimmt vielmehr die Möglichkeit, dass das Feld von einem Benutzer verschlüsselt wird.

- Wert: true/false
- Zielelement: Feld
- Standardwert: true für Zeichenfolgenfelder

Klartext für die Edge Encryption zulässig [edge_encryption_clear_text_allowed]

Legt fest, ob serverseitige Skripts unverschlüsselte Daten an eine verschlüsselte Zeichenfolge innerhalb des Felds für Benutzeraktionen anhängen dürfen, die über den Proxy-Server ausgeführt werden, oder an serverseitige automatisierte Skripts, z. B. geplante Aufgaben.

Bei Festlegung auf `true`ist das Anfügen von Daten zulässig. Bei „ `false`“ ist das Anfügen von Daten nicht zulässig.

- Wert: true/false
- Zielelement: Feld
- Standardwert: falsch

Domain Separation und Edge Encryption

Domänentrennung wird in begrenzten Fällen mit Edge Encryptionunterstützt. Edge Encryption bietet die Möglichkeit, Daten aus der Umgebung des Kunden mithilfe bestimmter Konfigurationen, Regeln und Schlüssel zu verschlüsseln, die im Proxy Edge Encryption definiert sind. Der Edge Encryption Proxy ist nicht domänenabhängig und unterstützt keine domänenspezifischen Einstellungen. Mit der Domain Separation können Sie Daten, Prozesse und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

Funktionsweise der Domänentrennung in der Edge Encryption

Die Edge Encryption kann verwendet werden, wenn keine domänenspezifischen Schlüssel, Konfigurationen und Regeln erforderlich sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Datenintegration mit Edge Encryption

Um Daten von Drittanbietern mit einer Instanz über Edge Encryption zu integrieren, müssen Sie die Daten über den Edge Encryption Proxy-Server mit unterstützten Integrationen weiterleiten. Unterstützte Integrationen verwenden Verschlüsselungsregeln des Basissystems, die Daten in jeder Payload auf Felder in einer Tabelle abbilden.

Daten in für die Verschlüsselung markierte Felder hochladen

Edge Encryption unterstützt nicht den Import von Daten aus oder den Export von Daten nach Excel, CSV, XML oder anderen Dateitypen in oder aus Feldern mit definierten Verschlüsselungskonfigurationen.

ODBC-Treiber

Verschlüsseln Sie Anforderungen und Datenabfragen über den Edge Encryption Proxy-Server mit dem ODBC-Treiber.

Weitere Informationen: Edge Encryption ODBC-Treiberintegration

MID-Server

Sie können MID-Server so konfigurieren, dass Daten über einen Edge Encryption Proxy-Server geleitet werden. Es gelten jedoch einige Einschränkungen.

Weitere Informationen: Edge Encryption MID-Server-Integration

REST/SOAP Web Services

Verwenden Sie REST/SOAP Web Services zum Aktualisieren oder Abrufen von Datensatzdaten über den Edge Encryption Proxy-Server.

Weitere Informationen: Webservices

JSONv2-Webservice

Verwenden Sie JSONv2-Webservice-APIs zum Aktualisieren oder Abrufen von Datensatzdaten über den Edge Encryption Proxy-Server. Verschlüsselungsregeln des Basissystems unterstützen APIs zum Abrufen und Ändern von Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um einen einzelnen Datensatz über die Datenänderungs-API einzufügen, verwenden Sie die Methoden `insert()` oder `insertMutiple()`.
- Um mehrere Datensätze über die Datenänderungs-API einzufügen, verwenden Sie die Methode `insertMultiple()`.

Weitere Informationen: JSONv2 Web Service

Um Daten von benutzerdefinierten Drittanbieter-Integrationen zu verschlüsseln, die oben nicht aufgeführt sind, erstellen Sie benutzerdefinierte Verschlüsselungsregeln. Weitere Informationen finden Sie unter Eine benutzerdefinierte Verschlüsselungsregel definieren.

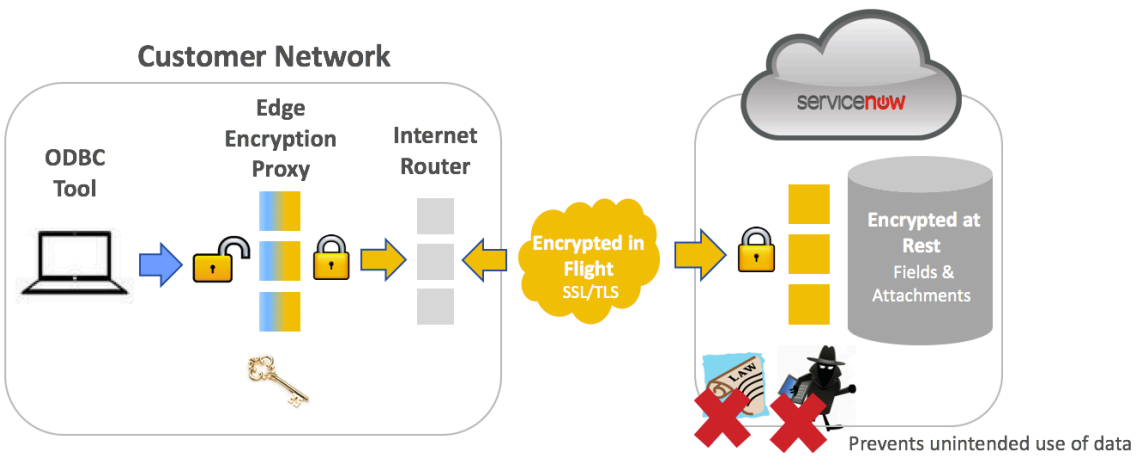
Anhänge zu zur Verschlüsselung markierten Datensätzen hochladen

Anhänge können in Tabellen hochgeladen werden, wobei die Anhangsverschlüsselung mithilfe von REST und SOAP Web Services konfiguriert wird.

Edge Encryption ODBC-Treiberintegration

Konfigurieren Sie Ihren ODBC-Treiber für die Abfrage von Daten, die mit Edge Encryption verschlüsselt sind. Der Edge Encryption Proxy-Server verschlüsselt ODBC-Treiberanfragen an die ServiceNow-Instanz, wenn Edge Encryption mit dem ODBC-Treiber integriert ist.

Verschlüsselte Antworten von der Instanz werden über den Edge Encryption Proxy-Server entschlüsselt, bevor sie an den ODBC-Treiber in Ihrem Netzwerk weitergeleitet werden.



Für eine erfolgreiche Integration muss der ODBC-Treiber dem Zertifikat des Edge Encryption Proxy-Servers vertrauen. Wenn das Zertifikat des Edge Encryption Proxy-Servers von einer Zertifizierungsstelle signiert wird, die vom ODBC-Treiber vertraut wird, wird dem Proxy-Server Edge Encryption automatisch vertraut. Wenn jedoch eine Zertifizierungsstelle, der der ODBC-Treiber vertraut, das Edge Encryption Proxy-Server-Zertifikat nicht signiert hat, müssen Sie das selbstsignierte Zertifikat in den ODBC-Truststore importieren.

Ein selbstsigniertes Zertifikat in den ODBC-Truststore importieren

Wenn eine Zertifizierungsstelle, der der ODBC-Treiber vertraut, das Edge Encryption Proxy-Server-Zertifikat nicht signiert hat, müssen Sie ein selbst signiertes Zertifikat in den ODBC-Truststore importieren. Sie können das Zertifikat vom Edge Encryption Proxy-Server exportieren und in den ODBC-Truststore importieren.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um festzustellen, ob eine vom ODBC-Treiber vertrauenswürdige Zertifizierungsstelle das Zertifikat des Edge Encryption Proxy-Servers signiert hat, führen Sie den folgenden Befehl im Schlüsselspeicherverzeichnis im Stammverzeichnis des Proxys aus, um eine Liste der vom ODBC-Treiber vertrauenswürdigen Zertifizierungsstellen anzuzeigen:

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts" -list
```

Hinweis:

In den meisten Fällen stellt der Client über ein Lastenausgleichsmodul eine Verbindung zu den Edge Encryption -Proxys her, sodass das Zertifikat das im Lastenausgleichsmodul konfigurierte Zertifikat ist.

Wenn zwischen dem Client und dem Edge-Proxy-Server kein Lastenausgleichsmodul vorhanden ist, ist das Zertifikat das vom Edge-Proxy vorgelegte Zertifikat und wird in der Datei *edgeencryption.properties* konfiguriert.

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

Weitere Informationen zum Bearbeiten von Eigenschaften finden Sie unter Zusätzliche Eigenschaften in der Edge Encryption-Eigenschaftendatei konfigurieren

Prozedur

1. Wechseln Sie in das Schlüsselspeicherverzeichnis im Proxy-Stammverzeichnis.
2. Überprüfen Sie den Schlüsselspeicher auf das selbstsignierte Zertifikat.
   a. Um den Schlüsselspeicher für das Zertifikat zu überprüfen, können Sie den folgenden Befehl ausführen, um alle Elemente im Schlüsselspeicher aufzulisten.

      ```
      keytool -list -keystore keystore.jceks -storetype jceks -v
      ```

   b. Suchen Sie den Schlüsselalias in der Liste der Elemente.
3. Exportieren Sie das Zertifikat mithilfe des Schlüsselalias in eine CER-Datei.

   ```
   keytool -export -alias <key alias> -keystore keystore.jceks -storetype jceks -rfc -file <file name>.cer
   ```
4. Wechseln Sie in Ihr ODBC-Truststore-Verzeichnis: ODBC\ip\Java\jre\lib\security\cacerts.
5. Importieren Sie das Zertifikat in Ihren ODBC-Truststore.

   ```
   keytool -keystore cacerts -importcert -alias $<key alias> -file <file name>.cer
   ```

Die ODBC-Treibereigenschaften festlegen

Legen Sie die ODBC-Treibereigenschaften so fest, dass Anforderungen über den Edge Encryption Proxy-Server geleitet werden.

Vorbereitungen

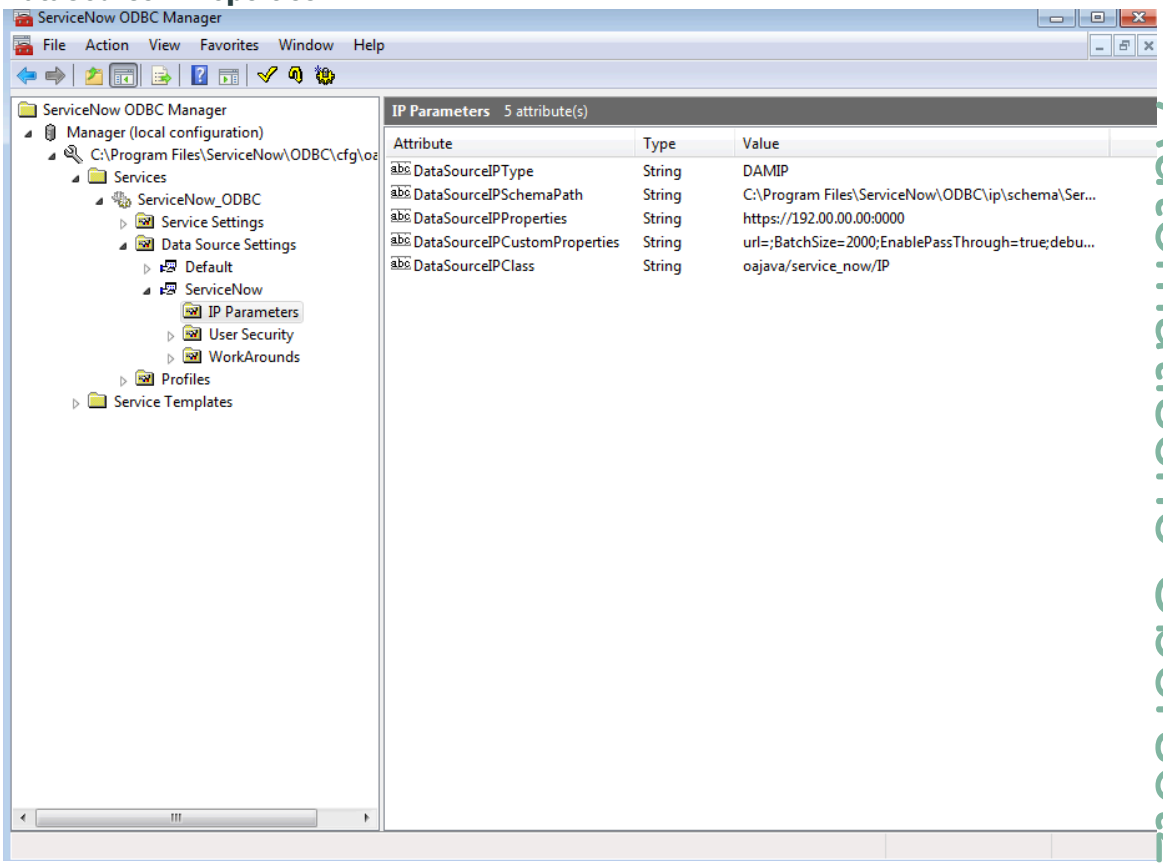
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie in Windows zu **Starten** > **Programme** > **ServiceNow ODBC-Verwaltungskonsole**.
2. Erweitern Sie das Stammverzeichnis der Konsolenstruktur um: ServiceNow ODBC Manager\Manager \<installation location>\Services\ServiceNow_ODBC\Data Source Settings\ServiceNow\IP Parameters.
3. Doppelklicken Sie auf das Attribut **DataSourceIPProperties**.
4. Ändern Sie den **Wert** auf die URL Ihres Edge Encryption Proxy-Servers, wie z. B. https://<IP address>:<port>

DataSourceIPProperties



5. Klicken Sie auf **OK**.

Nächste Maßnahme

Der ODBC-Treiber ist jetzt so konfiguriert, dass Anforderungen an die Instanz über den Edge Encryption Proxy-Server weitergeleitet werden.

Edge Encryption MID-Server-Integration

Konfigurieren Sie MID-Server so, dass Daten über den Edge Encryption Proxy-Server geleitet werden.

Bei der Integration mit MID-Server fungiert der Edge Encryption Proxy-Server als Endpunkt des MID-Server. Der Edge Encryption Proxy-Server verschlüsselt und entschlüsselt dann die zwischen der ServiceNow-Instanz und dem MID-Server übertragenen Daten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränkungen bei der Integration mit dem MID-Server

Wenn die Daten von MID-Server so konfiguriert sind, dass sie den Edge Encryption Proxy-Server durchlaufen, gelten die folgenden Einschränkungen:

- Die Verschlüsselung der ECC-Warteschlangenfelder wird nicht unterstützt.
- Verschlüsselte Daten können nicht mit Discovery oder Service-Mapping verwendet werden.

Den MID-Server auf den Edge Encryption Proxy-Server verweisen

Um Daten von MID-Server über den Edge Encryption Proxy-Server zu übertragen, aktualisieren Sie die MID-Server-Konfigurationsdatei, um MID-Server auf den Edge Encryption Proxy-Server zu verweisen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn MID-Server so konfiguriert ist, das der Edge Encryption Proxy-Server durchlaufen wird, können Sie die Web-Proxy-Eigenschaften in der MID-Server-Konfigurationsdatei nicht verwenden, um den Datenverkehr über den Edge Encryption Proxy-Server zu Ihrer Instanz zu leiten. Stattdessen müssen Sie den Edge Encryption Proxy-Server als den Endpunkt von MID-Server einstellen.

Prozedur

1. Navigieren Sie zum lokalen MID-Server-Verzeichnis und öffnen Sie die Datei config.xml.
2. Suchen Sie das Element `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` und ändern Sie die Eigenschaft „Wert“ auf die URL Ihres Edge Encryption Proxy-Servers.
   Beispiel: `http://hostname.mycompany.com:8081`
   Mit diesem Schritt wird MID-Server angewiesen, den Datenverkehr an den Edge Encryption Proxy-Server und nicht an die Instanz zu leiten. Der Edge Encryption Proxy-Server wiederum verschlüsselt alle erforderlichen Felder und leitet die Nutzdaten an die Instanz weiter.
3. Speichern und schließen Sie die Datei.
4. Starten Sie den MID-Server neu, wenn schon in Ausführung.

Diagnose und Leistung der Edge Encryption

Überwachen sie Performance-Trends des Edge Encryption Proxy-Servers und untersuchen Sie die vom Edge Encryption Proxy-Server generierten Fehler.

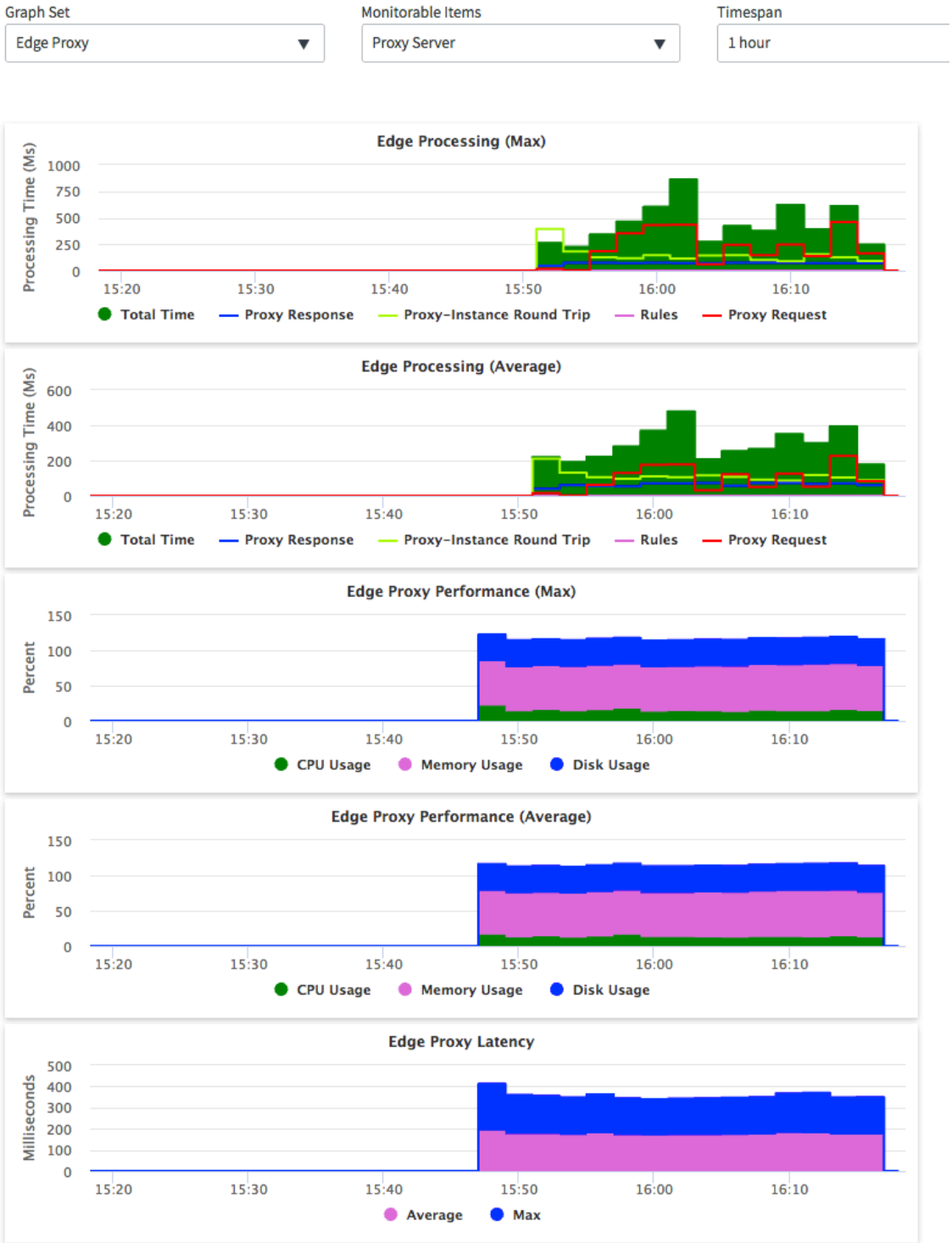
Edge-Proxy-Leistung

Sehen Sie sich die wichtigsten Performance-Trends des Edge Encryption Proxy-Servers mithilfe des Edge-Proxy-Diagramms auf der ServiceNow Performance-Homepage an. Überwachte Trends umfassen:

- Maximale und durchschnittliche Antwortzeit zwischen Client, Proxy-Server und Instanz.
- CPU, Speicherplatz und Speicherplatz des Host-Computers.
- Maximale und durchschnittliche Netzwerklatenz zwischen dem Proxy-Server und der ServiceNow-Instanz.

Hinweis:
Edge Encryption Proxy-Server mit doppelten Namen melden keine Performance-Trends.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Edge-Verarbeitung (Maximum und Durchschnitt)

Maximale und durchschnittliche Zeit in Millisekunden für die Verarbeitung einer Anforderung. Diese Datenpunkte sind allgemeine Trends im Zeitablauf.

- **Gesamtzeit**: Zeit, in der der Proxy-Server eine Anforderung von einem Client erhält und eine Antwort sendet. Dieser Datenpunkt ist die Summe der nachfolgenden Datenpunkte.
- **Proxy-Antwort**: Zeit, in der der Proxy-Server eine Antwort der Instanz verarbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

- **Proxy-Instanz-Rundlauf**: Zeit, in der der Proxy-Server eine Anforderung an die Instanz sendet und eine Antwort erhält. Enthält die Netzwerklatenz zwischen dem Proxy-Server und der Instanz sowie die Zeit, die die Instanz für die Verarbeitung der Anforderung benötigt.
- **Regeln**: Zeit, die der Proxy-Server benötigt, um eine Anforderung anhand definierter Verschlüsselungsregeln auszuwerten.
- **Proxy-Anforderung**: Zeit, in der der Proxy-Server eine Client-Anforderung verarbeitet und an die Instanz weiterleitet.

Edge Proxy-Performance (Maximum und Durchschnitt)

Maximaler und durchschnittlicher Prozentsatz der auf dem Host-Computer verwendeten Ressourcen.

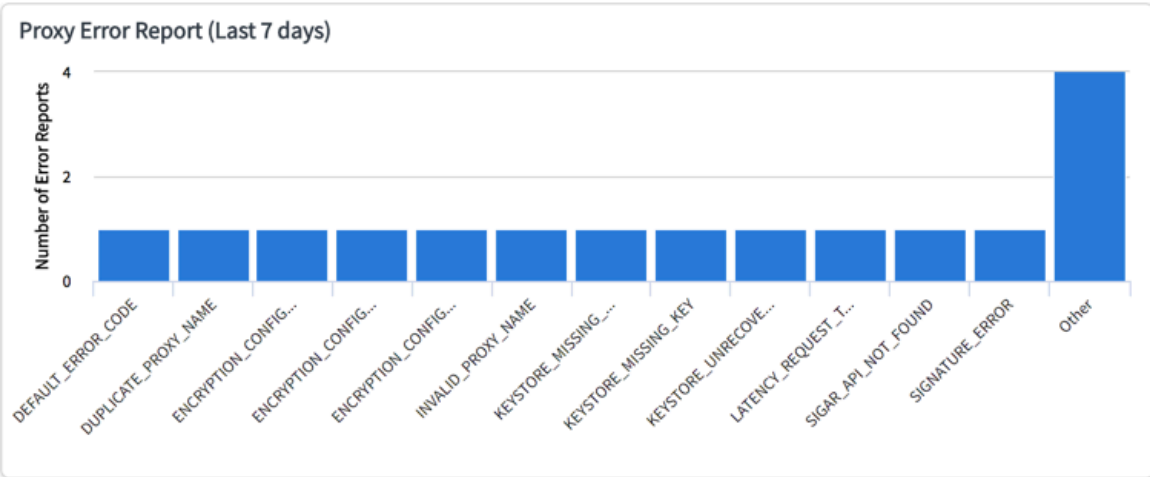
- CPU-Auslastung
- Speicherauslastung
- Festplattenauslastung

Edge-Proxy-Latenzzeit

Maximale und durchschnittliche Netzwerklatenz in Millisekunden zu einem bestimmten Zeitpunkt. Die Latenz wird durch die Rundlaufzeit bestimmt, die ein Proxy-Server benötigt, um einen einfachen Ping an die Instanz zu senden und eine Antwort zu empfangen.

Proxy-Fehlerberichte

Navigieren zu **Konfiguration der Edge Encryption** > **Diagnose und Fehlerbehebung** > **Proxy-Fehlerberichte** , um alle in den letzten sieben Tagen erfassten Proxy-Server-Fehler anzuzeigen.



Fehler werden über einen Zeitraum von einer Minute erfasst. Jede Minute wird ein Fehlerbericht generiert. Die vertikale Achse zeigt die Anzahl der Fehlerberichte der letzten sieben Tage an, die jeden Fehler enthalten. Selbst wenn beispielsweise der Fehler DEFAULT_ERROR_CODE über einen Zeitraum von einer Minute mehrmals ausgelöst wird, erreicht die Leiste DEFAULT_ERROR_CODE nur einen Fehler auf der Achse **Anzahl der Fehlerberichte**.

In dieser Ansicht können Sie:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Auf die einzelnen Proxy-Fehlercodeleisten klicken, um den Bericht über einen einzelnen Fehler für jeden Proxy-Server anzuzeigen. In dieser Ansicht können Sie erneut auf die Leiste klicken, um den Fehlertext in der Edge Encryption Proxy-Statistiktabelle [edge_encryption_stat] anzuzeigen. Folgen Sie den Links im Fehlertext, um weitere Informationen und mögliche Schritte zur Fehlerbehebung anzuzeigen.
- Klicken Sie auf **Andere**, um die zweite Seite des Fehlerberichts zu sehen.

Hinweis:
Wenn Sie mehr als einen Proxy-Server mit demselben Namen haben, wird im Proxy-Fehlerbericht ein einzelner Fehler DUPLICATE_PROXY_NAME angezeigt. Für Proxy-Server mit doppelten Namen werden keine anderen Fehler gemeldet. Wenn dieser Fehler auftritt, stellen Sie sicher, dass alle Proxy-Server eindeutige Namen haben.

Zusätzlich Überwachungsressourcen

Die Instanz verfolgt alle Verschlüsselungsproxys. Jeder Edge Encryption Proxy-Server registriert sich beim Start. Die Instanz wird benachrichtigt, wenn:

- Ein neuer Edge Encryption Proxy-Server gestartet wird.
- Ein Edge Encryption Proxy-Server absichtlich heruntergefahren wird.

Wenn ein Edge Encryption Proxy-Server versucht, sich bei einer Instanz zu registrieren, die Edge Encryption nicht installiert hat, wird der Proxy nicht gestartet.

Alle Verschlüsselungskonfigurationsdateien werden geprüft. Gelöschte Datensätze werden für alle Verschlüsselungskonfigurationsdateien geprüft. Audit-Datensätze werden in der Tabelle sys_audit abgelegt. Um den Verlauf eines bestimmten Konfigurationsdatensatzes anzuzeigen, zeigen Sie den Datensatz an, und klicken Sie auf **Verlauf** > **Liste** im Menü. Der Massenverschlüsselungsauftrag wird keinem Audit unterzogen.

Verwenden Sie die folgenden zusätzlichen Ressourcen, um Ihre Proxy-Server zu überwachen.

Tabelle	Beschreibung
Ungültige Einfügeversuche [sys_edge_encryption_invalid_insert_log]	Liste der Versuche, die folgenden Daten in verschlüsselten Feldern zu speichern: • Nicht verschlüsselte Daten. • Daten, die nicht von einem Edge Encryption Proxy stammen. Die Instanz lehnt alle Versuche ab, diese Daten zu speichern, und protokolliert sie anschließend. Wenn Sie die Rolle Security-Admin haben, können Sie die Protokolle in der Liste „Ungültige Einfügeversuche“ anzeigen.
Auftragsfehler [sys_encryption_job_execution]	Eine Liste der Aufträge, die nicht erfolgreich ausgeführt wurden.
Systemprotokolle	Die Instanz sucht regelmäßig nach Nachrichten von jedem registrierten Proxy-Server. Wenn ein Proxy-Server im erforderlichen Zeitraum keine Nachricht gesendet hat, wird ein Fehler protokolliert. Die Protokollnachricht enthält Informationen zum Verschlüsselungs-Proxy

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	und den letzten Zeitpunkt, zu dem der Proxy die Instanz gepingt hat. Wenn die Instanz feststellt, dass keiner der Verschlüsselungsproxys online ist, protokolliert sie eine Nachricht. Diese Meldungen werden zum Systemprotokoll hinzugefügt.

Die Edge Proxy-Statistikerfassung deaktivieren oder reduzieren

Verhindern Sie, dass der Edge Encryption Proxy-Server Edge Proxy Diagrammsatz-Statistiken an die ServiceNow Performance-Homepage sendet, oder reduzieren Sie die Häufigkeit der statistischen Erfassung.

Vorbereitungen

Erforderliche Rolle: admin oder security_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch das Hinzufügen von Eigenschaften in der Konfigurationsdatei edgeencryption.properties können Sie:

- Den Edge Proxy-Diagrammsatz deaktivieren.
- Das Intervall ändern, in dem die Statistiken vom Edge Encryption Proxy-Server erfasst werden. Standardmäßig werden Statistiken alle 30 Sekunden erfasst.

Prozedur

1. Öffnen Sie in Ihrem Installationsverzeichnis des Proxy-Servers die Konfigurationsdatei edgeencryption.properties im Ordner <installation directory>/conf/.
2. Fügen Sie einen der Eigenschaften des Edge Encryption Proxy-Servershinzu .
3. Starten Sie den Proxy-Server neu.

Erhöhen Sie die Debug-Protokollierung für den Edge Encryption -Proxy

Erhöhen Sie die Protokollierungsebene, um die Protokolle zu interpretieren und Probleme mit dem Proxy zu debuggen.

Derzeit gibt es drei Optionen zum Erhöhen der Debug-Protokollierung im Proxy Edge Encryption. Erhöhen Sie die Protokollierungsebene, um Probleme zu debuggen, und stellen Sie dem technischen Support Informationen zur Verfügung, um das Problem mit dem Vorteil ausführlicherer Protokollanweisungen zu untersuchen.

Abhängig vom zu debuggenden Problem richten Sie die Debug-Protokollierung auf eine von drei Arten ein:

- Andere Debugging-Probleme als SSL-Konnektivität
- Zeitmetriken für Anforderungen über den Proxy protokollieren
- Debugging von Problemen mit SSL-Konnektivität zwischen dem Edge Encryption-Proxy und der Instanz

Für alle Debug-Fälle können Sie die Protokolle in Ihrem eigenen anzeigen und interpretieren oder einen Incident öffnen, um eine Interpretation vom technischen Support von ServiceNow zu erhalten, der die Beschreibung des Problems und seine Reproduzierbarkeit bereitstellt.

Debugging-Probleme mit der Anwendung Edge Encryption außer SSL-Konnektivität

Verwenden Sie diese Methode, um Probleme mit der Anwendung Edge Encryption zu debuggen, ohne den Proxy anzuhalten und neu zu starten. Diese Schritte erhöhen die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollierungsebene und helfen bei der Behebung der Ursache durch ausführlichere Protokollanweisungen.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis:
An der Datei $proxy_installation_location/conf/log4j2.properties vorgenommene Änderungen werden innerhalb von etwa 60 Sekunden nach der Änderung vom Proxy übernommen. Sie müssen die Proxys nicht neu starten.

Prozedur

1. Suchen Sie in der Datei $proxy_installation_location/conf/log4j2.properties die folgende Zeile.

```
logger.edge.level=info
```

2. Ändern Sie die obige Zeile wie folgt:

```
logger.edge.level=debug
```

3. Speichern Sie die Änderung.
   Es kann bis zu 60 Sekunden dauern, bis die Änderung wirksam wird. Dies erfordert jedoch keinen Proxy-Neustart.
4. Reproduzieren Sie Ihr Problem.
5. Suchen Sie in der Datei $proxy_installation_location/logs/edgeencryption.log nach Debug-Protokollanweisungen im Zusammenhang mit der Anwendung.

Ergebnisse
Nachdem Sie die Eigenschaft geändert haben, werden zusätzliche Details in der Datei $proxy_installation_location/logs/edgeencryption.log angezeigt. Wenn Sie das Debugging abgeschlossen haben, machen Sie die an der Datei $proxy_installation_location/conf/log4j2.properties vorgenommene Änderung rückgängig.

Zeitmetriken für Anforderungen über den Proxy protokollieren

Aktivieren Sie die Protokollierung von Zeitmetriken, um eine Metrikanweisung für jede vom Proxy Edge Encryption verarbeitete Anforderung hinzuzufügen. Jede dieser Protokollanweisungen für Zeitmetriken enthält nützliche Informationen zur Anforderung, z. B. Verarbeitungszeiten und welche Verschlüsselungsregel verwendet wurde.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis:

Die zusätzlichen Protokollierungseinstellungen werden der Datei $proxy_installation_location/conf/log4j2.properties hinzugefügt. Vorgenommene Änderungen werden dynamisch innerhalb von etwa einer Minute nach den Änderungen an der Datei vom Proxy übernommen, sodass Sie die Proxys nicht neu starten müssen.

Prozedur

1. Ändern Sie die Datei $proxy_installation_location/conf/log4j2.properties, indem Sie die folgenden Zeilen am Ende der Datei hinzufügen

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
appender.timinglog.fileName=../logs/edgenetwork.log
appender.timinglog.filePattern=../logs/$
${date:yyyy-MM}/edgenetwork-%d{yyyy-MM-dd-HH}-%i.log.gz
appender.timinglog.layout.type=PatternLayout
appender.timinglog.layout.pattern=%d [%t] %-5p %m%n
appender.timinglog.policies.type=Policies
appender.timinglog.policies.size.type=SizeBasedTriggeringPolicy
appender.timinglog.policies.size.size=500MB
appender.timinglog.strategy.type=DefaultRolloverStrategy
appender.timinglog.strategy.max=4

logger.timing.name=com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache
logger.timing.level=debug
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. Speichern Sie die Datei.

Ergebnisse

Nachdem die Datei log4j.properties gespeichert wurde, werden die folgenden Arten von Nachrichten in der Protokolldatei $proxy_installation_location/logs/edgenetwork.log für Netzwerkzeiten angezeigt.

```
2022-07-21 12:56:15,783 [qtp1971991758-7700] DEBUG
 com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache -
 request_uri=/api/now/ui/presencesysparm_auto_request=true&cd=1658433375754
 request_method=POST client_request_received="2022-07-21 12:56:15,015"
 proxy_request_processing_time=6 all_rules_processing_time=0
 rule_executed="REST JSON" rule_execution_time=1 proxy_instance_round_trip=14
 proxy_response_processing_time=1 total_time_from_proxy=21 reponse_code=201
 glide_user=SCv3_1:BAz1ZK7ee9XoroG2nvMlixHpgTvsT4fY2bwQvnH2WdU=:y5HGsTTqo3Pjq6
G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

Die Werte in den Protokollnachrichten lauten wie folgt:

```
request_uri: The URI being requested

request_method: The HTTP method being used, for example, GET, POST, PUT, PATCH,
 DELETE

client_request_received: The timestamp noting when the HTTP client request arrived at the
 Edge proxy

proxy_request_processing_time: How long the Edge proxy took to process the request in
 milliseconds

all_rules_processing_time: Total time it took to execute all of the Edge Encryption rules for the
 request in milliseconds

rule_executed: The name of the encryption rule that was executed

rule_execution_time: How long it took to execute listed rule_executed in milliseconds

proxy_instance_round_trip: The time from when the Edge proxy sent the request to the instance
 until the instance sent the response and was received by the edge proxy in milliseconds
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

proxy_response_processing_time: How long the Edge proxy took to process the response in milliseconds

total_time_from_proxy: The total time from when the Edge proxy received the request from the client and returned the response to the client in milliseconds

response_code: HTTP response code

glide_user: The glide_user cookie value

jsessionid_suffix: The JSession cookie suffix associated with the request

Debuggen Sie Probleme mit SSL-Konnektivität zwischen dem Edge Encryption -Proxy und der Instanz

Verwenden Sie diese Methode, um Probleme mit der SSL-Konnektivität zwischen dem Edge Encryption -Proxy und Ihrer Instanz zu debuggen, z. B. wenn der Zugriff auf die Instanz über den Proxy fehlschlägt. Diese Schritte erhöhen die Protokollierung und helfen bei der Suche nach ausführlichen Protokollanweisungen.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis:
Das Debuggen der SSL-Konnektivität ist nur relevant, wenn Probleme mit dem TLS-Konnektivitätstyp behoben werden. In der Praxis ist dies nicht üblich und wird nur selten benötigt.

Prozedur

1. Den Proxy-Server stoppen.
2. Fügen Sie der Datei $proxy_installation_location/conf/wrapper.conf, einer Java-Starteigenschaft, die folgende Zeile hinzu:

   ```
   wrapper.java.additional.<next available number in sequence> = -Djavax.net.debug=all
   ```

   Beispiel:

   ```
   For example: wrapper.java.additional.4 = -Djavax.net.debug=all
   ```

3. Speichern Sie die Änderung, und starten Sie den Proxy-Server neu.
4. Reproduzieren Sie Ihr Konnektivitätsproblem.

Ergebnisse

Nach der Reproduktion des Problems finden Sie Debug-Protokollanweisungen im Zusammenhang mit dem SSL-Austausch in $proxy_installation_location/logs/wrapper_.<current date> .log -Datei. Wenn Sie mit dem Debuggen fertig sind. Sie können die zusätzliche Protokollierung remote durchführen, indem Sie die in den vorherigen Schritten erstellte Zeile entfernen oder auskommentieren.

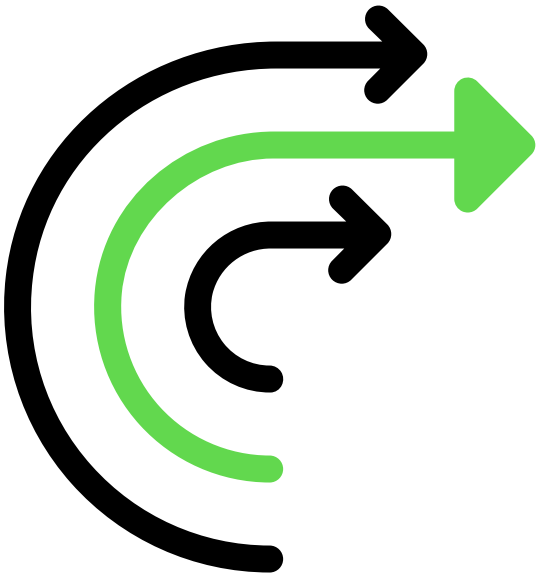
Protokolle

Das Modul „Logs“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben von Problemen und zum Debuggen von Transaktionen und Events innerhalb der Instanz verwenden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

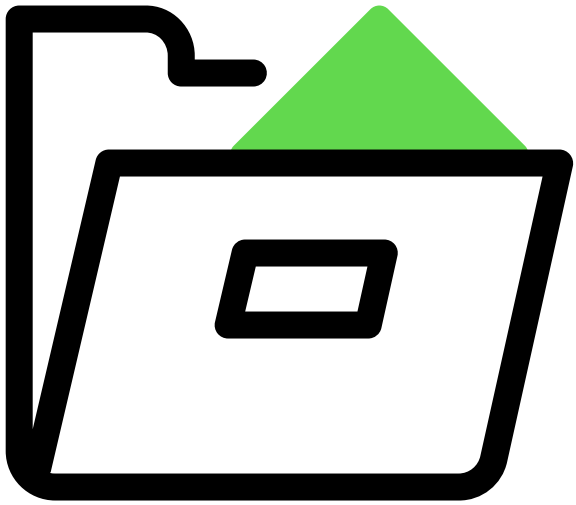
Erste Schritte

Systemprotokolle



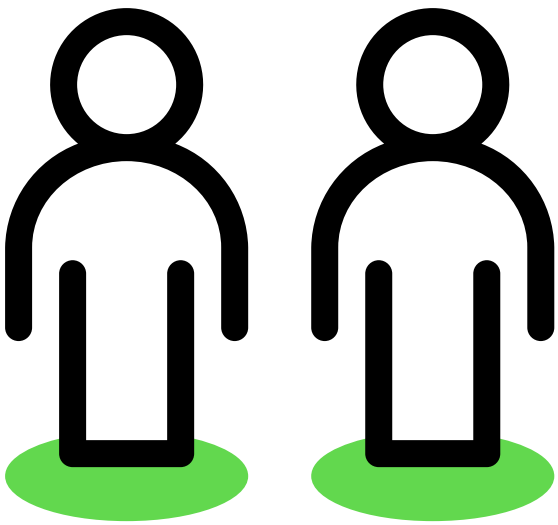
Das Modul „Systemprotokolle“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Events innerhalb der Instanz verwenden können.

Protokollexportservice



Log Export Service Mit (LES) können Sie Protokolle selektiv von der ServiceNow-Instanz an Hermes weiterleiten und sie dann für die Eingabe in die Systeme von verwenden.

Protokollierung, Audits und Fehler



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenden Sie eine Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Systemprotokolle

Das Modul „Systemprotokolle“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Events innerhalb der Instanz verwenden können.

Greifen Sie über das Modul „Systemprotokolle“ auf die folgenden Protokolle zu:

Protokoll	Beschreibung
Transaktionen	Alle Anwendungsaktivitäten für eine Instanz.
E-Mail und Push	Alle E-Mail-Benachrichtigungen und Push-Nachrichten, die von allen Instanzen im System gesendet werden.
Ereignisprotokolle	Alle System-Events, die innerhalb des Systems auftreten.
Importieren	Datenimportaktivität innerhalb der Plattform.
Tabellenänderungen	An allen Tabellen im System vorgenommene Änderungen.
Protokollierung für ausgehende Webservices	Alle ausgehenden Webserviceanforderungen wie REST- und SOAP-Anforderungen.
Signaturbilder	Elektronische Signaturen für das HR-Signaturpad.
System	Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse, z. B. Speichernutzung auf dem Servercomputer.

Verwenden Sie den Protokolldateibrowser, um Protokolle zu suchen und herunterzuladen. Sie können auch archivierte Protokolle im Protokollverlaufdurchsuchen.

Andere Protokolle

Ihre Instanz bietet zusätzlich zu den Protokollen im Systemprotokollmodul weitere Protokolle. Zum Beispiel bietet Modul „System Diagnostics“. Protokolle für den Upgradeverlauf und langsame Abfragen, mit denen Sie Einblicke erhalten können, wie sich Abfragen auf die Plattformleistung auswirken. Tabelle „Kunden-Updates“. zeichnet jede Änderung auf, die im System vorgenommen wird.

Systemprotokoll

Zeigen Sie Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse an, z. B. Speichernutzung auf dem Servercomputer.

Die folgenden Informationen werden im Systemprotokoll nachverfolgt:

- Workflows
- Konfiguration
- Chats-Sitzungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Transaktionen für jede Ansicht jeder Seite im System, einschließlich Ladezeiten für Netzwerk, Server und Browser
- Eingehende und ausgehende E-Mails
- Events, die im System ausgelöst werden
- Importe und Integrationen
- Systemwarnungen, Fehler und Skriptprotokolle
- Upgrade-Informationen für Plugin-Aktivierungen, Update Sets oder System-Upgrades

Protokolleinträge werden nur für den aktuellen Tag angezeigt. Um andere Protokolldateien anzuzeigen, verwenden Sie den Protokolldateibrowser. Dieses Protokoll enthält die folgenden Informationen für alle Vorkommen:

Systemprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Protokollierungsaktivität für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Ebene	Typ der Nachricht. Die Ebenen sind Debug, Fehler, Warnung und Information. • Eine Warnung ist ein Fehler, der behandelt und behoben wurde. • Ein Fehler ist etwas, das behoben werden muss.
Nachricht	Vom System generierte Nachricht bezüglich der Art des Vorkommens.
Quelle	Name des vom Vorkommen betroffenen Prozesses oder Bereichs. Beispielsweise kann die Quelle des Vorkommens E-Mail oder Speicher sein.
Quellpaket	Name des Anwendungspakets, das dem Vorkommen zugeordnet ist. Klicken Sie auf den Namen, um den Store-Anwendungsdatensatz [sys_store_app] für dieses Paket anzuzeigen.

Workflow-Protokollierung

- Jede ausgeführte Aktivität, einschließlich:
  - Datum und Uhrzeit des Starts
  - Datum und Uhrzeit des Endes
  - Status, z. B. Abgeschlossen, Abgebrochen, Zeitüberschreitung, Fehler
  - Ergebnis
  - Fehlerbeschreibung, wenn ein Fehler aufgetreten ist
- Übergangsverlauf, einschließlich:
  - Zeitpunkt des Übergangs
  - Aktivität wurde von umgestellt
  - Aktivität wurde in geändert
  - Welcher Übergang ausgelöst wurde
- Workflow-Protokoll, einschließlich aller Protokollanweisungen, die dem Workflow hinzugefügt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsinformationen

- Ausgeführte Aktion, einschließlich Einfügen, Aktualisieren und Löschen
- Kategorie des Change
- Mit dem Change aufgezeichnete Kommentare
- Name des Change
- XML-Unterschied des Change
- Update Set, dem der Change zugeordnet ist
- Datum und Uhrzeit des Change
- Benutzer, der die Änderung vorgenommen hat
- Tabelle, in der die Änderung vorgenommen wurde
- Name des Objekts, das geändert wird
- Typ des Objekts, das geändert wird
- Zeigen Sie die Änderung in vorgenommenen Änderungen an, um Änderungen an Formularen oder Listen anzuzeigen

Transaktionsprotokolle

Das Transaktionsprotokoll zeichnet alle Browseraktivitäten für eine Instanz auf. Um das Debuggen von Systemproblemen zu unterstützen, können Sie Transaktionsprotokolle nach Anwendungsbereich filtern und so die angezeigten Transaktionen auf Transaktionen beschränken, die aus bestimmten Bereichen stammen.

Das Transaktionsprotokoll enthält die folgenden Informationen für alle Aktivitäten.

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Anwendungsaktion für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Typ	Typ der aufgezeichneten Transaktion.
Erstellt von	Benutzer, der diese Aktivität erstellt hat.
Ursprungsanwendung	Anwendungsbereich, aus dem die Transaktion stammt. Global wird angezeigt, wenn die Transaktion aus dem globalen Bereich stammt.
Antwortzeit	Antwortzeit für die Anwendungsanforderung in Millisekunden.
Netzwerkzeit	Latenzzeit der Netzwerkantwort nach der Anwendungsanforderung in Millisekunden.
Ausgabelänge	Größe der Ausgabezeichenfolge, die von der Instanz an die Anwendung gesendet wird, in Byte.
SQL-Anzahl	Anzahl der für diese Aktivität ausgeführten SQL-Serverbefehle.
Business-Regel-Anzahl	Anzahl der für diese Aktivität ausgeführten Business Rules.
Business-Regel-Zeit	Verstrichene Zeit für die Ausführung der Business Rules für diese Aktivität.
URL	Anwendung oder Modul, mit der die Clientanwendung verbunden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
System-ID	Vom System generierter Bezeichner der Client-Instanz, die die Anforderung sendet. Diese ID wird für Clusterumgebungen verwendet, in denen mehrere Instanzen (Knoten) mit der Datenbank kommunizieren.
IP-Adresse	IP-Adresse des Clients, der die Anforderung sendet.
GZipped	Gibt an, ob eine komprimierte Webseite von der Anwendung angefordert wurde.
Protokoll	Von der Anwendung für diese Instanz verwendetes HTTP-Protokoll.

Client-Transaktionszeiten

Das Plugin „Client Transaction Timings“ verbessert die Systemprotokolle durch Bereitstellung zusätzlicher Informationen zur Dauer von Transaktionen zwischen Client und Server.

Sie können Leistungsprobleme bis zu ihrer Quelle verfolgen, indem Sie anzeigen, wo die Zeit verbraucht wird und wie Zeit während einer Transaktion aufgewendet wurde.

Dieses Plugin erfordert die Aktivierung von Response Time Indicator Response Time Indicator und erfasst Informationen aus den folgenden Browsern:

- Firefox
- Internet Explorer
- Chrome

Client-Transaktionsinformationen

Durch die Installation des Plugins wird das Modul „ *Client-Transaktionen* “ der Anwendung *„Systemprotokolle“ hinzugefügt*. Sie enthält eine Liste aller protokollierten Transaktionen zwischen Client und Server innerhalb des letzten Tages:

Client-Transaktionsinformationen

Feld	Beschreibung
Erstellt	Zeitpunkt, zu dem die Transaktion aufgezeichnet wurde.
Antwortzeit	Anzahl der ms, die vom Server für die Erfüllung der Transaktion aufgewendet wurden.
Business-Regel-Zeit	Anzahl der ms, die von Business Rules aufgewendet wurden, die durch die Transaktion ausgelöst wurden.
SQL-Zeit	Anzahl der von der SQL-Datenbank aufgewendeten ms.
Client-Antwortzeit	(Load_completion_time) – (start_time). Sie enthält die Serverzeit.
Client-Netzwerkzeit	Anzahl der ms, die vom Netzwerk aufgewendet wurde, über das der Client eine Verbindung herstellt
Browserzeit	Anzahl der vom Browser während der Transaktion aufgewendeten ms.
Clientskriptzeit	Die Anzahl der für die Ausführung von Client-Skripts aufgewendeten ms.
UI-Richtlinienzeit	Anzahl der für die Ausführung der UI-Richtlinie aufgewendeten ms.
Typ	Typ der Transaktion:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client-Transaktionsinformationen (Fortsetzung)

Feld	Beschreibung
	• Formular • Liste • Sonstige
Tabelle	Name der angezeigten Tabelle. Beispiel: incident, change_request.
Ansicht	Ansicht für dieses Formular/diese Liste.

Detaillierte Client-Informationen

Eine detailliertere Aufgliederung der Client-Zeiten für das gesamte Formular-Rendering (aber nicht das Listen-Rendering) wird ebenfalls nachverfolgt. Um Details anzuzeigen, führen Sie einen Drilldown in einen bestimmten Client-Transaktionsdatensatz durch, und beobachten Sie die zugehörige Liste am unteren Bildschirmrand.

Detaillierte Client-Informationen

Feld	Beschreibung
Reihenfolge	Reihenfolge während des Ladevorgangs, in dem dieser Vorgang aufgetreten ist.
Typ	Typ des Vorgangs.
Name	Beschreibender Name dieses bestimmten Vorgangs
Dauer	Anzahl der ms, die dieser Vorgang zum Abschluss benötigt hat.

Push-Protokolle

Konsultieren Sie das Push-Protokoll, um den Status von Push-Benachrichtigungen nachzuverfolgen, die sich in der Warteschlange zum Senden von Ihrem System befinden.

Um das Push-Protokoll anzuzeigen, navigieren Sie zu **Systemprotokolle** > **Push-Benachrichtigungen**. Benutzer müssen über die Rolle push_admin oder admin verfügen, um das Push-Protokoll anzeigen zu können.

Push-Protokollfelder

Feld	Beschreibung
Anspruch	Identifikationsnummer, die von der geplanten Aufgabe generiert wird, die die Push-Benachrichtigung sendet. Diese Zahl wird auf das Feld **Anspruch** angewendet, um die Konsistenz über mehrere geplante Push-Aufgaben hinweg sicherzustellen.
Nutzlast	Inhalt der Push-Benachrichtigung.
Anzahl Warteschlange	Anzahl der Versuche des Systems, die Push-Benachrichtigung zu senden. Der Status der Push-Benachrichtigung bezieht sich auf die Anzahl der Warteschlange.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Push-Protokollfelder (Fortsetzung)

Feld	Beschreibung
	• Wenn die Anzahl der Warteschlange länger als erwartet 0 ist, gibt es keine geplanten Aufgaben, die versuchen, die Push-Benachrichtigung zu senden. • Wenn die Anzahl der Warteschlangen größer als 0 ist und der **Typ** „ **Success**“ lautet, können Sie daraus schließen, wie oft das System versucht hat, die Push-Benachrichtigung zu senden, bevor es sie schließlich gesendet hat. • Wenn die Anzahl der Warteschlangen 10 erreicht, versucht das System nicht mehr, die Push-Benachrichtigung zu senden. Der **Typ** ändert sich in **failure**.
Anforderungs-ID	Eindeutige Identifikationsnummer für die Push-Benachrichtigung. Ähnlich wie die Nachrichten-ID für eine E-Mail wird die Anforderungs-ID als Korrelationstoken für die Push-Benachrichtigung verwendet.
Typ	Status, der angibt, ob die Push-Benachrichtigung gesendet wurde. Die Spalte „Typ“ kann folgende Werte haben: • **Fehler**: Die Nachricht konnte nicht gesendet werden. • **Ausstehend**: Die Nachricht wird zur Verarbeitung in die Warteschlange versetzt. • **Erfolg**: Die Nachricht wurde erfolgreich gesendet, obwohl sie nicht unbedingt vom mobilen Gerät empfangen wurde.

Zugehörige Informationen

Geplante Aufgaben

System-E-Mail-Protokoll und -Postfächer

Im System-E-Mail-Protokoll werden alle E-Mails erfasst, die von der Instanz erstellt oder empfangen werden. Systempostfächer sind gefilterte Ansichten dieses Protokolls.

Alle Benachrichtigungs-E-Mails, die von der Instanz erstellt oder empfangen werden, werden in einem E-Mail-Datensatz [sys_email] aufgezeichnet. Sie können zu einem Protokoll dieser Datensätze unter navigieren **Systemprotokolle** > **E-Mails**.

Die Systempostfächer sind gefilterte Ansichten der E-Mail-Tabelle [sys_email]. Die Instanz weist einen E-Mail-Datensatz abhängig von den Werten der Felder **Typ** und Status einem **Systempostfach** zu. Weitere Informationen finden Sie unter Systempostfächer .

Die folgenden Felder können in das Layout vom Systemprotokoll und von allen Systempostfächern aufgenommen werden:

E-Mail-Protokoll

Feld	Beschreibung
Mailbox	Das Systempostfach, das diesen E-Mail-Datensatz enthält. Die Instanz legt den Wert dieses Felds entsprechend den Werten der Felder **Typ** und **Status** fest.
Status	Der aktuelle Status der E-Mail (Fehler, Ignoriert, Verarbeitet oder Bereit).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Protokoll (Fortsetzung)

Feld	Beschreibung
Empfangstyp	Die Art der eingehenden E-Mail (Keine, Weiterleiten, Neu oder Antwort).
Typ	Der Status der E-Mail. Die Auswahlmöglichkeiten sind: • erhalten: Der Server hat diese E-Mail erhalten. • erhalten - ignoriert: Der Server hat diese E-Mail erhalten, sie wurde jedoch von der Instanz aufgrund von Aktionen bei eingehender E-Mail ignoriert. Normalerweise handelt es sich bei diesen E-Mails entweder um Spam oder um automatische Antworten. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - fehlgeschlagen: Der Server hat versucht, die E-Mail zu senden, und ist fehlgeschlagen. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - ignoriert: Der Server hat das Senden dieser E-Mail übersprungen. Normalerweise handelt es sich hierbei um eine E-Mail, die generiert wurde, jedoch keine Empfänger-E-Mail-Adresse hatte oder eine doppelte E-Mail ist. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - bereit: Die E-Mail kann gesendet werden, wurde jedoch vom Mail-Server nicht gesendet. Normalerweise bleibt eine E-Mail nur für kurze Zeit in diesem Status. • send-translation-ready: Die E-Mail wird während der E-Mail-Übersetzung generiert und gesendet. Normalerweise bleibt eine E-Mail nur für kurze Zeit in diesem Status. • gesendet: Die E-Mail wurde von der Instanz ohne Fehler oder Probleme gesendet.
Ziel	Eine Dokument-ID-Referenz auf den Datensatz, wenn die E-Mail durch Einfügen, Aktualisieren oder Löschen eines bestimmten Datensatzes generiert wird.
Anwender	Der Name des Benutzers aus dem Benutzerdatensatz der Instanz, von der die E-Mail-Benachrichtigung gesendet wurde. **Hinweis:** Dies ist ein Zeichenfolgen-Feld.
Benachrichtigungstyp	Der Typ der Benachrichtigung. Die Auswahlmöglichkeiten lauten wie folgt: • Keiner • SMS • SMTP
UID	Die eindeutige ID der auf dem Server gespeicherten E-Mail.
Erstellt	Datum und Uhrzeit der E-Mail-Aktivität für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Gelöscht	Gibt für eingehende E-Mails an, ob die E-Mail vom E-Mail-Server gelöscht wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Protokoll (Fortsetzung)

Feld	Beschreibung
Gewichtung	Die Gewichtung der E-Mail, die die Sendepriorität relativ zu anderen Benachrichtigungen in derselben Tabelle bestimmt.
Wichtigkeit	Ein Hinweis darauf, dass die E-Mail mit einem geänderten Wichtigkeitsgrad gesendet wurde, z. B. Dringend.
Auslösendes Ereignis und Benachrichtigung	Für durch Benachrichtigungen generierte E-Mails: eine eingebettete Liste, in der das Ereignis und die Benachrichtigung gespeichert sind, durch die die E-Mail erstellt wurde.
Betreff	Der E-Mail-Betreff. Für Benachrichtigungen erstellen Sie den Betrefftext in **Systembenachrichtigung** > **E-Mail** > **Benachrichtigungen**.
Fehlerzeichenfolge	Die vom E-Mail-Server erfasste Fehlerzeichenfolge, um festzustellen, warum die E-Mail nicht gesendet wurde. Dies wird nur protokolliert, wenn die E-Mail fehlgeschlagen ist.
Empfänger	Die E-Mail-Adressen der Empfänger
Textkörper	Der Textkörper der E-Mail, der in unformatiertem HTML-Markup angezeigt wird. Verwenden Sie den zugehörigen Link „HTML-Textvorschau“, um den Nachrichtentext als gerenderten HTML-Code anzuzeigen.
Content Typ	Der E-Mail-Content Typ
Kopfzeilen	Alle in die E-Mail eingebetteten Header.

Ereignisprotokolle

Das Event-Protokoll zeichnet alle System-Events auf, die innerhalb der Now Platformauftreten.

Dieses Protokoll enthält die folgenden Informationen für alle auftretenden Events:

Ereignisprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit des Ereignisses für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Name	Name des Events, wie in der Event-Registrierung aufgeführt.
URI	HTTP-Abfrage, die das Event generiert hat.
Parm1	Event-spezifischer Wert, der vom Event und dem Empfänger abhängt.
Parm2	Event-spezifischer Wert, der vom Event und dem Empfänger abhängt.
Tabelle	Datenbanktabelle, auf die für dieses Event reagiert wurde.
Verarbeitet	Datum und Uhrzeit der Ereignisverarbeitung. Diese Zeit spiegelt das Gebietsschema des Computers wider, auf dem die Instanz ausgeführt wird.
Verarbeitungsdauer	Zeitaufwand für die Verarbeitung dieses Ereignisses in Millisekunden.
Warteschlange	Name der Prozessorwarteschlange.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importprotokolle

Das Importprotokoll zeigt Informationen in einem ausführlichen Format zu Datenimportaktivitäten innerhalb der Plattform an.

Eine detailliertere Ansicht der Import Sets, die ein bestimmtes Protokoll erstellt haben, finden Sie unter **Importsätze** > **Verlauf umwandeln**.

Dieses Protokoll enthält die folgenden Informationen für alle Importe:

Importprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit des Imports für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Ebene	Typ der angezeigten Nachricht. Für Importdateien lautet die Ebene „Information“.
Nachricht	Vom System generierte Nachricht zum Status des Imports.
Quelle	Name der externen Quelle des Imports, z. B. eine Integration.

Modul „System Diagnostics“.

Die System Diagnostics-Anwendung stellt Protokolle bereit, die sich auf die -Plattform beziehen.

Diese Protokolle sind verfügbar:

Upgradeverlauf

Verfolgt jedes Upgrade auf eine Instanz nach.

Langsame Abfragen

Bietet Einblicke, wie sich Abfragen auf die Plattformleistung auswirken. Weitere Informationen finden Sie unter Langsame Abfrageprotokolle verwenden .

Tabelle „Kunden-Updates“.

Im System vorgenommene Änderungen werden chronologisch in der Tabelle „Kunden-Updates “ [sys_update_xml] aufgezeichnet. Es gibt einige Ausnahmen, wie unten erwähnt.

Um zu dieser Tabelle zu navigieren, geben Sie sys_update_xml.list in den Navigationsfilter ein. Weitere Informationen zu Update Sets finden Sie unter System-Update Sets .

Die folgenden Informationen werden zu jeder Aktualisierung gespeichert:

Tabelle „Kunden-Updates“.

Feld	Beschreibung
Name	Ein Name, der den aktualisierten Datensatz identifiziert.
Erstellt	Datum und Uhrzeit der Erstellung des Kunden-Update-Datensatzes.
Erstellt von	Der Benutzer, der den Change durchgeführt hat.
Typ	Der Typ des Updates.
Aktualisiert	Datum und Uhrzeit der Aktualisierung des Kunden-Update-Datensatzes.
Aktualisiert von	Der Benutzer, der das Update durchgeführt hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Kunden-Updates“. (Fortsetzung)

Feld	Beschreibung
Updates	Die Häufigkeit, mit der der Datensatz aktualisiert wurde.
Zielname	Der Name des geänderten Elements.
Ansicht	Die Ansicht des Formulars, das geändert wurde, wenn es sich um eine Formularlayoutänderung handelte.
Nutzlast	Der XML-Inhalt des Datensatzes nach der Änderung.
Remote-Update-Satz	Ein Verweis auf dieses Update Set, wenn die Änderung von einem Remote-Update Set durchgeführt wurde.
Lokales Update Set	Das Update Set, dem die Änderung zugeordnet ist.

Hinweis:
Einige Anwendungsänderungen werden nicht durch Kunden-Update-Datensätze (sys_update_xml) Beispiele dargestellt:

- Arten von Metadaten, bei denen updateSynch = false ist
- Kaskadierende Änderungen an Tabellen und Feldern, z. B. Änderungen des Anzeigenamens
- Nicht aufgelöste Metadatenreferenzen aus anderen Anwendungen (führt zu keinem „Anzeigewert“ für das Element)
- sys_id ändert sich für das Zusammenfügen von Dateien
- Änderungen an Flow/Flow-Aktionen, die sys_documentation generieren können
- ua_table_license_config-Datensätze, die bei der Tabellenerstellung generiert werden
- Jobs, die im Hintergrund ausgeführt werden, z. B. Natural Language Processing
- Fälle, in denen sys_update_xml manuell geändert oder entfernt wird

Weitere Informationen finden Sie unter Changes committen .

Protokollverlauf

Das System verwendet Tabellenrotation und Tabellenerweiterung, um ältere Protokolle zu archivieren.

Standardmäßig verwendet das System den folgenden Zeitplan, um allgemeine Protokolle zu archivieren:

Gemeinsamer Protokollarchivierungszeitplan

Tabelle	Archivzeitplan	Rotationen	Typ
Ereignis [ecc_event]	Jeden Tag	7	Rotation
Warteschlange [ecc_queue]	Jeden Tag	7	Rotation
Ereignis [sysevent]	Jeden Tag	7	Rotation
Protokoll [syslog]	Jede Woche	8	Rotation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gemeinsamer Protokollarchivierungszeitplan (Fortsetzung)

Tabelle	Archivzeitplan	Rotationen	Typ
Transaktionsprotokoll [syslog_transaction]	Jede Woche	8	Rotation
E-Mail [sys_email]	Alle 30 Tage	8	Erweiterung

Verwenden Sie den Protokolldateibrowser

Die Instanz stellt die Dienstprogramme Protokolldateibrowser und Protokolldateidownload bereit.

Verwenden **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Browser** , um Systemprotokolleinträge anzuzeigen. Sie können nach Protokolldateien suchen, indem Sie die folgenden Filter verwenden:

Protokolldateibrowser

Feld	Beschreibung
Startzeit	Startdatum und -uhrzeit des zu durchsuchenden Bereichs für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Sitzungs-ID	Vom System generierte Hexadezimalzeichenfolge, die die Sitzung identifiziert, die den Protokolleintrag generiert hat.
Endzeit	Enddatum und -uhrzeit des zu durchsuchenden Bereichs für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Nachricht	Vom System generierte Beschreibung des Vorkommens.
Ebene	Typ der angezeigten Nachricht. Die Ebenen sind Debug, Fehler, Warnung und Information. Eine Warnung ist ein Fehler, der behandelt und behoben wurde. Ein Fehler ist etwas, das behoben werden muss.
Thread-Name	Vom System generierter Bezeichner des Threads, der die Protokolldatei erstellt hat.
Maximale Zeilen	Maximale Anzahl der für einen bestimmten Filter zurückgegebenen Datensätze.

Die Instanz erstellt alle 2 Tage komprimierte Archive von Systemprotokollen und löscht Protokollarchive nach 21 Tagen.

Wichtig:
Wenn ein Knoten stillgelegt wird, werden die Protokolldateien des Knotens sofort gelöscht, was bedeutet, dass sie weitere 21 Tage lang nicht archiviert werden.

Sie können Protokolldateiarchive herunterladen und mit anzeigen **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**. Wählen Sie ein Protokollarchiv aus der Liste aus, und klicken Sie dann unter *Zugehörige Links* auf **Protokoll herunterladen**, um das Archiv zu öffnen oder zu speichern.

Hinweis:
Protokolldateien sind nur für den Knoten verfügbar, bei dem Sie derzeit angemeldet sind. Um den aktuell angemeldeten Knoten anzuzeigen, navigieren Sie zu **Systemdiagnostik** > **Statistiken**.

Verwenden Sie die neue Schaltfläche **Syslog-Datensätze** anzeigen in den Formularen „Transaktion“ und „Aktive Transaktion“, um alle Systemprotokolleinträge anzuzeigen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

die während der Ausführung der Transaktion generiert wurden. Eine Transaktion kann eine beliebige Anzahl von syslog-Einträgen haben. Die mehreren syslog-Einträge für alle Transaktionen erschweren die Zuordnung einer Transaktion zu ihren jeweiligen syslog-Einträgen. Die UI-Aktion **„Syslog-Datensätze** anzeigen“ hilft bei der Zuordnung der aktiven und abgeschlossenen Transaktionen zu ihren jeweiligen Syslog-Einträgen, indem eine URL zum Abfragen der Syslog-Tabelle erstellt wird. Das Identifizieren der richtigen Syslog-Einträge für eine bestimmte Transaktion hilft beim Debuggen und Behandeln von Sicherheitsbedenken.

Verbesserte Protokollierungssicherheit

Erkunden Sie das Feld **Attribution** in den Knotenprotokollzeilen, um das Skript oder die Komponente zu identifizieren, die die Protokollnachricht generiert hat. Transaktionsstartzeilen enthalten das neue Feld, um den Typ der gestellten Anforderung zu identifizieren.

Mit den neuen Erweiterungen können Sie Folgendes erreichen:

- Verfolgen Sie den Quellersteller jeder der Protokollzeilen
- Wenn die Absenderinformationen nicht verfügbar sind, geben Sie den Java-Klassennamen und eine Zuordnung aus
- Am Anfang jeder Transaktionsposition enthält sie die Transaktions-ID und den Transaktionstyp

Verwenden Sie die Transaktions-ID jeder Protokollzeile, um die in jeder Protokollzeile angegebenen Informationen zu verstehen. Sobald Sie den Transaktionstyp identifiziert haben, erhalten Sie die Absenderinformationen für jede Protokollzeile. Sowohl der Transaktionstyp als auch die Herkunftsinformationen jeder Protokollzeile zusammen geben Ihnen die erforderlichen Quellinformationen für jede Knotenprotokollzeile.

Hinweis:
Die Skripttypen SYS_UI_MACRO und SERVICE_PORTAL_WIDGET in der Zuordnung werden nicht gemeldet.

Transaktionstypen

Im Folgenden finden Sie die Liste der Transaktionstypen:

- Liste
- Formular
- XMLHttp
- Bericht
- SOAP
- Exportieren
- Zeitplaner
- Textsuche
- Sonstige
- REST
- JSON
- AMB
- Archiv

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Batch-REST
- Instanz-Scan

Systemeigenschaften

Die folgenden Systemeigenschaften sind für die Funktion erforderlich:

- Glide.log.append.attribution: Diese Eigenschaft ist standardmäßig aktiviert. Aktiviert/deaktiviert die Attributinformationen jeder Knotenlinie
- Glide.db.log.append.classname.attribution: Diese Eigenschaft ist standardmäßig aktiviert. Aktiviert/deaktiviert die Protokollierung der Java-Klassennamenzuordnung

Vermeiden Sie Protokollmanipulationen

Konfigurieren Sie Schutzregeln für Systemprotokolltabellen, um den Umfang der Änderung und Löschung von Anwendungsprotokolldatensätzen zu begrenzen. Mit den Regeln können Sie die Protokollierung von Änderungen oder Änderungsversuchen in diesen Tabellen festlegen.

Wenn Sie security_admin sind, aktivieren Sie das Plugin „Protected Tables“ (com.glide.protected_tables), mit dem die Plattform Aktualisierungs-, Einfüge- und Löschvorgänge für die folgenden Systemprotokolltabellen einschränken kann:

- syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- syslog_app_scope
- opened_table_configuration (Konfiguration nicht änderbar)

Hinweis:
Das Plugin „com.glide.protected_tables“ bietet nur Schutz für die oben genannten Systemprotokolltabellen. Jeder Versuch, einen Datensatz zu aktualisieren, einzufügen oder zu löschen, protokolliert eine Nachricht in der Tabelle „protected_table_log“.

Weitere Informationen finden Sie unter Protokollschutz-Plugins installieren und konfigurieren.

Sie können für jede Systemprotokolltabelle eine der folgenden Protokollschutzstufen angeben.

- Versuch blockieren und protokollieren: Blockiert alle Änderungen und protokolliert den Versuch
- Nur den Versuch blockieren: Blockiert alle Änderungen und protokolliert den Versuch nicht
- Nur den Versuch protokollieren: Blockiert die Änderung nicht, protokolliert jedoch den Versuch
- Nicht blockieren und Versuch nicht protokollieren: Blockiert die Änderung nicht und protokolliert den Versuch nicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Plattform verwendet die für jede der Systemprotokolltabellen angegebenen Protokollschutzstufen, um Versuche zum Ändern eines Datensatzes nach der ursprünglichen Erstellung zu blockieren und/oder zu protokollieren.

Hinweis:
Wenn Sie security_admin sind, können Sie die standardmäßigen Protokollschutzstufen in jeder der Systemprotokolltabellen überschreiben, um sie an die Anpassungen in Ihrer Instanz anzupassen.

Alle Versuche, die Systemprotokolltabellen zu ändern, werden in der Tabelle „protected_table_log“ protokolliert.

Hinweis:
Wenn die Schutzstufe für eine Tabelle nicht angegeben ist, werden Änderungsversuche nicht in der Tabelle „protected_table_log“ protokolliert.

Um die Plugin-Vorgänge für Tabellen im Admin-Bereich zu deaktivieren, setzen Sie die Eigenschaft com.glide.security.protected_table.enabled auf false. Weitere Informationen finden Sie unter Erstellen einer Protokollschutzeigenschaft.

Protokollschutz-Plugin konfigurieren

Konfigurieren Sie die Schutzregeln für jede Tabelle und jeden Vorgang, um die Konfiguration des Protokollschutz-Plugins abzuschließen.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Geschützte Tabellen** > **Protokollschutz**.
   Die Seite „Administratorbereich“ wird angezeigt.

   Hinweis:
   Ab Release Utah ist das Plugin „Protected Tables“ standardmäßig installiert, aber deaktiviert.

2. Erhöhen Sie Ihre Rolle auf security_admin, um mit der Konfiguration des Plugins fortzufahren.

   a. Wählen Sie **Systemadministrator aus**.

   b. Wählen Sie **Rolle erweitern aus**.
   Das Dialogfeld „Rolle erhöhen“ wird angezeigt.

   c. Wählen Sie die Option security_admin aus, um Ihre Rolle zu erweitern, und wählen Sie **Aktualisieren**.

3. Konfigurieren Sie die Schutzregeln für jede Tabelle und jeden Vorgang.
   Die Schutzregeln gelten für Aktualisieren, Einfügen und Löschen. Die Schutzstufen können für einige Tabellen nicht geändert werden. Die Tabellen syslog und syslog_app_scope haben feste Werte für Aktualisierungs- und Löschschutz. Die Tabelle „protected_table_configuration“ verfügt über feste Schutzwerte für alle drei Vorgänge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für die sysevent-Tabelle kann der Einfügeschutz nicht auf „Blockieren“ festgelegt werden.

Wenn Sie „Auf **untergeordnete Tabellen anwenden** “ für syslog im vorherigen Release aktiviert hatten, werden die untergeordneten Tabellen dem Protokollschutz mit denselben Schutzregeln wie syslog beim Upgrade auf den Release Utah hinzugefügt. Dies geschieht nur für syslog, nicht für andere Tabellen.

4. Aktivieren Sie die Funktion, indem Sie den **Umschalter Protokollschutz aktivieren** aktivieren.

Hinweis:
Sie können dieses Plugin nur deaktivieren, indem Sie die Eigenschaft com.glide.security.protected_table.enabled in der Tabelle „sys_properties“ ändern.

Erstellen Sie eine Protokollschutzeigenschaft

Erstellen Sie eine Protokollschutzeigenschaft, um das Risiko einer Protokollmanipulation zu vermeiden.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Wenn die Eigenschaft `com.glide.security.protected_table.enabled` in der Liste „Systemeigenschaften“ nicht vorhanden ist, wählen Sie **Neu**.
   Das neue Systemeigenschaften-Formular wird angezeigt.
2. Füllen Sie die Details im Formular aus

Felder	Beschreibung
Name	Name der Eigenschaft com.glide.security.protected_table.enabled
Anwendung	Anwendung mit der Eigenschaft.
Beschreibung	Beschreibung der Eigenschaft
Auswahlmöglichkeiten	
Typ	Werttyp: „true“ oder „false“.
Wert	Tatsächlicher Wert der Eigenschaft
Cache ignorieren	Option zum Ignorieren des Cache-Inhalts
Privat	Option, um die Eigenschaft als privat zu definieren ○ Leserollen ○ Schreibrollen

3. Wählen Sie **Absenden** aus, um die Eigenschaft zu erstellen.

Log Export Service (LES)

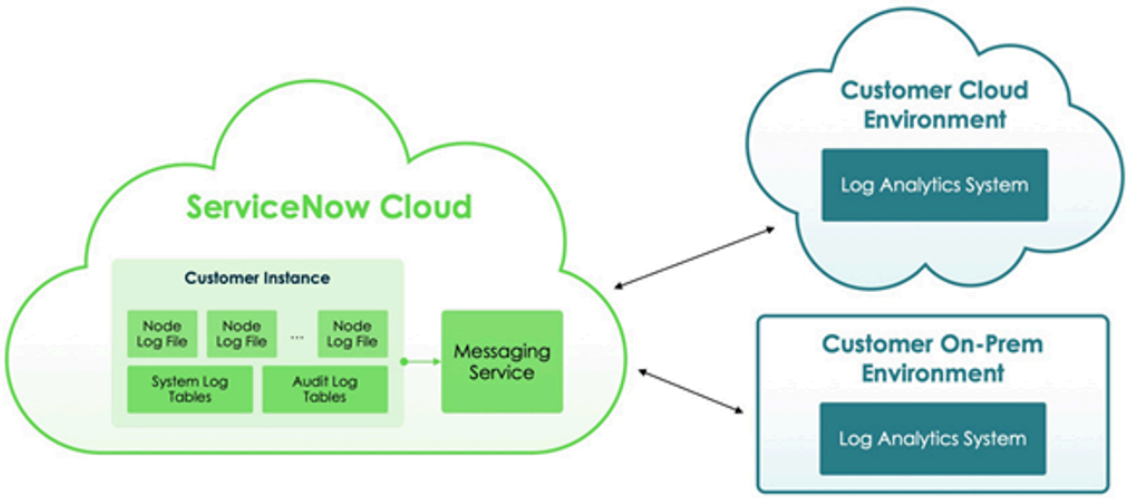
Log Export Service Mit (LES) können Sie Ihre Instanzsystem- und Anwendungsprotokolle nahtlos in die Sicherheitsanalysetools Ihres Unternehmens exportieren. Der Service bietet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine hoch skalierbare und nahezu in Echtzeit erfolgende Integration mit Ihren Analysetools, die einfach einzurichten und zu warten ist.

Mit dem Integrationstool können Sie Ihre Analyselösungen für Folgendes nutzen:

- Erkennen Sie ServiceNow Sicherheitsbedrohungen und analysieren Sie Security Incidents
- Beheben und optimieren Sie die Leistung der App ServiceNow .
- Überwachen und optimieren Sie die Benutzer-Experience von ServiceNow .



LES leitet eine Kopie der Protokoll-Events an Hermes Messaging-Serviceweiter, sobald sie generiert werden.

Hermes Messaging-Service ist ein Multi-Mandanten-, Multi-Cluster-, Datentransport- und Warteschlangenservice, der auf Apache Kafka] basiert und es Ihrer Instanz ermöglicht, große Mengen von Kafka-Events zu erzeugen und zu verbrauchen. Hermes Messaging-Service ist eine Now Platform-Fähigkeit, die als Teil von Stream Connect für Apache Kafka, Log Export Service (LES) und Instanzübergreifende Datenreplikation (IDR) verfügbar ist.

Die externen Protokollanalysesysteme, entweder in der Cloud oder lokal, können die Protokoll-Events aus dem Hermes Messaging-Serviceverwenden und verarbeiten. LES bietet drei Konnektivitätsoptionen zum Verwenden der Protokolle:

- Dedizierter MID-Server: Ein dedizierter MID-Server wird lokal oder in der Cloud installiert, der automatisch eine Verbindung zu Hermes Messaging-Serviceherstellt, kontinuierlich Protokoll-Events abruft und sie dann über eine REST-Verbindung an Protokollanalysetools weiterleitet.
- Nutzen Sie den Kafka-Connector aus Ihrer Protokollanalyselösung (z. B. Splunk): Ein Kafka-Connector aus dem Protokollanalyseprodukt Ihrer Wahl wird lokal oder in der Cloud installiert, der automatisch eine Verbindung zu Hermes Messaging-Serviceherstellt, Protokoll-Events kontinuierlich abruft und dann veröffentlicht sie an Protokollanalysetools weiter.
- Direkt aus Ihrem Kafka-System: Ihr Kafka-System stellt eine direkte Verbindung mit dem Hermes Messaging-Service her und verwendet die nativen Kafka-Protokollbefehle und die Konnektivität, um Protokoll-Events daraus abzurufen.

Um LES zu konfigurieren und zu verwalten, müssen Sie es aus dem installieren ServiceNow Store . Die LES-Anwendung bietet Guided Setups, die Sie bei der Installation des Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

unterstützen, Seiten zum Konfigurieren des Service (Protokollquellen, Verbraucher und Ziele) und Berichte, um die Erstellung und Nutzung von Protokollen zu verstehen.

Hinweis:
Sie können auch eine neue Quellkonfiguration erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Protokollquellenkonfiguration.

Log Export Service Rollen

Log Export Service wird mit diesen Rollen installiert.

Anwendungsadministrator [sn_logstoanalytics.admin]

Weitere Informationen zum Verwalten von Pro-Benutzer-Abonnements finden Sie unter . Wenden Sie sich an Ihren Kundenbetreuer.

Diese Rolle wird zusammen mit der LES-Anwendung installiert und ermöglicht Nicht-Administratoren die Verwendung der Anwendung.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Erweitert

Gibt an, ob die Rolle eine erhöhte Rolle ist. Erweiterte Rollen werden keinen Benutzern oder Gruppen zugewiesen und müssen durch Erhöhung verwendet werden. Weitere Informationen finden Sie unterFühren Sie eine Erhöhung auf eine privilegierte Rolle durch.

Nein.

Besondere Überlegungen

Keine.

Systemadministrator [admin]

Weitere Informationen zum Verwalten von Pro-Benutzer-Abonnements finden Sie unter . Wenden Sie sich an Ihren Kundenbetreuer.

Die Administratorrolle ist für die Einrichtung der LES Store-Anwendung erforderlich.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

- sn_templated_snip.template_snippet_admin
- sn_employee.admin
- taxonomy_admin
- sn_ace.ace_user
- sn_hr_sp.esc_admin

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Erweitert

Gibt an, ob die Rolle eine erhöhte Rolle ist. Erweiterte Rollen werden keinen Benutzern oder Gruppen zugewiesen und müssen durch Erhöhung verwendet werden. Details finden Sie unter Führen Sie eine Erhöhung auf eine privilegierte Rolle durch.

Nein.

Besondere Überlegungen

Keine.

Protokollquellen

Log Export Service (LES) kann Protokollquellen aus einigen Systemprotokolltabellen, der Audit-Tabelle und Anwendungsknoten-Protokolldateien exportieren.

Im Folgenden finden Sie die Protokollquellen, die von LES exportiert werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Systemprotokolltabellen
  - syslog-Tabelle: Zeigen Sie Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse an, z. B. Speichernutzung auf dem Servercomputer
  - syslog_transaction-Tabelle: Alle Browseraktivitäten für eine Instanz anzeigen
  - Tabelle sys_outbound_http_log: Zeigt alle Anforderungen und Antworten für ausgehende Webservices wie REST und SOAP an
- Audit-Tabelle: Verwenden Sie die sys_audit-Tabellenansicht, um Änderungen an zu prüfenden Tabellen vorzunehmen
- Anwendungsknoten-Protokolldateien: Verwenden Sie die localhost-Protokolldateien, um Anwendungsknotenfehler anzuzeigen. Ihre Instanz verfügt über mehrere Knoten, und jeder Knoten verfügt über mehrere Protokolldateien.

Unter Systemprotokolle erfahren Sie mehr über das Schema und den Zweck der oben genannten Protokollquellen.

Erstellen Sie eine Protokollquellenkonfiguration

Regulieren und legen Sie Filter für die weiterzuleitenden Protokolle fest, indem Sie eine Protokollquellenkonfiguration erstellen.

Vorbereitungen

Erforderliche Rolle: admin oder sn_logstoanalytics.admin

Prozedur

1. Navigieren zu **Alle** > **Protokollexportservice**.
   Eine Liste der Quellkonfigurationen wird angezeigt.
2. Wählen Sie **Neu** aus, wenn Sie eine neue Quellkonfiguration erstellen möchten.
   Sie können auch eine vorhandene Quellkonfiguration auswählen, wenn Sie sie ändern möchten.
   Das Quellformular wird angezeigt.
3. Füllen Sie die Felder des Formulars aus.

Quellformular

Felder	Beschreibung
Quelltyp	Typen der Protokollquellen ○ Knotenprotokoll ○ Tabelle Weitere Informationen finden Sie unter Protokollquellen.
Protokollebene	Eine Reihe von Standardprotokollierungsebenen, die zur Steuerung der Protokollierungsausgabe verwendet werden können. Gemäß der Konvention leitet jede Ebene Protokolle mit gleichem oder höherem Schweregrad weiter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Hinweis: Dieses Feld ist nur sichtbar, wenn eine der folgenden Bedingungen erfüllt ist. ○ Wenn Sie Knotenprotokoll als Quelltyp auswählen ○ Wenn Sie Tabelle als Quelltyp auswählen und die Tabelle syslog ist
Akzeptiert	Gibt das Format an, in dem die Protokolle an Hermes weitergeleitet werden. Sie können entweder als JSON oder als Nur-Text gesendet werden.
Tabelle	Auswahl der Tabelle für Tabellentypprotokolle. **Hinweis:** Dieses Feld ist nur sichtbar, wenn Sie Tabelle als Quelltyp auswählen.
Filtertyp	Bedingungen zum selektiven Weiterleiten von Protokollen. **Hinweis:** Dieses Feld ist nur sichtbar, wenn Sie entweder syslog oder sys_audit als Tabelle auswählen.

4. Wählen Sie Absenden aus, um eine neue **Quellkonfiguration** zu erstellen.

Kafka-Verbraucher

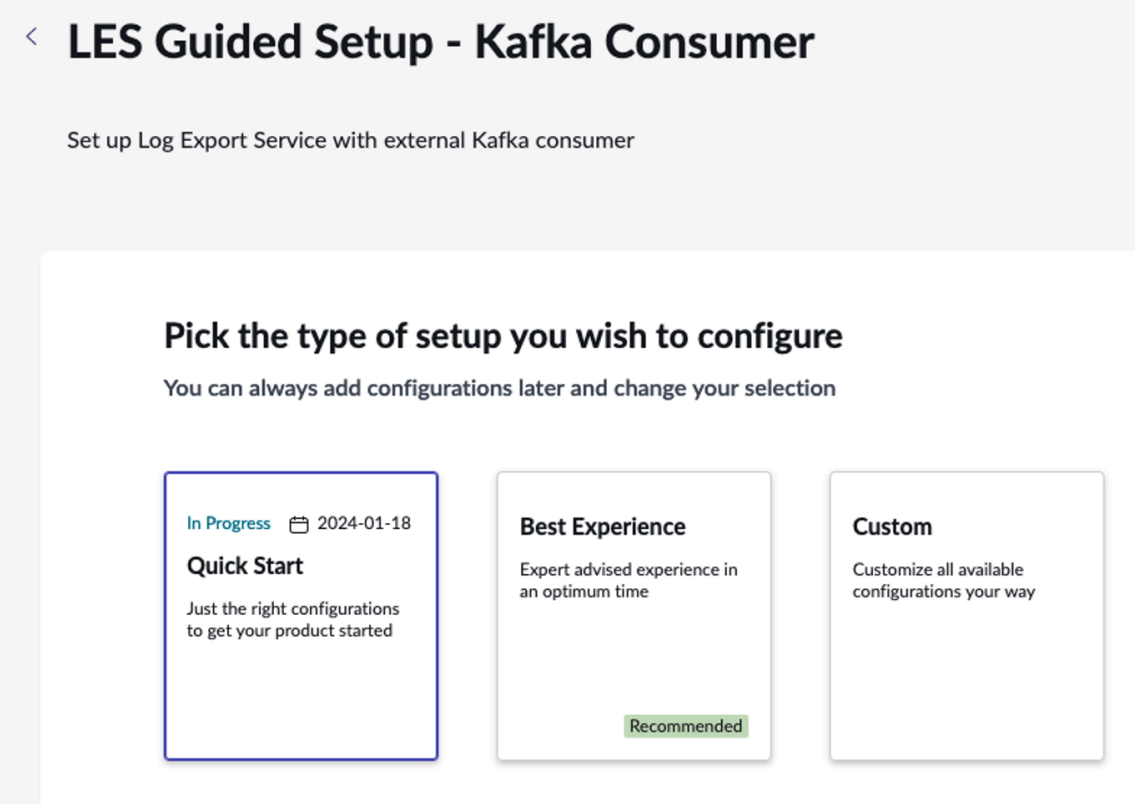
Verwenden Sie das Guided Setup, um die Erstkonfiguration von LES zu durchlaufen. Das Guided Setup unterstützt Sie bei der Planung der Einführung des Produkts und der Durchführung der grundlegenden Konfiguration für die Veröffentlichung.

Das geführte Setup organisiert Konfigurationsaktivitäten in Kategorien. Jede Kategorie enthält Informationen wie Planungsleitfäden, Schritte vor dem Setup und Links zu nützlichen Hilfeinhalten. Kategorien stellen auch eine Reihe von Links zu den Seiten in Ihrer Instanz bereit, auf denen Sie die Konfiguration durchführen. Im Guided Setup-Prozess wird nachverfolgt, was Sie abgeschlossen haben, sodass Sie anhalten und dort wieder beginnen können, wo Sie aufgehört haben.

Guided Setup-Homepage

Die Homepage für das geführte Setup enthält eine Übersicht über die Konfigurationstypen für das geführte Setup. Sie können den Typ des geführten Setups auswählen und **Fortfahren** wählen, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



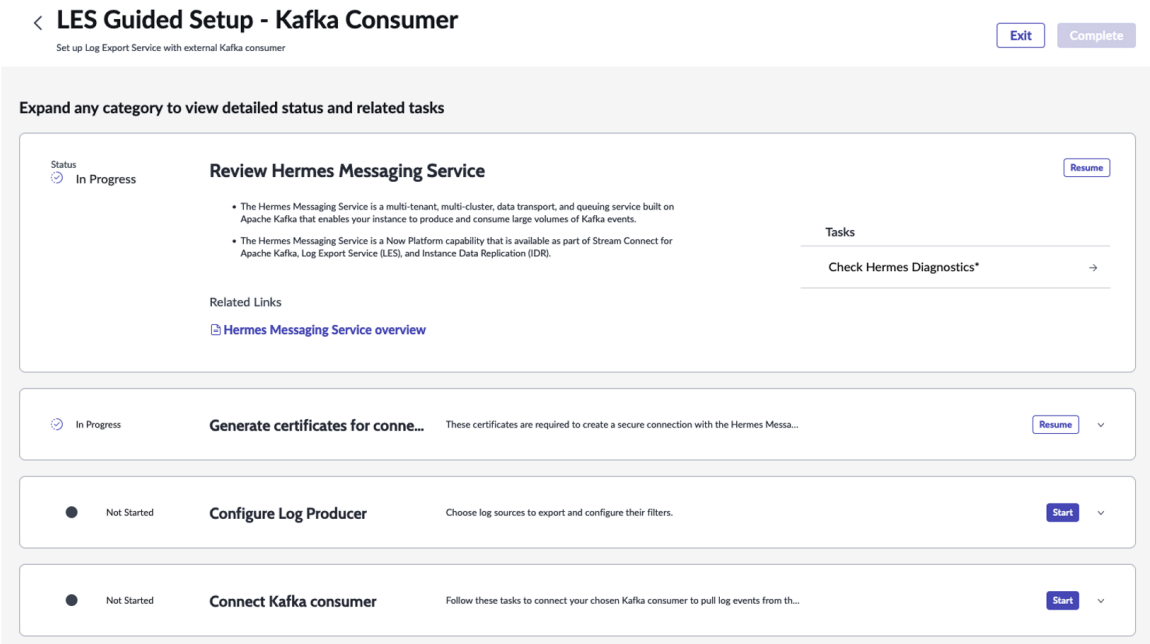
Alle drei Setups auf dieser Seite, Schnellstart/Beste Experience/Benutzerdefiniert, bieten die gleichen Aufgaben und Funktionen. Es ist erforderlich, dass, um die Integration zwischen der ServiceNow-Instanz und dem Zielprotokoll-Analysetool mit dem jeweiligen Administrator zu koordinieren. Der Log Analytics-Administrator muss sein Tool so konfigurieren, dass eine sichere Verbindung zur ServiceNow-Instanz hergestellt wird. Es wird empfohlen, das Dokument Set up a secure connection to the Hermes Messaging Service vorab für den Log Analytics-Administrator freizugeben. Auch wenn Sie eine Aufgabe als abgeschlossen markiert haben, können Sie zurückgehen und sie wieder als „In Bearbeitung“ markieren. Klicken Sie dazu zuerst auf das Feld **Bearbeiten** in der oberen rechten Ecke für die Kategorie. Klicken Sie dann auf das Kontrollkästchen **Bearbeiten** für die Aufgabe, die Sie deaktivieren möchten. Das **Kontrollkästchen Als abgeschlossen** markieren wird nicht mehr markiert.

Guided Setup-Kategorienseite

Die Kategorienseite enthält eine Übersicht und Beschreibungen der Kategorien und zugehörigen Aufgaben. Sie können entweder auf den Dropdown-Pfeil klicken, um Informationen zur Kategorie anzuzeigen, oder auf die Schaltfläche Start, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Führen Sie die Aufgaben unter jeder Kategorie aus, indem Sie die Setup-Anweisungen befolgen.

Geführtes Setup für Kafka-Verbraucher

Implementieren Sie die folgenden Schritte für ein vollständiges Guided Setup für Kafka-Verbraucher.

Vorbereitungen

Navigieren zu **Log Export Service (LES)** > **Kafka-Verbraucher** > **Geführtes Setup**. Wählen Sie den Setup-Typ aus, den Sie konfigurieren möchten, und klicken Sie auf **Fortfahren**.

Erforderliche Rolle: admin

Prozedur

1. Überprüfung des Hermes-Messaging-Service: Überprüfen Sie die folgenden Informationen, um die Hermes-Diagnose zu bestehen.
   - Setup-Informationen: Die folgenden Bootstrap-Informationen werden verwendet, um eine Verbindung zum Hermes Messaging Service herzustellen. „Producer Bootstrap“ ist die Verbindung, die zum Senden von Nachrichten an Hermes verwendet wird, und „Consumer Bootstrap 1 & 2“ wird zum Abrufen von Nachrichten von Hermes verwendet.
     - Hersteller-Bootstrap
     - Verbraucher-Bootstrap 1
     - Verbraucher-Bootstrap 2
   - Instanz-PKI: Die Komponente „Instance Public Key Infrastructure“ (PKI) ermöglicht es einer ServiceNow-Instanz, als Aussteller in einer X.509-Vertrauenshierarchie zu fungieren.
   - Bootstrap-Konnektivität: Klicken Sie auf **Test ausführen**, um sicherzustellen, dass der externe Client eine Verbindung zu den definierten Instanzports (Ersteller und Verbraucher) herstellen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Instanzkonnektivität: Klicken Sie auf **Test ausführen**, um sicherzustellen, dass die Instanz Nachrichten senden und empfangen kann.
- Themen anzeigen: Klicken Sie auf das aufgelistete Thema, um den Zeitstempel der letzten bekannten Nachricht abzurufen.

2. Generieren von Zertifikaten für eine sichere Verbindung mit dem Hermes-Messaging-Service und Abrufen von Protokoll-Events daraus

   Sie werden diese Zertifikate verwenden, wenn Sie eine Verbindung zu Ihrem externen System herstellen.

   Richten Sie eine sichere Verbindung zum Hermes-Messaging-Service ein. Weitere Informationen finden Sie unter Set up a secure connection to the Hermes Messaging Service. Sie benötigen diese Zertifikate für die Authentifizierung und Autorisierung auf dem Client, der die Protokolle von Hermes abruft.

   Hinweis:
   Für diesen Schritt sind die Rollen admin oder Hermes_admin erforderlich.

3. Protokollersteller konfigurieren: Wählen Sie Protokollquellen aus, um sie zu exportieren, und konfigurieren Sie ihre Filter.
   Führen Sie die folgenden Aufgaben aus, um den Protokollersteller zu konfigurieren.

   - Konfigurieren Sie Protokollquellen für den Export: Erstellen Sie einen Quelldatensatz für jede der Protokollquellen, die Sie exportieren möchten.

     Hinweis:
     Die Rollen admin oder sn_logstoanalytics.admin sind erforderlich, um diesen Schritt abzuschließen

     a. Klicken Sie oben rechts auf **Neu**

     b. Wählen Sie einen Quelltyp aus

     c. Wählen Sie die entsprechenden Filter für den ausgewählten Quelltyp aus

     Hinweis:
     Filter unterscheiden sich je nach ausgewähltem Quelltyp

     d. Klicken Sie auf Aktualisieren.
     Nach erfolgreicher Erstellung wird der Name des Hermes-Themas angezeigt, in das diese Protokollquelle exportiert wird. Notieren Sie sich den Themennamen. Sie benötigen ihn später bei der Konfiguration Ihres Protokollverbrauchersystems. Das Feld Aktiv steuert, ob diese Protokollquelle exportiert wird oder nicht. Wenn Fehler angezeigt werden, kehren Sie zur Aufgabe „Hermes-Diagnose überprüfen“ zurück, und überprüfen Sie den Hermes-Status.

   - Protokollersteller validieren: Sobald Sie eine Quelle erstellt haben, aus der Protokolle erstellt werden sollen, können Sie Live-Protokolldatensätze im Thema mithilfe von anzeigen **Hermes Messaging Service** > **Hermes-Themeninspektor**.

     a. Wählen Sie Externe Themen aus

     b. Klicken Sie auf Listenthemen

     c. Wählen Sie die Zeile mit Ihrem Thema aus dem vorherigen Schritt aus (aufgelistet in Quellen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Passen Sie das Startdatum der Nachricht an, falls erforderlich

e. Klicken Sie auf **Ansicht**, um eine Protokollnachricht anzuzeigen, die in das Thema exportiert wurde

4. Kafka-Verbraucher verbinden: Befolgen Sie diese Aufgaben, um den ausgewählten Kafka-Verbraucher zu verbinden und Protokoll-Events aus Hermes abzurufen.

- Kafka-Verbraucher identifizieren: Je nach Log Analytics-Architektur haben Sie zwei Optionen.
  - Wenn Sie ein eigenes Kafka-System haben und dieses für die Protokollzusammenfassung auswählen, können Sie über das native Kafka-Protokoll eine direkte Verbindung zum Hermes Messaging Service herstellen.
  - Wenn Sie Ihr Protokollanalysetool direkt mit dem Hermes-Messaging-Service verbinden möchten, müssen Sie einen Kafka-Connector bereitstellen, der von Ihrem Protokollanalysesystem unterstützt wird (d. h. Splunk Connect für Kafka).

  Hinweis:
  In beiden Fällen müssen Sie mit dem Administrator für diese Systeme zusammenarbeiten, um die Verbindung mit dem Hermes Messaging Service zu koordinieren.

- Hermes-Zertifikate in das Kafka-Verbrauchersystem importieren: Melden Sie sich bei Ihrem Kafka-Verbrauchersystem an, und stellen Sie sicher, dass Sie über die entsprechenden Administratorberechtigungen verfügen, um es zu konfigurieren und eine Verbindung mit einem externen System herzustellen. Importieren Sie die in der Aufgabe „Sichere Verbindung zum Hermes-Messaging-Service einrichten“ generierten Zertifikate in Ihren Kafka-Connector oder Kafka-Server. Befolgen Sie die Anweisungen in der Dokumentation für den von Ihnen ausgewählten Kafka-Verbraucher.
- Kafka-Prozesse konfigurieren: Der Hermes Messaging Service ist auf hohe Verfügbarkeit ausgelegt. Zwei Prozesse sind erforderlich, um Nachrichten von Hermes zu verarbeiten. Zwei Prozesse sind erforderlich, da Hermes ein Paar Kafka-Cluster für Failover-Zwecke verwendet. Wenn ein Cluster ausfällt, werden Daten für den anderen Hermes Kafka-Cluster generiert.

  In Ihrem Kafka-Verbrauchersystem müssen Sie zwei separate Verbraucherprozesse erstellen, um eine Verbindung zu beiden Hermes Kafka-Clustern herzustellen. Für beide Prozesse geben Sie dasselbe Hermes Kafka-Thema an, müssen jedoch zwei separate Bootstrap-Adressen konfigurieren:

  - <instance_name>.service-now.com:4100,<instance_name>.service-now.com:4101,<instance_name>.service-now.com:4102,<instance_name>.service-now.com:4103
  - <instance_name>.service-now.com:4200,<instance_name>.service-now.com:4201,<instance_name>.service-now.com:4202,<instance_name>.service-now.com:4203

  Wichtige Hinweise:

  - Wenn Sie von externen Systemen aus auf das Kafka-Thema zugreifen, müssen Sie „snc“ voranstellen.<instance name> .“ zu dem Thema, an das die Protokolle weitergeleitet werden.
  - Konfigurieren Sie jeden Verbraucher mit derselben Kafka-Verbrauchergruppen-ID.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Installieren Sie Ihre Schlüsselspeicher- und Truststore-Dateien an einem Speicherort, auf den Ihre Verbraucher zugreifen können.
- Wenn Ihre Verbraucher dies benötigen, geben Sie die Eigenschaften der Kafka-JSON-Konverter an, um Schemas zu deaktivieren: „key.converter.schemas.enable=false“, „value.converter.schemas.enable=false“

○ Überprüfen, ob Kafka-Verbraucher Protokolle aus Hermes abrufen: Verifizieren Sie in Ihrem ausgewählten Kakfa-Verbraucher, dass Sie Protokoll-Events aus dem Hermes-Messaging-Service abrufen können.

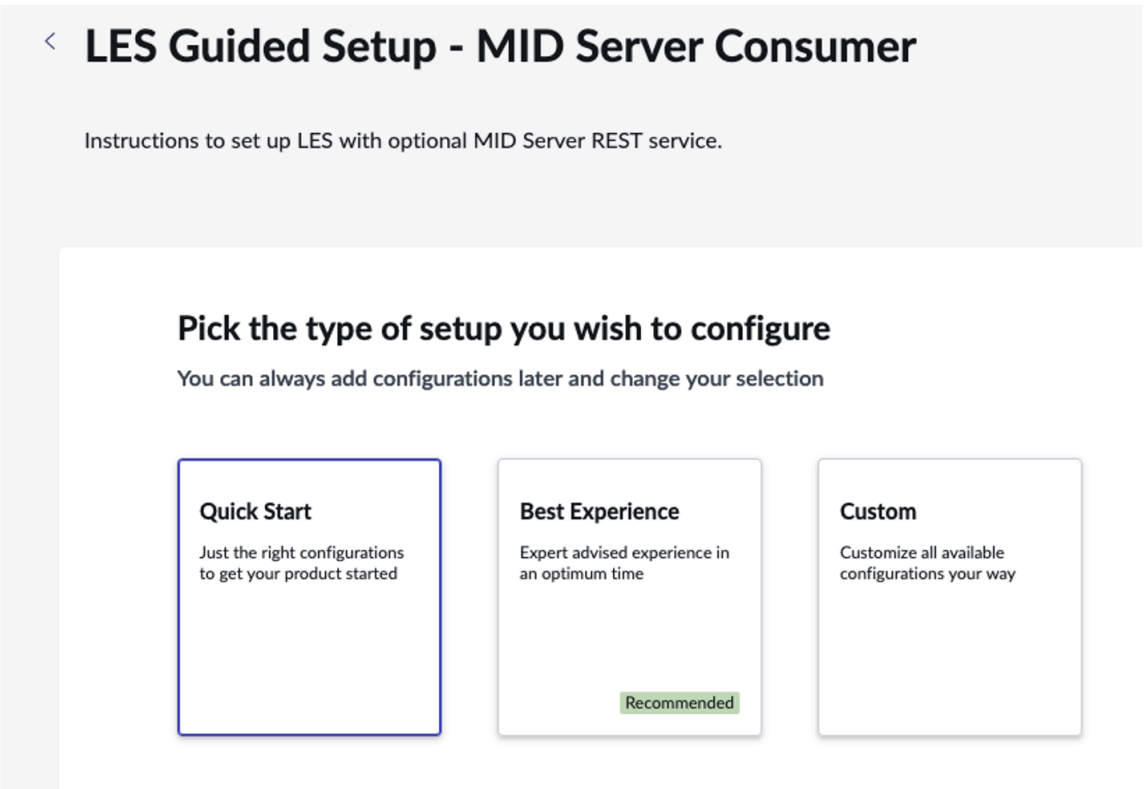
MID-Server-Verbraucher

Verwenden Sie das Guided Setup, um die Erstkonfiguration von LES zu durchlaufen. Das Guided Setup unterstützt Sie bei der Planung der Einführung des Produkts und der Durchführung der grundlegenden Konfiguration für die Veröffentlichung.

Das geführte Setup organisiert Konfigurationsaktivitäten in Kategorien. Jede Kategorie enthält Informationen wie Planungsleitfäden, Schritte vor dem Setup und Links zu nützlichen Hilfeinhalten. Kategorien stellen auch eine Reihe von Links zu den Seiten in Ihrer Instanz bereit, auf denen Sie die Konfiguration durchführen. Im Guided Setup-Prozess wird nachverfolgt, was Sie abgeschlossen haben, sodass Sie anhalten und dort wieder beginnen können, wo Sie aufgehört haben.

Guided Setup-Homepage

Die Homepage für das geführte Setup enthält eine Übersicht über die Konfigurationstypen für das geführte Setup. Sie können den Typ des geführten Setups auswählen und **Fortfahren** wählen, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.



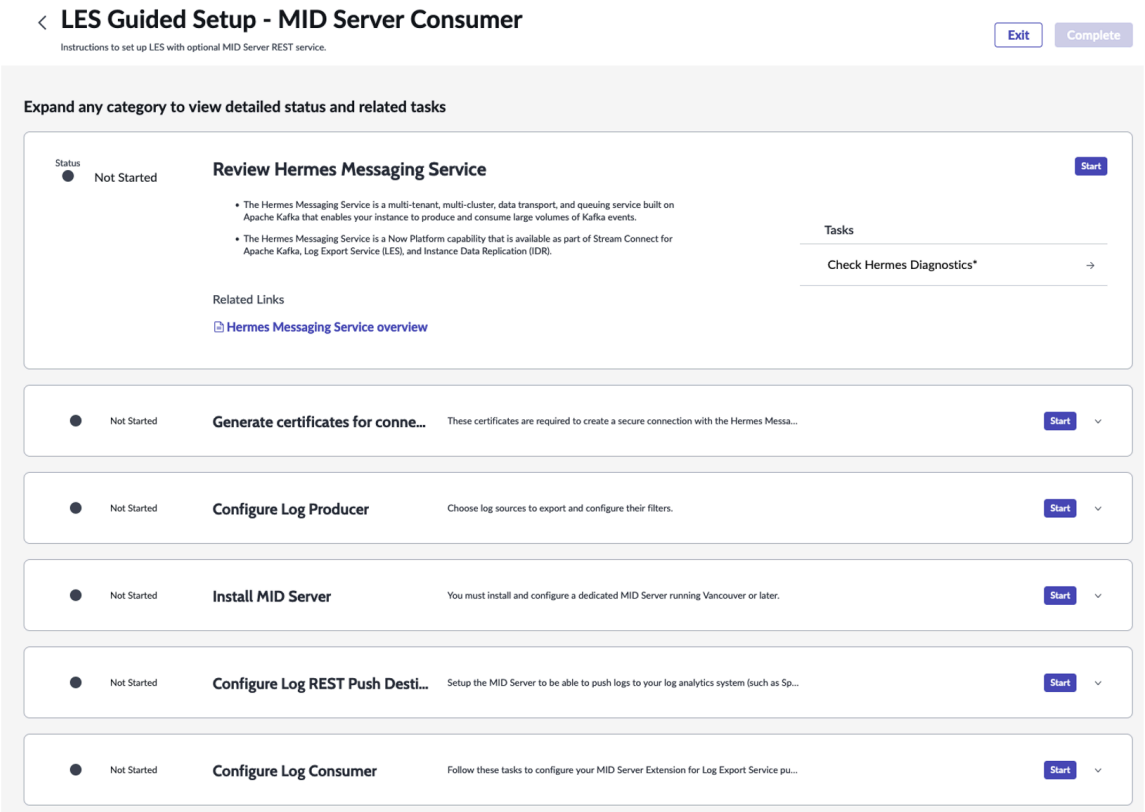
Alle drei Setups auf dieser Seite, Schnellstart/Beste Experience/Benutzerdefiniert, bieten die gleichen Aufgaben und Funktionen. Ein dedizierter MID Server ist erforderlich, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

kontinuierlich Protokolle von Ihrer Instanz an Ihr Protokollanalysesystem zu streamen. Der MID Server benötigt ein einmaliges Setup, um eine sichere Verbindung zum Hermes Messaging Service herzustellen. Auch wenn Sie eine Aufgabe als abgeschlossen markiert haben, können Sie zurückgehen und sie wieder als „In Bearbeitung“ markieren. Klicken Sie dazu zuerst auf das Feld **Bearbeiten** in der oberen rechten Ecke für die Kategorie. Klicken Sie dann auf das Kontrollkästchen **Bearbeiten** für die Aufgabe, die Sie deaktivieren möchten. Das Feld **Als abgeschlossen** markieren wird nicht mehr markiert.

Guided Setup-Kategorienseite

Die Kategorienseite enthält eine Übersicht und Beschreibungen der Kategorien und zugehörigen Aufgaben. Sie können entweder auf den Dropdown-Pfeil klicken, um Informationen zur Kategorie anzuzeigen, oder auf **Start** klicken, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.



Führen Sie die Aufgaben unter jeder Kategorie aus, indem Sie die Setup-Anweisungen befolgen.

Guided Setup für MID Server-Verbraucher

Implementieren Sie die folgenden Schritte für ein vollständiges Guided Setup für MID Server-Verbraucher.

Vorbereitungen

Navigieren zu **Log Export Service (LES)** > **MID-Server-Verbraucher** > **Geführtes Setup**. Wählen Sie den Setup-Typ aus, den Sie konfigurieren möchten, und klicken Sie auf **Fortfahren**.

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Überprüfung des Hermes-Messaging-Service: Überprüfen Sie die folgenden Informationen, um die Hermes-Diagnose zu bestehen.
   - Setup-Informationen: Die folgenden Bootstrap-Informationen werden verwendet, um eine Verbindung zum Hermes Messaging Service herzustellen. „Producer Bootstrap“ ist die Verbindung, die zum Senden von Nachrichten an Hermes verwendet wird, und „Consumer Bootstrap 1 & 2“ wird zum Abrufen von Nachrichten von Hermes verwendet.
     - Hersteller-Bootstrap
     - Verbraucher-Bootstrap 1
     - Verbraucher-Bootstrap 2
   - Instanz-PKI: Die Komponente „Instance Public Key Infrastructure“ (PKI) ermöglicht es einer ServiceNow-Instanz, als Aussteller in einer X.509-Vertrauenshierarchie zu fungieren.
   - Bootstrap-Konnektivität: Klicken Sie auf **Test ausführen**, um sicherzustellen, dass der externe Client eine Verbindung zu den definierten Instanzports (Ersteller und Verbraucher) herstellen kann.
   - Instanzkonnektivität: Klicken Sie auf **Test ausführen**, um sicherzustellen, dass die Instanz Nachrichten senden und empfangen kann.
   - Themen anzeigen: Klicken Sie auf das aufgelistete Thema, um den Zeitstempel der letzten bekannten Nachricht abzurufen.
2. Generieren von Zertifikaten für eine sichere Verbindung mit dem Hermes-Messaging-Service und Abrufen von Protokoll-Events daraus

   Richten Sie eine sichere Verbindung zum Hermes-Messaging-Service ein. Weitere Informationen finden Sie unter Set up a secure connection to the Hermes Messaging Service . Sie benötigen diese Zertifikate für die Authentifizierung und Autorisierung auf dem Client, der die Protokolle von Hermes abruft.

   Hinweis:
   Für diesen Schritt sind die Rollen admin oder Hermes_admin erforderlich.

3. Protokollersteller konfigurieren: Wählen Sie Protokollquellen aus, um sie zu exportieren, und konfigurieren Sie ihre Filter.
   Führen Sie die folgenden Aufgaben aus, um den Protokollersteller zu konfigurieren.
   - Konfigurieren Sie Protokollquellen für den Export: Erstellen Sie einen Quelldatensatz für jede der Protokollquellen, die Sie exportieren möchten.

     Hinweis:
     Die Rollen admin oder sn_logstoanalytics.admin sind erforderlich, um diesen Schritt abzuschließen

     a. Klicken Sie oben rechts auf **Neu**

     b. Wählen Sie einen Quelltyp aus

     c. Wählen Sie die entsprechenden Filter für den ausgewählten Quelltyp aus

     Hinweis:
     Filter unterscheiden sich je nach ausgewähltem Quelltyp

     d. Klicken Sie auf Aktualisieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach erfolgreicher Erstellung wird der Name des Hermes-Themas angezeigt, in das diese Protokollquelle exportiert wird. Notieren Sie sich den Themennamen. Sie benötigen ihn später bei der Konfiguration Ihres Protokollverbrauchersystems. Das Feld Aktiv steuert, ob diese Protokollquelle exportiert wird oder nicht. Wenn Fehler angezeigt werden, kehren Sie zur Aufgabe „Hermes-Diagnose überprüfen“ zurück, und überprüfen Sie den Hermes-Status.

- Protokollersteller validieren: Sobald Sie eine Quelle erstellt haben, aus der Protokolle erstellt werden sollen, können Sie Live-Protokolldatensätze im Thema mithilfe von anzeigen **Hermes Messaging Service** > **Hermes-Themeninspektor**.

  a. Wählen Sie Externe Themen aus

  b. Klicken Sie auf Listenthemen

  c. Wählen Sie die Zeile mit Ihrem Thema aus dem vorherigen Schritt aus (aufgelistet in Quellen).

  d. Passen Sie das Startdatum der Nachricht an, falls erforderlich

  e. Klicken Sie auf **Ansicht**, um eine Protokollnachricht anzuzeigen, die in das Thema exportiert wurde

4. MID Server installieren: Sie müssen einen dedizierten MID Server mit Vancouver oder höher installieren und konfigurieren.
Führen Sie die folgenden Aufgaben aus, um den MID Server zu installieren.

- Dedizierten MID Server installieren: Der vom Log Export Service verwendete MID Server sollte nur für diesen Zweck dediziert sein und es darf nicht erwartet werden, dass er andere Prozesse ausführt. Dies ist wichtig, um sicherzustellen, dass exportierte Protokollnachrichten rechtzeitig an Ihren REST-Endpunkt übermittelt werden. Sie können den neuen MID Server entweder mit Use MID Server guided setup installieren oder manuell installieren. Befolgen Sie für die manuelle Installation zuerst die Dokumentation Configure MID Server network connectivity und anschließend die Dokumentation Installing the MID Server .
- MID Server validieren: Sie müssen den MID Server nach der Installation manuell validieren, damit er Automatisierungsaufgaben ausführen kann. Informationen zur Validierung des dedizierten MID Servers für LES finden Sie unter Validate the MID Server

5. Push-Ziel für Protokoll-REST konfigurieren: Richten Sie den MID Server so ein, dass Protokolle an Ihr Protokollanalysesystem (z. B. Splunk) übertragen werden können.
Führen Sie die folgenden Aufgaben aus, um das REST-Push-Ziel des Protokolls zu konfigurieren.

- MID-Eigenschaften hinzufügen: Sie müssen MID Server-Eigenschaften hinzufügen, damit eine Verbindung zu Hermes hergestellt werden kann. Navigieren Sie zu **MID Server** >**Eigenschaften**, und legen Sie die entsprechenden Werte für jede der unten aufgeführten Eigenschaften fest.

Name	Wert
mid.les.kafka.ssl.truststore.password	<password>
mid.les.kafka.ssl.keystore.password	<password>
mid.les.kafka.ssl.key.password	<password>
mid.les.kafka.ssl.truststore.location	<your_path>/<truststore> .p12
mid.les.kafka.ssl.keystore.location	<your_path>/<keystore> .p12
mid.les.kafka.ssl.truststore.type	PKCS12

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Wert
mid.les.kafka.ssl.keystore.type	PKCS12
mid.les.kafka.client.id	<instance_name>
mid.les.kafka.group.id	snc<instance_name> .Gruppe1
mid.les.kafka.bootstrap.server	<instance_name>.<domain> :4100, . :4101, . :4102, . :4103
mid.les.kafka.set2.bootstrap.server	<instance_name>.<domain> :4200, . :4201, . :4202, . :4203

Befolgen Sie diese Hinweise, um einige der oben genannten Werte zu erhalten

- <password>ist das Passwort, das Sie für den Schlüsselspeicher und den Truststore festgelegt haben
- <your_path>ist der Dateipfad zu dem Verzeichnis, in dem Sie die heruntergeladenen Schlüsselspeicher- und Truststore-Dateien aufbewahren. Die Zertifikate müssen sich auf dem Server befinden, auf dem Sie MID ausführen
- <instance_name>ist der Name Ihrer ServiceNow-Instanz. Wenn Sie sich nicht sicher sind, finden Sie sie in der Tabelle „sys_properties“.
- Sie können die Werte für mid.les.kafka.bootstrap.servers und mid.les.kafka.set2.bootstrap.servers von der Seite „Hermes-Diagnose“ abrufen. Navigieren zu **Hermes Messaging Service** > **Diagnosen** und kopieren Sie die Zeichenfolgen unter Consumer Bootstrap 1 bzw. Consumer Bootstrap 2.

◦ Ziel konfigurieren: Erstellen Sie einen neuen Zielkonfigurationsdatensatz, der den REST-Endpunkt definiert, an den diese Erweiterung Protokolle weiterleitet.

Hinweis:
Die Rollen admin oder sn_logstoanalytics.admin sind erforderlich, um diesen Schritt abzuschließen.

a. Navigieren zu **Log Export Service (LES)** > **Zielkonfigurationen**

b. Erstellen Sie einen neuen Konfigurationsdatensatz

c. Geben Sie die URL für den gewünschten Endpunkt für die exportierten Protokollquellen an

d. Suchen Sie nach oder erstellen Sie neue Anmeldeinformationen, um eine Verbindung zu Ihrem Endpunkt herzustellen. Beachten Sie beim Erstellen von Anmeldeinformationen für Ihren Endpunkt, dass nur die folgenden Anmeldeinformationstypen mit LES gültig sind: Standardauthentifizierung, OAuth, API-Schlüssel

e. Suchen oder erstellen Sie ein neues Transformationsskript. Wir liefern mit dem vordefinierten Skript **SplunkTransform** for Splunk

6. LOG-Verbraucher konfigurieren: Führen Sie diese Aufgaben aus, um Ihre MID Server-Erweiterung für Log Export Service-Zwecke zu konfigurieren.

◦ LES-Verbraucherkontext konfigurieren: In diesem Schritt aktualisieren Sie den LES-Verbraucherdatensatz, sodass er auf dem dedizierten MID-Server ausgeführt wird, den Sie gerade für den Log Export Service installiert haben. Navigieren zu **MID-Server** > **Erweiterungen** > **LES-Verbraucherkontext** und aktualisieren den LES-Verbraucherdatensatz, indem Sie die folgenden Felder festlegen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf „LES-Verbraucher“, um den MID Server-Kontextdatensatz zu öffnen
- Wählen Sie Spezifischer MID Server für das Feld „Ausführen auf“ aus
- Geben Sie den Namen des MID, den Sie im vorherigen Schritt für das Feld „MID Server“ validiert haben, ein

Klicken Sie zum Speichern auf **Aktualisieren**.

Hinweis:
Wir liefern mit einem vordefinierten Kontext. Erstellen Sie keinen zweiten. Dies kann unbeabsichtigte Konsequenzen haben.

- Verbraucher konfigurieren: Erstellen Sie einen neuen Verbraucherdatensatz, der den Prozess darstellt, der Teil der MID Server-Erweiterung „Log Export Service“ ist. Navigieren zu **Log Export Service (LES)** > **Verbraucher** und erstellen Sie einen neuen Konfigurationsdatensatz, in dem Sie das Hermes-Thema angeben, aus dem Protokollnachrichten abgerufen werden sollen, und das Ziel, an das sie weitergeleitet werden sollen.

  a. Neuen Verbraucherdatensatz erstellen

  b. Wählen Sie ein Quellthema aus der Dropdown-Liste aus

  c. Wählen Sie die Zielkonfiguration aus

  d. Verbraucher starten

- Überprüfen Sie die MID Server-Integration: Navigieren Sie zu **Log Export Service (LES)** > **Verbraucher** und die Felder Status und Statusdetail des definierten Datensatzes anzeigen. Die Informationen in diesen Feldern melden den aktuellen Status des Prozesses, der auf dem MID-Server ausgeführt wird, einschließlich aller Fehler, die beim Weiterleiten von Nachrichten an den REST-Endpunkt aufgetreten sind. Wenn der Verbraucherstatus angibt, dass der Prozess gestartet wurde, sollten Sie in der Lage sein, Ihren Endpunkt zu überprüfen, um die an ihn weitergeleiteten Protokolle anzuzeigen. Darüber hinaus können Sie die Protokolle auf dem MID Server anzeigen, um festzustellen, ob zusätzliche Details zu möglicherweise aufgetretenen Fehlern vorhanden sind. Sie können auch die Debug-Protokollierung auf dem MID Server aktivieren, um bei Bedarf zusätzliche Informationen zu erhalten.

Überprüfen Sie den täglichen Protokollexport nach Quellbericht

Analysieren Sie die Größe jeder Datenprotokollquelle, indem Sie den täglichen Protokollexport nach Quellbericht überprüfen. Der Bericht zeigt die Anzahl der Protokoll-Events, die von jeder Protokolltabelle pro Tag generiert werden.

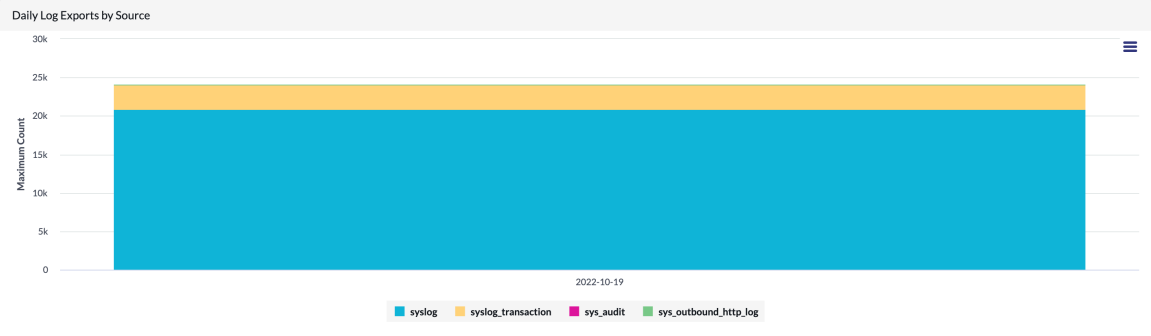
Vorbereitungen

Erforderliche Rolle: admin oder sn_logstoanalytics.admin

Prozedur

1. Navigieren zu **Alle** > **Protokollexportservice** > **Täglicher Protokollexport nach Quelle**.
2. Überprüfen Sie die täglichen Protokollanzahlen, die in den folgenden Tabellen pro Tag erstellt werden.
   - syslog
   - syslog_transaction
   - sys_audit
   - sys_outbound_http_log

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Abhängig von der Größe der Datenquellen können Sie entscheiden, ob Sie sie in den LES-Exportbericht aufnehmen möchten.

Hinweis:
Sie können einen farbcodierten Balken im Diagramm auswählen, der zum Bericht „Tägliche Zusammenfassung des Protokollexports“ weitergeleitet wird, in dem Sie die Filter ändern können, um die Daten weiter zu analysieren. Sie können die Anzahl der vom Log Export Service zu exportierenden Protokoll-Events reduzieren, indem Sie Protokollquellfilter konfigurieren. Die Protokolldateien des Anwendungsknotens sind in diesem Bericht nicht enthalten.

Protokollierung, Auditing und Fehler (Härtung der Instanzsicherheit)

Wenden Sie eine Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Weitere Informationen darüber, was in der Instanz protokolliert werden kann, finden Sie unter Systemprotokolle. Stellen Sie sicher, dass es einen Zeitplan für die Überwachung von Systemereignissen wie Anmeldungen und fehlgeschlagenen Anmeldungen gibt, indem Sie verwenden **Systemprotokolle** > **Ereignisse**.

SQL-Fehlermeldungen deaktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.db.loguser*, um die Darstellung von SQL-Fehlermeldungen in einem Browser zu deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.db.loguser
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	So deaktivieren Sie die Anzeige von SQL-Fehlermeldungen im Browser.
Typ	Wahr|Falsch
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Dies hat keine Auswirkungen auf die Funktionalität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Mittel) Keine vertraulichen SQL-Informationen, die einem Angreifer helfen könnten, sollten als Teil der Fehlermeldung auf einer Webseite angezeigt werden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

Geheimnisverwaltung

Verwenden Sie ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter, die Ihren Geschäftsanforderungen entspricht.

Erkunden

Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Secrets Management kennen.

Analysieren

Erfahren Sie mehr über das Dashboard „Geheimnisverwaltung“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren	
Planen Sie Ihre Kernkonfigurationen.	

Geheimnisverwaltung erkunden

Verwenden Sie ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter, die Ihren Geschäftsanforderungen entspricht.

Wichtig:
Administratoren müssen über die Rolle verfügen, um Module und Datensätze im Zusammenhang mit der Geheimnisverwaltung anzuzeigen. Informationen zur Geheimnisverwaltungsrolle finden Sie unter Geheimnisverwaltungsrollen.

Wählen Sie zwischen Core- und Enterprise-Versionen von Secrets Management

Wählen Sie je nach Ihren Geschäftsanforderungen zwischen Secrets Management Core und Secrets Management Enterprise.

Geheimnisverwaltungs-Core	Geheimnisverwaltung Enterprise
Secrets Management Core kann in Ihrer Instanz ohne zusätzliche Kosten aktiviert werden. Das Plugin bietet die Möglichkeit, Geheimnisgruppen mit Kriterien in nicht benutzerdefinierten Tabellen zu verwenden, die in der Plattform ServiceNow bereitgestellt werden und von Anwendungsentwicklungsteams von ServiceNow erstellt wurden.	Secrets Management Enterprise enthält zusätzliche Funktionen, die Administratoren beim Erstellen und Verwalten von Geheimnisgruppen unterstützen. Enterprise bietet zusätzlich zu den in Core aufgeführten Funktionen die folgenden Funktionen. • Verwenden Sie granulare Zugriffskontrollen, um geheime Gruppen basierend auf einem der folgenden Kriterien zu erstellen. ◦ Umfang ◦ Tabelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheimnisverwaltungs-Core	Geheimnisverwaltung Enterprise
	○ Spalte ○ Datensatz • Erstellen Sie für den Client zugängliche geheime Schlüssel, die mit Ihrem eigenen Schlüssel verschlüsselt werden, auf den ServiceNow nicht zugreifen kann. • Verwenden Sie das Dashboard „Geheimnisverwaltung“, um die in Ihrer Instanz konfigurierten geheimen Gruppen zu überprüfen und sich über potenzielle Sicherheitsprobleme zu informieren. **Hinweis:** Secrets Management Enterprise ist ein kostenpflichtiges Plugin, das Mitarbeiter von ServiceNow in Ihrer Produktionsinstanz aktivieren müssen.

Verwenden Sie Geheimnisgruppen, um Ihre Geheimnisse zu organisieren

Verwenden Sie die Geheimnisverwaltung, um Ihre Geheimnisse in Gruppen zu organisieren und dann Zugriffsrichtlinien auf Gruppenebene auf diese Geheimnisse anzuwenden.

Grundlegende geheime Gruppe

Diese Gruppen gelten für alle Geheimnisse in einem Bereich. Diese Geheimnisse werden durch ein gemeinsames kryptografisches Modul und Modulzugriffsrichtlinien entschlüsselt.

Geheime Gruppe mit Kriterien

Geheime Gruppen mit Kriterien funktionieren genauso wie eine einfache geheime Gruppe, verfeinern jedoch anhand von Kriterien weiter, was enthalten ist. Zu diesen Kriterien gehören:

- Anwendungsbereich
- Paket
- Tabelle
- Geheime Spalte
- Filterdatensatz

Geheime Gruppen beider Typen können für die Instanz oder den Client zugänglich gemacht werden.

Geheime Gruppen auf Instanzseite

Geheime Gruppen auf Instanzseite enthalten Geheimnisse, die von Ihrer Instanz entschlüsselt werden können.

Clientseitige geheime Gruppen

Clientseitige Geheimnisgruppen verwenden ein öffentliches und privates Schlüsselpaar, um sicherzustellen, dass Geheimnisse nur vom Client entschlüsselt werden können. Wenn Sie eine Gruppe mit geheimen Schlüsseln erstellen, auf die der Client zugreifen kann, laden Sie den öffentlichen Schlüssel in die Instanz hoch und speichern den privaten Schlüssel auf Ihrem MID Server. Die Instanz verwendet den öffentlichen Schlüssel, um Ihre geheimen Schlüssel zu verschlüsseln. Sie können jedoch nur mit dem privaten Schlüssel entschlüsselt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Weitere Informationen zu diesen Gruppentypen finden Sie unter Client-Seite verstehen Geheimnisverwaltung.

Verwenden Sie geheime Gruppen für eine detailliertere Steuerung

Während password2 auf der Plattform ServiceNow verfügbar ist, bietet Secrets Management die folgenden zusätzlichen Funktionen.

Granulare Zugriffskontrollen	**Password2** Mit password2 können Administratoren den Zugriff auf einen Anwendungsbereich steuern, aber den Zugriff auf Elemente innerhalb des Bereichs nicht einschränken. **Geheimnisverwaltung** Mit Geheimnisverwaltung können Administratoren den Zugriff basierend auf von ihnen definierten Kriterien einschränken. Kriterientypen können auf Kriterien wie Paket, Tabelle oder Spalte basieren.
Sicherer Speicher	Für clientseitige geheime Gruppen verwendet Secrets Management ein neues Verschlüsselungsschema. In diesem Verschlüsselungsschema speichert ServiceNow den Verschlüsselungsschlüssel nicht. Aus diesem Grund hängt die Sicherheit Ihrer Daten nicht von der Sicherheit von ServiceNow ab.

Wenden Sie Modulzugriffsrichtlinien auf Ihre Gruppen an

Nachdem Sie Ihre geheimen Schlüssel in einer geheimen Gruppe gruppiert haben, können Sie Richtlinien anwenden, die bestimmen, wie Sie auf Gruppenebene auf diese geheimen Schlüssel zugreifen können. Modulzugriffsrichtlinien sind die Zugriffskontrollmechanismen, die Sie auf kryptografische Module anwenden, um Steuerungen auf Instanzebene zu definieren, z. B. einen Gültigkeitszeitraum für den kryptografischen Schlüssel. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über Modulzugriffsrichtlinien.

Mit Secrets Management installierte Tabellen

Secrets Management fügt diese Tabellen hinzu oder ändert sie.

Neue Tabellen	
[sn_sm_secret_group]	Speichert geheime Gruppen
[sn_sm_secret_group_criteria]	Speichert geheime Kriteriengruppen
[sn_sm_secrets]	Speichert umschlossene Geheimnisse
[sn_sm_identity_group]	Definiert die Identitätsgruppe für die Zuordnung einer Gruppe von Identitäten zum öffentlichen Schlüssel
[sys_kmf_wrapped_module_key]	Speichert die umschlossenen symmetrischen kryptografischen Schlüssel
Geänderte Tabellen	
[sys_kmf_crypto_module]	Kryptografischer Modultyp hinzugefügt. (Kryptografisches Identitätsmodul oder kryptografisches Modul für geheime Gruppe)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[sys_kmf_module_key]	• Speichert den konzeptionellen geheimen Verschlüsselungsschlüssel (ohne Schlüsselmaterial) • Speichert den öffentlichen Identitätsschlüssel
[sys_kmf_crypto_caller_policy]	Neuer Modulzugriffsrichtlinientyp hinzugefügt

Client-Seite verstehen Geheimnisverwaltung

Erfahren Sie, wie Sie mit Geheimnisverwaltung den Zugriff auf geheime Schlüssel und Gruppen verwalten.

Terminologie

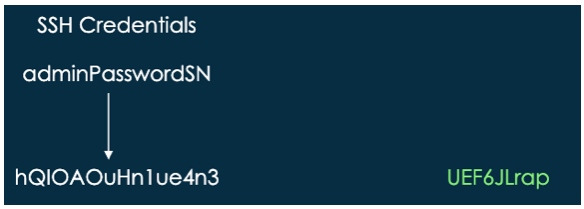
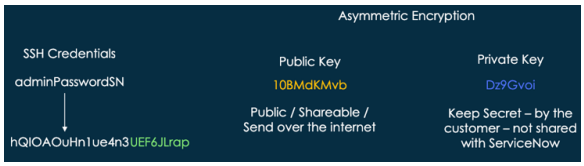
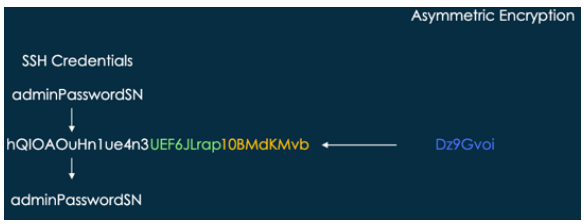
Die clientseitige Verwaltung von Geheimnissen bietet eine Methode zum Verwalten von Geheimnissen ohne die Verwendung von Proxys und ohne ServiceNow Zugriff auf Ihre entschlüsselten Daten. Um diesen Prozess zu verstehen, beginnen Sie mit den folgenden Verschlüsselungsbegriffen.

Begriff	Beschreibung
Symmetrische Verschlüsselung	Bei der symmetrischen Verschlüsselung wird ein und derselbe Schlüssel zum Verschlüsseln und Entschlüsseln von Daten verwendet. Wenn Daten mit einem symmetrischen Schlüssel verschlüsselt werden, genügt dieser Schlüssel, um sie zu entschlüsseln.
Symmetrischer Schlüssel	Der symmetrische Schlüssel verschlüsselt ein Geheimnis und wandelt Ihr Klartext-Passwort in unlesbaren Geheimtext um.
Asymmetrische Verschlüsselung	Bei der asymmetrischen Verschlüsselung werden zwei Schlüssel verwendet, einer zum Verschlüsseln und ein anderer zum Entschlüsseln.
Öffentlicher Schlüssel	Der öffentliche Schlüssel ist eine Hälfte des asymmetrischen Schlüsselpaars. Dieser Schlüssel wird in Ihrer Instanz gespeichert, die den Schlüssel zum Verschlüsseln eines symmetrischen Schlüssels verwendet. Dieser verschlüsselte symmetrische Schlüssel kann nur entschlüsselt werden, wenn er mit dem privaten Schlüssel gekoppelt ist.
Privater Schlüssel	Der private Schlüssel ist eine Hälfte des asymmetrischen Schlüsselpaars. Dieser Schlüssel wird in einem Schlüsselspeicher auf Ihrem MID-Server gespeichert. ServiceNow hat keinen Zugriff auf diesen Schlüssel. In Kombination mit dem öffentlichen Schlüssel wird das asymmetrische Schlüsselpaar zum Entschlüsseln Ihrer Geheimnisse verwendet.

Clientseitiger Verschlüsselungsprozess

Ein symmetrischer Schlüssel verschlüsselt Anmeldeinformationen (in diesem Fall ein Administratorpasswort) und ändert sie von lesbarem Klartext in verschlüsselten Geheimtext.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der symmetrische Schlüssel (grün dargestellt) kann auf die Anmeldeinformationen angewendet werden, um sie zu verschlüsseln oder zu entschlüsseln.	
An diesem Punkt beginnt die asymmetrische Verschlüsselung mit öffentlichen Schlüsseln (gelb) und privaten Schlüsseln (blau).	
Der öffentliche Schlüssel verschlüsselt die Anmeldeinformationen zusammen mit dem symmetrischen Schlüssel. Der symmetrische Schlüssel ist jetzt geschützt und kann nicht zum Entschlüsseln der Anmeldeinformationen verwendet werden. Obwohl der öffentliche Schlüssel diese Verschlüsselung durchführen kann, kann er nicht allein zum Entschlüsseln verwendet werden.	
Nach der Verschlüsselung mit dem öffentlichen Schlüssel wird der private Schlüssel benötigt, um die Anmeldeinformationen zu entschlüsseln. Da nur der Kunde über diesen Schlüssel verfügt, ist er der einzige, der auf die verschlüsselten Anmeldeinformationen zugreifen darf.	

Vom Client zugängliche geheime Schlüssel konfigurieren

Erfahren Sie, wie Sie Ihre Instanz für die Verwendung von vom Client zugänglichen geheimen Schlüssel konfigurieren.

Verwenden Sie diese Beispielimplementierung, um Geheimnisverwaltung zu konfigurieren, ohne Proxys zu verwenden oder ServiceNow Zugriff auf Ihre entschlüsselten Daten zu gewähren.

Weitere Informationen zur Verwendung von clientseitigem Geheimnisverwaltung zum Verwalten des Zugriffs auf Passwörter und Gruppen finden Sie unter Client-Seite verstehen Geheimnisverwaltung.

Bei diesen Anweisungen wird davon ausgegangen, dass in Ihrem lokalen Netzwerk ein MID-Server konfiguriert ist. Weitere Informationen zu diesem Prozess finden Sie unter MID Server .

Prozessübersicht

1. **Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat**

   Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat mit Terminal-Befehlen in Ihrer lokalen Umgebung.

2. **Fügen Sie Ihr Zertifikat dem ServiceNow Trusted Key Store hinzu**

   Laden Sie Ihren Schlüssel und Ihr Zertifikat in den vertrauenswürdigen Schlüsselspeicher ServiceNow hoch.

3. **Erstellen Sie eine geheime Gruppe mit Kriterien**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Gruppe für Ihre geheimen Schlüssel. Geheimnisgruppen, um Ihre Geheimnisse in Gruppen zu organisieren. Mit diesen Gruppen können Sie Zugriffsrichtlinien auf diese Geheimnisse auf Gruppenebene anwenden. Ordnen Sie dann Ihre geheime Gruppe einer Identitätsgruppe zu, und fügen Sie Ihren MID-Server dieser Identitätsgruppe hinzu.

4. **Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen**

   Erstellen Sie Anmeldeinformationen, um sich bei einem Drittanbietersystem zu authentifizieren, und testen Sie, dass ServiceNow nicht auf die Anmeldeinformationen zugreifen kann.

5. **Laden Sie das öffentliche/private Schlüsselpaar auf den MID Server hoch**

   Laden Sie Ihr öffentliches/privates Schlüsselpaar auf Ihren MID-Server hoch. Mit diesem Schlüsselpaar kann der MID Server Authentifizierungsanforderungen von Ihrer Instanz verarbeiten.

6. **Konfigurieren Sie Flow Designer, um die Integration zu verwalten**

   Verwenden Sie in Ihrer Instanz Flow Designer, um eine Integration zwischen Ihrem lokalen Netzwerk und Ihrer Instanz zu verwalten.

7. **Testen Sie die End-to-End-Integration von clientseitig verschlüsselten Geheimnissen**

   Testen Sie Ihre Integration, und überprüfen Sie die Ausführungsdetails, um sicherzustellen, dass Ihre Konfiguration funktioniert.

Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat

Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat mit Terminal-Befehlen in Ihrer lokalen Umgebung.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Öffnen Sie in Ihrer lokalen Umgebung Terminal (unter Mac oder Linux) oder die Befehlszeile (unter Windows).
2. Verwenden Sie im Terminal `cd`, um in den Ordner zu wechseln, in dem Sie Ihre Verschlüsselungsschlüssel speichern möchten.
3. Geben Sie im Terminal Folgendes ein:

   ```
   openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509 -days 365 -out sm_public_cert.pem
   ```

   Hinweis:
   In diesem Beispiel wird OpenSSL zum Generieren von Schlüsseln und Zertifikaten verwendet. Sie können andere vergleichbare Tools basierend auf Ihren Anforderungen ersetzen.

   Der Befehl generiert einen privaten Schlüssel und ein öffentliches Zertifikat (mit dem entsprechenden öffentlichen Schlüssel). Es folgt eine Reihe von Aufforderungen zur Eingabe erforderlicher Informationen, beginnend mit „Landesname“.

4. Füllen Sie die Eingabeaufforderungen mit den angeforderten Informationen aus.
   Die folgenden Eingabeaufforderungen werden angezeigt.
   - Ländername
   - Bundesland/Kantonname
   - Ortsname (z. B. Stadt)
   - Organisationsname (z. B. Unternehmen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Name der Organisationseinheit (z. B. Abschnitt)
- Allgemeiner Name (z. B. vollständig qualifizierter Hostname)
- E-Mail-Adresse

Arbeiten Sie mit Ihrem Sicherheitsteam zusammen, um sicherzustellen, dass Sie die richtigen Zertifikatinformationen eingeben.

```
Country Name (2 letter code) []:US
State or Province Name (full name) []:CO
Locality Name (eg, city) []:Boulder
Organization Name (eg, company) []:ServiceNow
Organizational Unit Name (eg, section) []:Product Management
Common Name (eg, fully qualified host name) []:fake@servicenow.com
Email Address []:fake@servicenow.com
```

5. Überprüfen Sie den Ordner, den Sie in Schritt 2 ausgewählt haben, um sicherzustellen, dass der private Schlüssel und das öffentliche Zertifikat erstellt wurden.
   Wenn Sie dieselben Dateinamen wie im Beispiel von Schritt 3 verwendet haben, sollten die folgenden Dateien angezeigt werden:
   - sm_private_key.pem
   - sm_public_cert.pem
6. Verwenden Sie im selben Ordner den folgenden Befehl:

Wichtig:
Der zu verwendende Befehl hängt von Ihrem Betriebssystem ab.

Für Linux:	`cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`
Für Windows:	`sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`

Dieser Befehl bündelt den privaten Schlüssel und das öffentliche Zertifikat in einer einzigen Datei, die in späteren Schritten auf Ihren MID Server geladen wird.

7. Überprüfen Sie den Ordner erneut, um sicherzustellen, dass die neue Datei mit Ihrem privaten Schlüssel (sm_keypair_bundle.pem) und Ihrem öffentlichen Zertifikat erstellt wurde.

Fügen Sie Ihr Zertifikat dem ServiceNow Trusted Key Store hinzu

Laden Sie Ihren Schlüssel und Ihr Zertifikat in den vertrauenswürdigen Schlüsselspeicher ServiceNow hoch.

Vorbereitungen

Erforderliche Rolle: keine

Das öffentliche Zertifikat, das Sie in diesem Beispiel erstellt haben, wird als „selbstsigniertes“ Zertifikat betrachtet (d. h. es stammt nicht von einer vertrauenswürdigen Stammautorität). Sie müssen das Zertifikat dem vertrauenswürdigen Schlüsselspeicher ServiceNow hinzufügen, damit es verwendet werden kann. Wenn Sie ein Zertifikat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwenden, das von einer Zertifizierungsstelle stammt, müssen Sie diesen Schritt nicht ausführen.

Prozedur

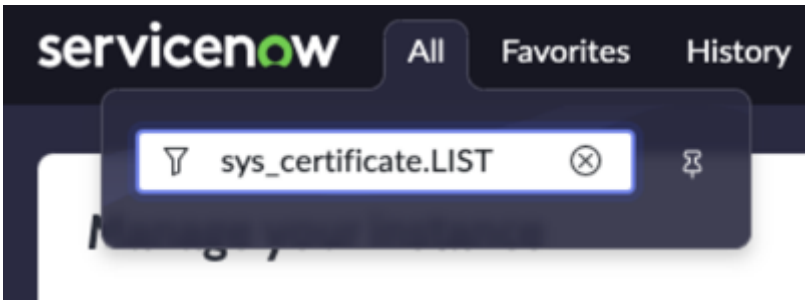
1. Öffnen Sie in Ihrer lokalen Umgebung Terminal (unter Mac oder Linux) oder die Befehlszeile (unter Windows).
2. Verwenden Sie im Terminal `cd`, um in den Ordner zu wechseln, in dem Sie Ihre Verschlüsselungsschlüssel erstellt haben.
3. Geben Sie im Terminal den folgenden Befehl ein:

   ```
   cat sm_public_cert.pem
   ```

   Sie müssen den Inhalt Ihres öffentlichen Zertifikats anzeigen, um es in den vertrauenswürdigen Schlüsselspeicher zu kopieren. Dieser `cat-` Befehl zeigt das Zertifikat an.

4. Kopieren Sie die Zertifikatinformationen in die Zwischenablage.
   Beginnen Sie mit und schließen Sie die Zeile `-----BEGIN CERTIFICATE-----` ein, enden Sie mit und schließen Sie die Zeile `-----END CERTIFICATE-----` ein.
5. Navigieren Sie in Ihrer Instanz ServiceNow zur **X.509-Zertifikatliste**, indem Sie `sys_certificate.LIST` im Navigationsfilter eingeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie **Neu** aus, um einen **X.509-Zertifikatdatensatz** zu erstellen.
7. Füllen Sie im Formular die folgenden Felder aus.

X.509-Zertifikatfelder

Feld	Wert
Name	Name des Zertifikats Dieser Name kann ein beliebiger Name sein.
Format	Wählen Sie **PEM aus** **Hinweis:** PEM-Dateien (Privacy Enhanced Mail) sind eine Art von PKI-Dateien (Public Key Infrastructure), die für Schlüssel und Zertifikate verwendet werden. Die Datensätze, die Sie in den vorherigen Schritten erstellt haben, sind von diesem Dateityp.
Typ	Wählen Sie **Trusted Store-Zertifikat aus**
Kurzbeschreibung	Beschreibung des Zertifikats Geben Sie einen Wert ein, der Sie darüber informiert, wofür dieses Zertifikat verwendet wird.
PEM-Zertifikat	Fügen Sie die Zertifikatinformationen ein, die Sie in Schritt 4 kopiert haben.

8. Wählen Sie **Absenden** aus, um den Datensatz zu speichern.

Erstellen Sie eine geheime Gruppe mit Kriterien

Erstellen Sie eine Gruppe für Ihre geheimen Schlüssel. Geheimnisgruppen, um Ihre Geheimnisse in Gruppen zu organisieren und Zugriffsrichtlinien auf Gruppenebene auf diese Geheimnisse anzuwenden. Ordnen Sie dann Ihre geheime Gruppe einer Identitätsgruppe zu, und fügen Sie dieser Identitätsgruppe Ihren MID Server hinzu.

Vorbereitungen

Erforderliche Rolle: admin, KMF_admin

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen mit Kriterien**.
2. Wählen Sie **Neu** aus, um eine **geheime Gruppe mit Kriteriendatensatz** zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie im Formular die folgenden Felder aus.

Geheime Gruppe mit Kriterienfeldern

Feld	Wert
Gruppenname	Name der geheimen Gruppe Dieser Name kann ein beliebiger Name sein.
Geheimer Typ	Wählen Sie **Vom Client zugänglich aus**
Autogen-Modul	Aktivieren Sie das Kontrollkästchen
Kurzbeschreibung	Beschreibung der geheimen Gruppe Geben Sie einen Wert ein, der Sie darüber informiert, wofür diese Gruppe verwendet wird.
Kriteriumstyp	Wählen Sie **Zieltabelle aus**
Zieltabelle	Wählen Sie **SSH-Anmeldeinformationen [ssh_credentials] aus.**

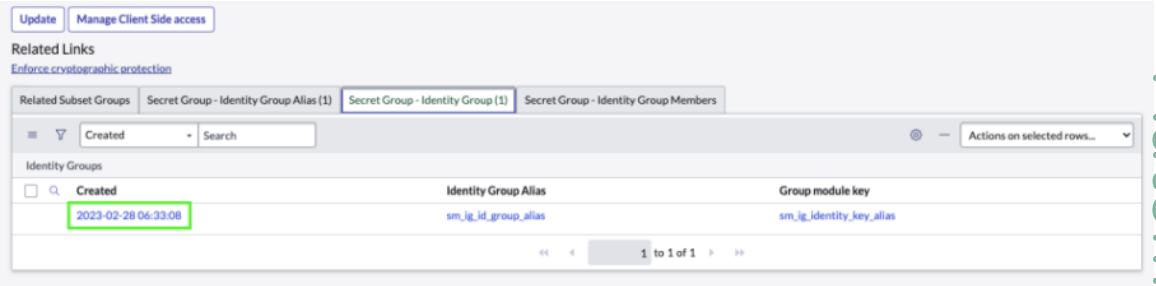
4. Klicken Sie mit der rechten Maustaste auf die Formularkopfzeile, und wählen Sie im Kontextmenü **Speichern** aus, um den Datensatz zu speichern.
5. Stellen Sie sicher, dass das Kontrollkästchen **Aktiv** nicht aktiviert ist.
6. Klicken Sie auf die Schaltfläche **Clientseitigen Zugriff verwalten**, um eine Identitätsgruppe zu erstellen. Ein Fenster für **Identitätsgruppenalias** wird angezeigt.
7. Klicken Sie auf die Schaltfläche **Neu**.
8. Klicken Sie auf das Referenzsymbol ( ) neben dem Feld **Identitätsgruppenalias**.
9. **Geben Sie im Feld Gruppenaliasname** einen Wert ein.
   Dieser Name kann ein beliebiger Wert sein.
10. Wählen Sie **Absenden**.
11. Klicken Sie auf die Schaltfläche **Identitätsschlüssel** hochladen.
    Das Fenster **„Identität des öffentlichen Schlüsselzertifikats importieren** “ wird angezeigt.
12. Geben Sie im Feld **Identitätsschlüssel-Alias** einen Wert ein.

> **Wichtig:**
> Dieser Wert kann beliebig sein, muss jedoch genau mit dem übereinstimmen, was Sie in den späteren Schritten in den MID Server einfügen.

13. Wählen Sie **Importieren aus**
    Das Fenster „ **Anhang** “ wird angezeigt.
14. Wählen **Sie Datei auswählen aus**.
15. Wählen Sie das öffentliche Zertifikat aus, das Sie in den vorherigen Schritten erstellt haben.
    Dieses Zertifikat muss die Datei `sm_public_cert.pem` sein.
16. Klicken Sie auf das X-Symbol, um das Fenster zu schließen.
17. Klicken Sie auf **OK**, um das Fenster **„Identität des öffentlichen Schlüsselzertifikats** importieren“ zu schließen.
    Ein blaues Banner **Schlüssel und Zertifikate wurden erfolgreich in die Instanz importiert, das** einen erfolgreichen Import bestätigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

18. Wählen Sie **Absenden**.
    Die Liste „ **Identitätsgruppen“ wird** angezeigt.
19. Aktivieren Sie die Checkbox links neben dem Identitätsgruppendatensatz in der Liste.
20. Klicken Sie auf die Schaltfläche **Geheime Gruppe** zuordnen.
    Sie kehren zu Ihrem Datensatz **„Geheime Gruppe mit Kriterien“** zurück. Die zugehörigen Listen „Geheime Gruppe – **Identitätsgruppenalias**“ und „ **Geheime Gruppe – Identitätsgruppe“** sind sichtbar. Diese zugehörigen Listen zeigen die Datensätze an, die Sie in den vorherigen Schritten erstellt haben.
21. Wählen Sie in der zugehörigen Liste **Geheime Gruppe – Identitätsgruppe** das Feld **Erstellt** für den Datensatz in dieser Liste aus.



    Ein **Identitätsgruppendatensatz wird** angezeigt.
22. Klicken Sie in der zugehörigen Liste **Identitätsgruppenmitglieder auf** die Schaltfläche **Neu**.
    Ein **Identitätsgruppenmitgliedsdatensatz wird** angezeigt.
23. Wählen Sie im Feld **Mitgliedstabelle** die **Option MID Server [ecc_agent] aus**.
24. Wählen Sie das Referenzsymbol ( ) neben dem Feld **„Identitätsgruppenmitglied“** und dann Ihren MID Server aus.

    Hinweis:
    Wenn Sie das Kontrollkästchen **Alle Datensätze einbeziehen** aktivieren, werden alle mit Ihrer Instanz verbundenen MID Server der Identitätsgruppe hinzugefügt.

25. Klicken Sie auf **OK**, um das Fenster **„Dokument** auswählen“ zu schließen.
26. Wählen Sie **Absenden**.
27. Navigieren Sie zurück zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen mit Kriterien**, und öffnen Sie den Datensatz, den Sie in Schritt 2 erstellt haben.
28. Aktivieren Sie das Feld **Aktiv**.
29. Wählen Sie **Aktualisieren** aus, um den Datensatz zu speichern.

Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen

Erstellen Sie Anmeldeinformationen, um sich bei einem Drittanbietersystem zu authentifizieren, und testen Sie, dass ServiceNow nicht auf die Anmeldeinformationen zugreifen kann.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

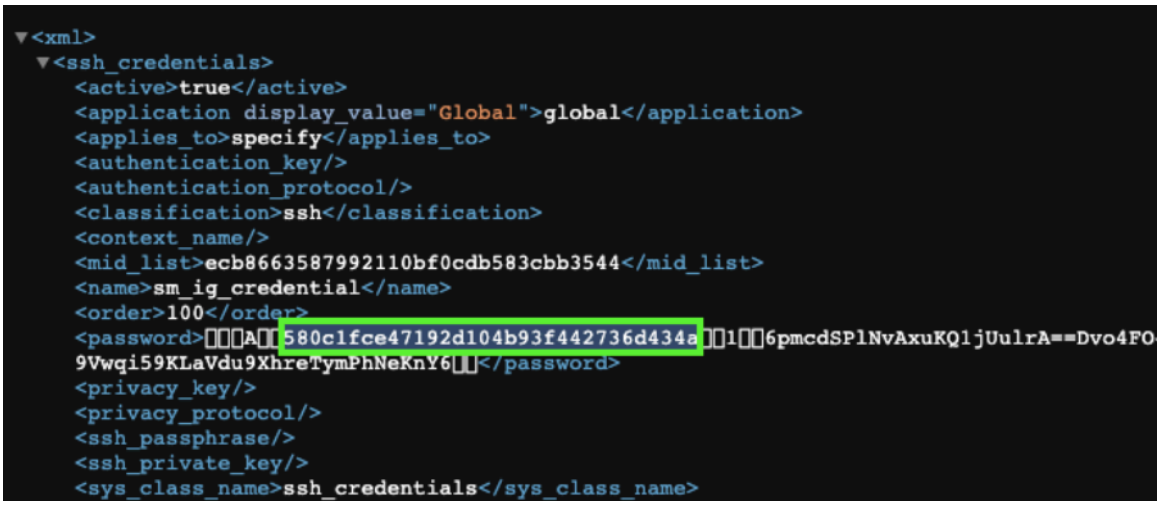
1. Navigieren Sie zur Liste der **SSH-Anmeldeinformationen**, indem Sie `ssh_credentials.list` im Navigationsfilter eingeben.
2. Wählen Sie **Neu** aus, um einen **SSH-Anmeldeinformationsdatensatz** zu erstellen.
3. Füllen Sie im Formular die folgenden Felder aus.

SSH-Anmeldeinformationsformular

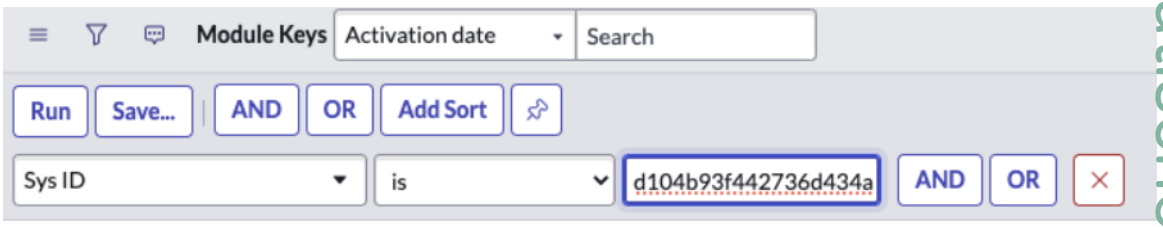
Feld	Wert
Name	Geben Sie einen Namen für Ihren Anmeldeinformationsdatensatz ein. Dieser Name kann ein beliebiger Wert sein.
Betrifft	Wählen Sie **Spezifische MID Server aus**
MID-Server	Wählen Sie Ihren MID Server aus.
Benutzernamen	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das mit dem Benutzer verbundene Passwort in das Feld **Benutzername** ein.

4. Wählen Sie das Schlosssymbol ( ) neben dem Feld **Alias für Anmeldeinformationen** aus.
5. Wählen Sie das Referenzsymbol ( ) aus, um die Liste der **Aliasse für Verbindungen und Anmeldeinformationen** zu öffnen.
6. Wählen Sie **Neu** aus, um einen Datensatz für den **Alias für Verbindungen und Anmeldeinformationen** zu erstellen.
7. Geben Sie einen Namen in das Feld **Name** ein.
8. Wählen Sie im Feld **Typ** die Option **Anmeldeinformationen** aus.
9. Wählen Sie **Absenden**.
   Sie kehren zum **SSH-Anmeldeinformationsdatensatz** zurück. In den nächsten Schritten testen Sie, ob die Anmeldeinformationen verschlüsselt sind.
10. Klicken Sie mit der rechten Maustaste auf die Formularkopfzeile, und wählen Sie **XML anzeigen aus**.
11. Suchen Sie nach<password> XML-Tag innerhalb der XML.
12. Kopieren Sie die sys_id innerhalb dieses<password> -Tag in die Zwischenablage.
    Die sys_id ist ein 32-stelliger Code, der den symmetrischen Schlüssel darstellt, der zum Verschlüsseln dieser Anmeldeinformationen verwendet wird. Das verschlüsselte Passwort, das Sie in die Tabelle „SSH-Anmeldeinformationen“ eingegeben haben, befindet sich rechts neben den beiden Kästchen in derselben Zeile.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



13. Navigieren Sie zur Liste „Modulschlüssel“, indem Sie sys_kmf_module_key.list**im** Navigationsfilter eingeben.
14. Filtern Sie die Liste nach Datensätzen, bei denen das Feld **Sys-ID** mit der sys_id übereinstimmt, die Sie in Schritt 12 kopiert haben, und wählen Sie **Ausführen**aus.



Ihre Suche sollte einen einzelnen **Modulschlüssel** -Datensatz zurückgeben. Dieser Datensatz zeigt, dass Sie erfolgreich einen symmetrischen Schlüssel erstellt haben und ihn verwenden.

15. Navigieren Sie zur Liste der umschlossenen **Modulschlüssel,** indem Sie im Navigationsfilter sys_kmf_wrapped_module_key.list eingeben.
16. Filtern Sie die Liste nach Datensätzen, bei denen das Feld **Krypto-Modul** mit dem Kryptografiemodul übereinstimmt, das Sie in den vorherigen Schritten erstellt haben, und wählen Sie **Ausführen**aus.
    Ihre Suche sollte einen einzelnen **umschlossenen Modulschlüssel** -Datensatz zurückgeben. In dieser Liste können Sie Folgendes überprüfen:
    - Die Spalte **Wrapped key material** (Umwickeltes Schlüsselmaterial) zeigt, dass der symmetrische Schlüssel innerhalb des Krypto-Moduls (das zum Verschlüsseln der SSH-Anmeldeinformationen verwendet wird) durch den öffentlichen Schlüssel verschlüsselt wird, den Sie in die Identitätsgruppe hochgeladen haben.
    - Das Feld **Sys-ID des umschlossenen Schlüssels** zeigt an, dass es sich um den Schlüssel (den symmetrischen Schlüssel des Krypto-Moduls) handelt, der von der **Sys-ID des Wrapping-Schlüssels** (dem in die Identitätsgruppe hochgeladenen öffentlichen Schlüssel) verschlüsselt wird.

Hinweis:
Wenn die vorherigen Felder standardmäßig nicht in Ihrer Liste enthalten sind, können Sie sie der Liste hinzufügen, indem Sie auf das Symbol „Liste **personalisieren** “ („Liste personalisieren“) klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laden Sie das öffentliche/private Schlüsselpaar auf den MID Server hoch

Laden Sie Ihr öffentliches/privates Schlüsselpaar auf Ihren MID Server hoch. Mit diesem Schlüsselpaar kann der MID Server Authentifizierungsanforderungen von Ihrer Instanz verarbeiten.

Vorbereitungen

Erforderliche Rolle: keine

Da ServiceNow keinen Zugriff auf den privaten Schlüssel hat, kann er ihn nicht mit dem öffentlichen Schlüssel koppeln, um den symmetrischen Schlüssel zu entschlüsseln, und dann die Anmeldeinformationen entschlüsseln. Wenn der MID Server versucht, diese verschlüsselten Anmeldeinformationen zu verwenden, kann er die Anmeldeinformationen für die Authentifizierung ohne Zugriff auf den privaten Schlüssel nicht entschlüsseln.

In diesen Schritten laden Sie den privaten Schlüssel auf den MID Server hoch, um den öffentlichen/privaten Schlüsselbund abzuschließen. Dieser Upload gewährt dem MID Server Zugriff, ohne ServiceNow Zugriff zu gewähren.

Um dem MID Server Zugriff auf den privaten Schlüssel zu gewähren, müssen Sie einen Befehl erstellen, der als Administrator in PowerShell ausgeführt werden soll. In diesem Beispiel gilt der Befehl für die Azure Windows-VM.

Wichtig:

Stellen Sie sicher, dass das System, auf dem Sie diese Schritte ausführen, Zugriff auf den MID Server und die Schlüsselpaardatei hat.

Prozedur

1. Suchen Sie in Ihrer lokalen Umgebung den Ordner, in dem Sie Ihr Schlüsselpaar in den Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat -Schritten erstellt haben.
2. Suchen und kopieren Sie den vollständigen Pfad zur Datei „ `manage-certificates.bat` “.

   Hinweis:
   Diese Datei befindet sich in Ihrem MID Server-Ordner. Je nachdem, wo Sie Ihren MID Server-Ordner gespeichert haben, kann Ihr Pfad wie folgt aussehen:

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat
   ```

3. Erstellen Sie eine Textdatei, und fügen Sie den Pfad in die Datei ein.
4. Fügen Sie in der Textdatei nach dem Pfad Folgendes hinzu:
   `-a your_identity_key_alias`

   Ersetzen Sie `your_identity_key_alias` durch den Namen des Identitätsschlüssel-Alias, den Sie beim Hochladen Ihres öffentlichen Zertifikats erstellt haben.

5. Suchen und kopieren Sie den vollständigen Pfad zu Ihrer Schlüsselpaardatei.

   Hinweis:
   Wenn Sie die Namen in diesen Schritten verwendet haben, heißt diese Datei `sm_keypair_bundle.pem`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Fügen Sie in Ihrer Textdatei diesen Pfad am Ende der Zeile hinzu, und fügen Sie ein Leerzeichen zwischen diesem Pfad und den vorherigen Informationen hinzu.
   Der Text in Ihrer Textdatei sollte in etwa wie in diesem Beispiel aussehen:

```
C:
\Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat -a your_identity_key_alias
 C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
```

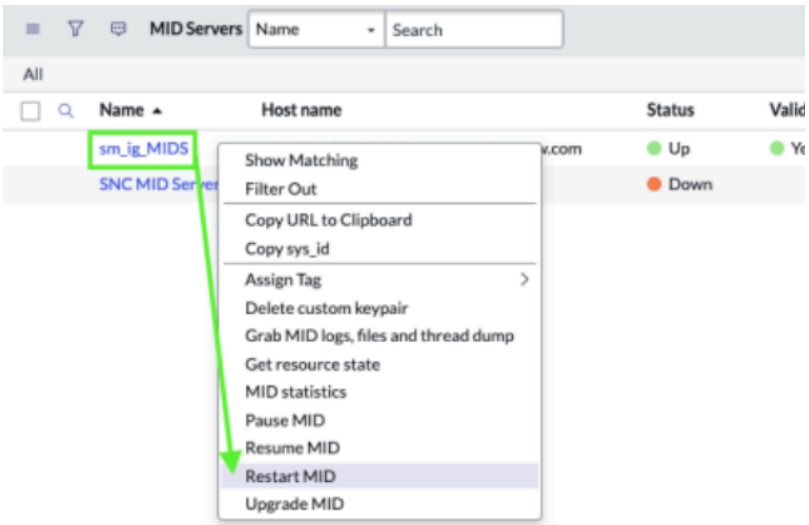
Hinweis:
In diesem Beispiel befindet sich die Datei `sm_keypair_bundle.pem` auf dem Desktop, um den Pfad zu verkürzen.

7. Kopieren Sie den gesamten Text der Textdatei in die Zwischenablage.
8. Suchen Sie auf Ihrem System nach PowerShell, und wählen Sie die Option **Als Administrator** ausführen aus.
9. Fügen Sie den Text aus Ihrer Textdatei in PowerShell ein, und drücken Sie die Eingabetaste.
   Bei Erfolg wird die folgende Meldung angezeigt:

```
Installed certificate with alias: <your_identity_key_alias> into the MID keystore.
```

Tipp:
Wenn diese Meldung nicht angezeigt wird, stellen Sie sicher, dass Ihr Befehl keine Fehler, Leerzeichen oder unnötigen Anführungszeichen enthält. Stellen Sie sicher, dass der vollständige Pfad korrekt eingegeben wurde.

10. Starten Sie Ihren MID Server neu, indem Sie zu Ihrem MID Server-Datensatz navigieren, mit der rechten Maustaste auf den Datensatz klicken und **MID neu starten**auswählen.



Durch einen Neustart des MID Servers wird das hochgeladene Schlüsselpaar im MID-Schlüsselspeicher zur Verwendung mit Vorgängen synchronisiert. Warten Sie, **bis** der MID Server mit dem Status In Betrieb und dem validierten Wert **Ja** neu gestartet wurde, bevor Sie fortfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Flow Designer, um die Integration zu verwalten

Verwenden Sie in Ihrer Instanz Flow Designer, um eine Integration zwischen Ihrem lokalen Netzwerk und Ihrer Instanz zu verwalten.

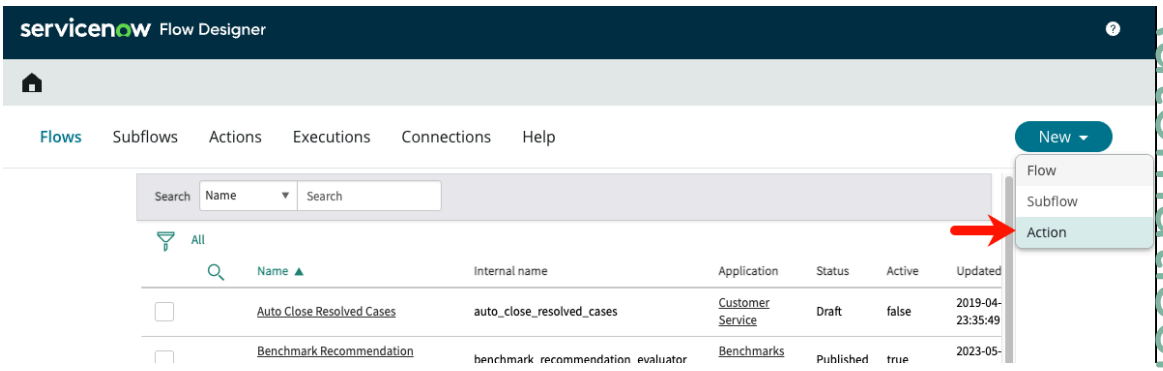
Vorbereitungen

Erforderliche Rolle: admin

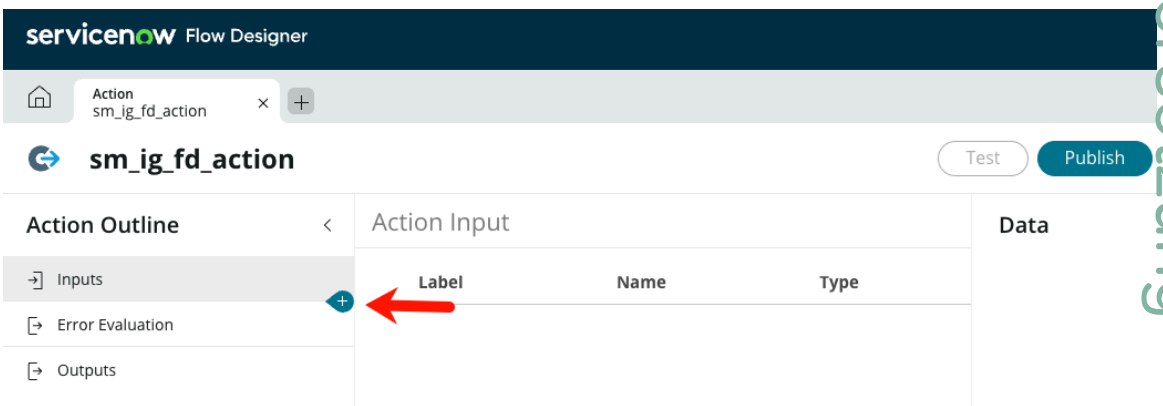
In diesen Schritten der Anleitung erstellen Sie einen Flow Designer -Workflow, um eine Textdatei auf Ihrem lokalen System zu erstellen.

Prozedur

1. Navigieren Sie in Ihrer Instanz zu **Alle** > **Prozessautomatisierung** > **Flow Designer**.
2. Erstellen Sie eine Aktion in ServiceNow, indem Sie **Neu** und **Aktion**auswählen.



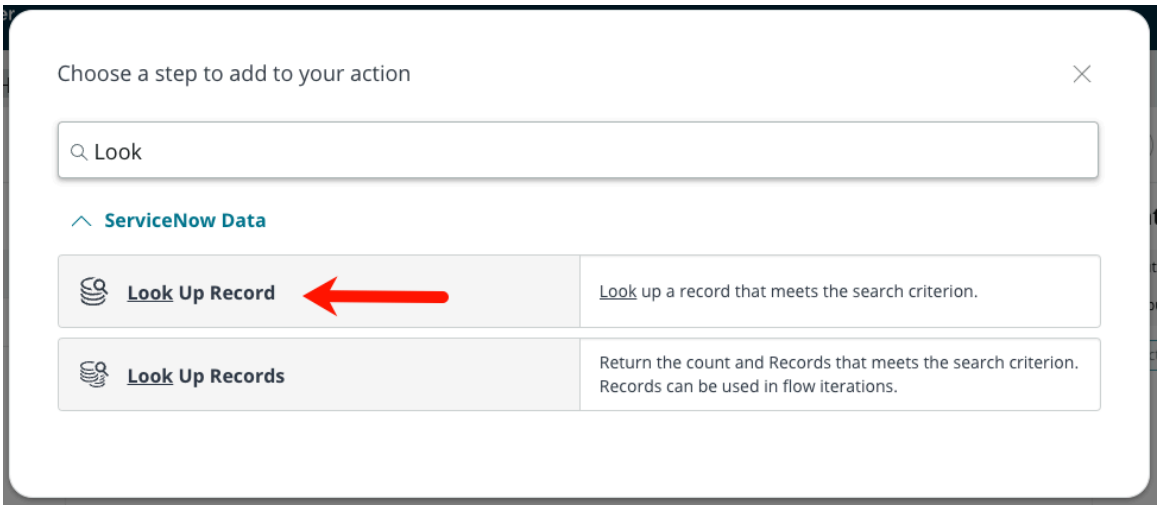
3. Geben Sie einen Namen in das Feld **Aktionsname** ein, und wählen Sie **Absenden**aus.
4. Erstellen Sie einen Schritt, indem Sie das Pluszeichen zwischen **Eingaben** und **Fehlerauswertung** in der **Aktionsgliederung**auswählen.



5. **Wählen Sie im Fenster Einen Schritt auswählen, den Sie Ihrer Aktion hinzufügen** möchten die **Option Datensatz suchen aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie im Schrittabschnitt „ **Datensatz** nachschlagen“ im Feld **Tabelle** die **Option MID Server [ecc_agent]** aus.
7. Erstellen Sie einen weiteren Schritt, indem Sie das Pluszeichen unter Ihrem **Schritt „Datensatz nachschlagen“**auswählen.
8. **Wählen Sie im Fenster Einen Schritt auswählen, den Sie Ihrer Aktion hinzufügen möchten** die Option **SSH**aus.

   Hinweis:
   Wenn die Option **SSH** nicht angezeigt wird, müssen Sie das erforderliche Plugin aktivieren.

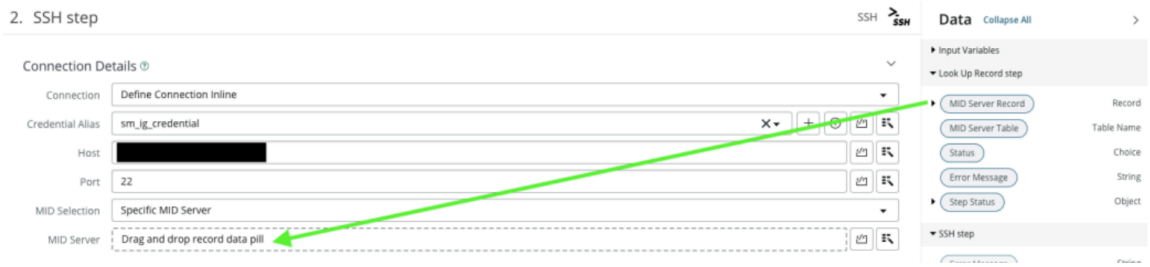
9. Geben Sie im Abschnitt „ **SSH-Schritt** “ die folgenden Informationen ein:

Feld	Wert
Verbindung	Wählen **Sie Verbindung inline definieren aus**
Anmeldeinformationsalias	Wählen Sie den Anmeldeinformationsalias für die SSH-Anmeldeinformationen aus, die in vorherigen Schritten erstellt wurden.
Host	Geben Sie die IP-Adresse für den Host ein, mit dem Sie über SSH eine Verbindung herstellen.
Port	Geben Sie 22 ein.
MID-Auswahl	Wählen Sie **Spezifischer MID Server aus**.

10. Um das Feld **MID Server** auszufüllen, ziehen Sie die Pille **MID Server-Datensatz** aus dem **Datenabschnitt** auf der rechten Seite in das Feld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Warnung:
Wenn Sie die Pille in das Feld ziehen, wählen Sie die Pille und nicht den schwarzen Pfeil links von der Pille aus.

11. Geben Sie im Abschnitt „ **SSH-Konfiguration** “ den folgenden Wert in das Feld **Befehl** ein.

```
/bin/date > sm_ig_text_file.txt
```

Dieser Befehl erstellt eine Textdatei in Ihrem lokalen System unter Verwendung der entschlüsselten Geheimnisse des MID-Servers. Der MID Server gewährt Zugriff auf die Instanz ServiceNow (über Flow Designer), ohne der Instanz ServiceNow] jemals Zugriff auf das entschlüsselte Geheimnis zu gewähren.

Tipp:
Der Befehl `/bin/date` fügt das aktuelle Datum/die aktuelle Uhrzeit in die erstellte Textdatei ein. Dieser Befehl zeigt, dass die Integration in Echtzeit basierend auf dem aktuellen Datum/der aktuellen Uhrzeit im Vergleich zum Erstellungsdatum der Textdatei erfolgt.

12. Klicken Sie oben rechts auf dem Bildschirm auf die Schaltfläche **Speichern**, um den Workflow zu speichern.

Testen Sie die End-to-End-Integration von clientseitig verschlüsselten Geheimnissen

Testen Sie Ihre Integration, und überprüfen Sie die Ausführungsdetails, um sicherzustellen, dass Ihre Konfiguration funktioniert.

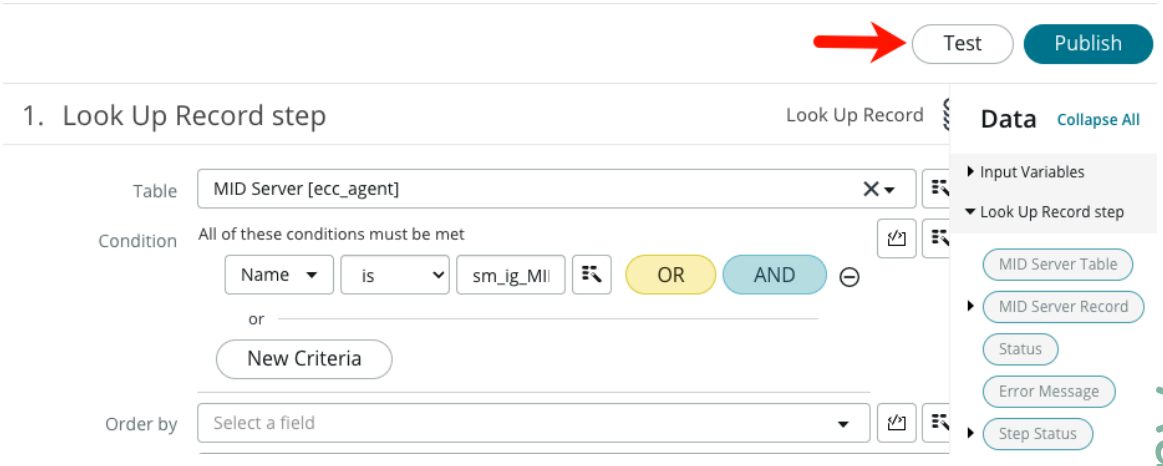
Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie in Flow Designer oben rechts auf dem Bildschirm auf die Schaltfläche **Test**.



2. **Wählen** Sie im Fenster „Testaktion“ die **Option Test ausführen**aus.
3. Wählen Sie **aus. Ihr Test wurde ausgeführt. Zeigen Sie die Ausführungsdetails der Aktion an.**
4. Aktualisieren Sie Ihren Bildschirm, bis oben rechts auf dem Bildschirm **Testlauf – Abgeschlossen** angezeigt wird.
5. Klicken Sie unten links auf dem Bildschirm auf den Pfeil **Schritte**.
6. Scrollen Sie nach unten, bis eine Überschrift **Schrittausgabedaten** mit der folgenden Erfolgsmeldung angezeigt wird:

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. Nachdem Sie diese Nachricht in Flow Designerangezeigt haben, stellen Sie sicher, dass Ihre Textdatei in Ihrem lokalen System erstellt wurde.

Dashboard „Geheimnisverwaltung“.

Verwenden Sie das Dashboard für die Geheimnisverwaltung, um die in Ihrer Instanz konfigurierten geheimen Gruppen zu überprüfen und sich über Sicherheitsprobleme zu informieren.

Geheime Gruppenübersicht

Auf der Registerkarte **Geheime** Gruppenübersicht werden Informationen zu Ihren konfigurierten geheimen Gruppen angezeigt. Verwenden Sie diese Registerkarte, um Informationen zu den in Ihrer Instanz konfigurierten geheimen Gruppen anzuzeigen.

Geheime Gruppe nach Typ

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigt ein Kreisdiagramm mit geheimen Gruppen an, die in Ihrer Instanz installiert sind, gruppiert nach Geheimnistyp (Instanzseite der Clientseite).

Geheime Gruppe nach Kriteriumstyp

Zeigt ein Kreisdiagramm mit geheimen Gruppen mit Kriterien an, die in Ihrer Instanz nach dem Typ der verwendeten Kriterien konfiguriert sind.

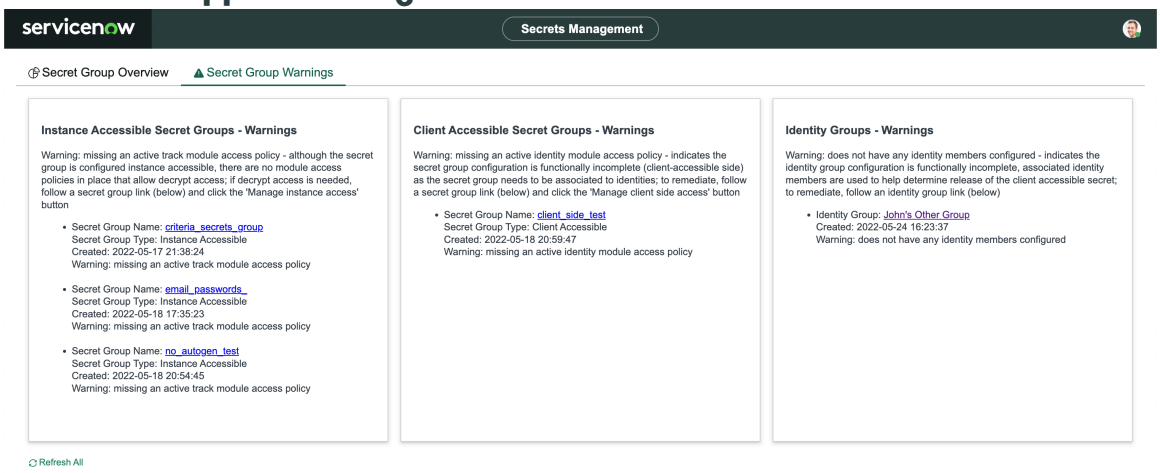
Anzahl der inaktiven Geheimnisgruppen

Zeigt die Anzahl der inaktiven geheimen Gruppen an, die in Ihrer Instanz konfiguriert sind.

Anzahl der dedizierten Geheimnisse.

Zeigt die Anzahl der Geheimnisse in Basis-Geheimnisgruppen an.

Geheime Gruppenwarnungen



Auf der Registerkarte **Geheime** Gruppenwarnungen werden Warnungen im Zusammenhang mit Ihren geheimen Gruppen und Identitätsgruppen angezeigt.

Geheime Gruppen mit Instanzzugriff – Warnungen

Diese Karte zeigt Warnungen an, wenn geheime Gruppen ohne aktive Zugriffsrichtlinien vorhanden sind. Wählen Sie einen geheimen Gruppennamen aus, um diesen Datensatz anzuzeigen.

Für Client zugängliche geheime Gruppen – Warnungen

Diese Karte zeigt Warnungen an, wenn für den Client zugängliche geheime Gruppen vorhanden sind, die keine aktive Identitätsmodul-Zugriffsrichtlinie (MAP) aufweisen. Wählen Sie einen geheimen Gruppennamen aus, um diesen Datensatz anzuzeigen.

Identitätsgruppen – Warnungen

Diese Karte zeigt Warnungen an, wenn Identitätsgruppen vorhanden sind, für die keine Gruppenmitglieder konfiguriert sind. Wählen Sie den Identitätsgruppennamen aus, um den Datensatz anzuzeigen.

Hinweis:
Das Dashboard „Geheimnisverwaltung“ ist Teil von Geheimnisverwaltung Enterprise. Secrets Management Enterprise ist ein kostenpflichtiges Plugin, das Mitarbeiter von ServiceNow in Ihrer Produktionsinstanz aktivieren müssen.

Geheimnisverwaltungsrollen

Mit der Geheimnisverwaltung werden diese Rollen hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheimnisadministrator [sn_secrets.admin]

Weisen Sie anderen Benutzern Nicht-Admin-Secret-Rollen zu. Geheimnisadministratoren haben die gleichen Berechtigungen wie Geheimnismanager und -anzeiger.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Wichtig:
Vermeiden Sie es, eine Administratorrolle zu gewähren, wenn spezialisiertere Rollen verfügbar sind.

- Ein Benutzer muss über die Rollen admin und security_admin verfügen, um die Rolle sn_secret.admin zu erhalten.
- Vermeiden Sie die Gewährung einer Administratorrolle, wenn gezieltere Rollen verfügbar sind.

Geheimnismanager [sn_secrets.manager]

Gewähren Sie diese Rolle Benutzern, die in der Lage sein müssen, eine der folgenden Funktionen auszuführen.

- Geheime und geheime Gruppendatensätze anzeigen
- Zeigen Sie den Zugriffsverlauf und andere Informationen zu Nutzungsaktivitäten an
- Erstellen Sie geheime Gruppen und Filter
- Erstellen Sie Geheimnisanbieter
- Verschieben Sie geheime Schlüssel zwischen geheimen Gruppen
- Ändern Sie die Einstellungen für geheime Gruppe und geheimen Anbieter

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Wichtig:
Geheimnismanager können Geheimnisse nicht im Nur-Text-Format sehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheimnisbetrachter [sn_secrets.viewer]

Gewähren Sie diese Rolle Benutzern, die in der Lage sein müssen, geheime und geheime Gruppendatensätze anzuzeigen.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Erstellen Sie ein kryptografisches Modul für geheime Gruppen

Erstellen Sie ein kryptografisches Modul für geheime Gruppen, um die Verschlüsselung und Entschlüsselung durchzuführen.

Vorbereitungen
Erforderliche Rolle:

- Administrator
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

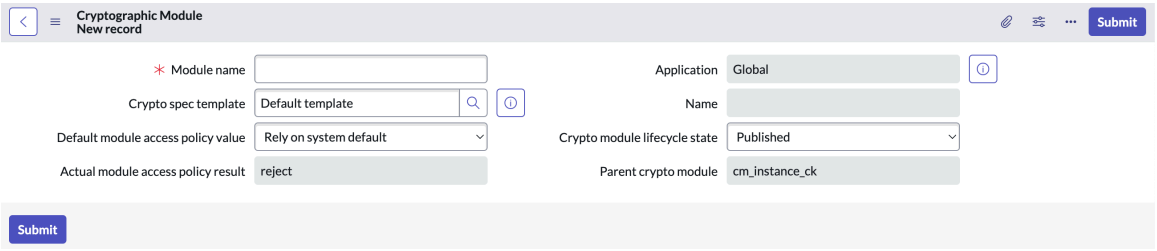
Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Krypto-Modul für geheime Gruppe erstellen**.
2. Wählen Sie den Typ des Gruppen-Krypto-Moduls aus, das Sie erstellen möchten.

Typ des kryptografischen Moduls	Beschreibung
Ein über die Instanz zugängliches Geheimnis-Krypto-Modul erstellen	Erstellen Sie für die Instanz zugängliche geheime Schlüssel, die von Ihrer Instanz entschlüsselt werden können.
Erstellt ein geheimes Krypto-Modul, auf das der Client zugreifen kann	Erstellen Sie für den Client zugängliche geheime Schlüssel, die mit Ihrem eigenen Schlüssel verschlüsselt werden, auf den ServiceNow nicht zugreifen kann.

3. Füllen Sie die Felder im Formular **„Kryptografisches Modul** “ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Modulname	Beschreibender Name für Ihr Modul
Anwendung	Anwendungsbereich, der Ihr Modul enthält. Dieses Feld wird automatisch mit dem aktuellen Modul ausgefüllt.
Krypto-Spezifikationsvorlage	**Standardvorlage** ist standardmäßig ausgewählt.
Name	Name des Moduls. Dieser Name wird basierend auf dem Anwendungs- und Modulnamen automatisch von generiert.
Standardwert der Modulzugriffsrichtlinie	○ Systemvorgabe verwenden ○ Ablehnen ○ Titel
Lebenszyklusstatus kryptografisches Modul	Gibt an, ob sich das Modul im Status „ **Entwurf“** oder **„Veröffentlicht** “ befindet.
Tatsächliches Ergebnis der Modulzugriffsrichtlinie	Dieses Feld dient zu Informationszwecken und ist schreibgeschützt.
Übergeordnetes kryptografisches Modul	Das übergeordnete kryptografische Modul, das durch den im vorherigen Schritt ausgewählten kryptografischen Modultyp bestimmt wird. Dieses Feld ist schreibgeschützt.

4. Wählen Sie **Absenden**.

Erstellen Sie eine geheime Basisgruppe

Erstellen Sie eine Basis-Geheimnisgruppe, um alle Geheimnisse unabhängig von ihren Kriterien zu gruppieren.

Vorbereitungen

Erforderliche Rolle: admin

Grundlegende Geheimnisgruppen können jedes Geheimnis enthalten, das Sie ihnen hinzufügen, unabhängig von Tabelle, Bereich oder Anwendung. Nach der Erstellung fügen Sie der Gruppe manuell Geheimnisse hinzu. Um eine Gruppe speziell für alle geheimen Schlüssel zu erstellen, die ein gemeinsames Attribut verwenden, erstellen Sie mithilfe der Anweisungen in Erstellen Sie eine geheime Gruppe mit Kriterieneine geheime Gruppe mit Kriterien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**.
2. Wählen Sie **Neu**.
3. Im **Feld Welche Art von geheimer Gruppe möchten Sie erstellen?** Wählen Sie **Basisgeheime Gruppe**aus.
4. Füllen Sie die Felder im Formular **„Geheime Gruppe“** aus.

Geheime Gruppenfelder

Feld	Beschreibung
Gruppenname	Name der Gruppe **Hinweis:** Geheime Gruppennamen dürfen nur Kleinbuchstaben, Ziffern und Unterstriche (_) enthalten.
Geheimnistyp	Gibt an, ob die Gruppe **über Instanzzugriff** oder **Clientzugriff verfügt**.
Autogen-Modul	Generiert ein neues kryptografisches Modul für diese geheime Gruppe. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist standardmäßig aktiviert.
Anwendung	Die bereichsbezogene Anwendung für diesen Datensatz. Dieses schreibgeschützte Feld wird automatisch mit dem aktuellen Bereich ausgefüllt.
Kurzbeschreibung	Beschreibung der Gruppe
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das mit dieser Gruppe verwendet werden soll. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist nur sichtbar, wenn **Autogen-Modul** nicht ausgewählt ist. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über Modulzugriffsrichtlinien **Hinweis:** Sie können die Modulzugriffsrichtlinien für Ihre geheime Gruppe mithilfe der Schaltfläche **Instanzzugriff verwalten** überprüfen.

5. Klicken Sie auf **Absenden**.

Hinweis:
Nach der Erstellung ist eine geheime Gruppe standardmäßig inaktiv. Kehren Sie zum Gruppendatensatz zurück, und wählen Sie **Aktiv** aus, um die Gruppe zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine geheime Gruppe mit Kriterien

Erstellen Sie eine Geheimnisgruppe mit Kriterien, um in Passwort2-Felder eingegebene Geheimnisse automatisch zu organisieren, wenn sie gemeinsame Kriterien wie Tabelle, Bereich oder Anwendung verwenden.

Vorbereitungen

Erforderliche Rolle: admin

Geheimnisse innerhalb dieses Typs von geheimen Gruppen müssen gemeinsame Kriterien aufweisen. Erwägen Sie für Gruppen ohne diese Einschränkung die Erstellung einer Gruppe mit Basisgeheimnissen. Erfahren Sie mehr über das Erstellen einer geheimen Basisgruppe in Erstellen Sie eine geheime Basisgruppe.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**.
2. Wählen Sie **Neu**.
3. Im **Feld Welche Art von geheimer Gruppe möchten Sie erstellen?** Wählen Sie **Geheime Gruppe mit Kriterien**aus.
4. Füllen Sie die Felder im Formular **„Geheime Gruppe“** aus.

Geheime Gruppenfelder

Feld	Beschreibung
Gruppenname	Name der Gruppe **Hinweis:** Geheime Gruppennamen dürfen nur Kleinbuchstaben, Ziffern und Unterstriche (_) enthalten.
Geheimnistyp	Gibt an, ob die Gruppe **über Instanzzugriff** oder **Clientzugriff verfügt.**
Autogen-Modul	Generiert ein neues kryptografisches Modul für diese geheime Gruppe. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist standardmäßig aktiviert.
Anwendung	Die bereichsbezogene Anwendung für diesen Datensatz. Dieses schreibgeschützte Feld wird automatisch mit dem aktuellen Bereich ausgefüllt.
Kurzbeschreibung	Beschreibung der Gruppe
Kriteriumstyp	Die Kriterien, die die Geheimnisse in dieser Gruppe gemeinsam nutzen. ○ Umfang ○ Paket ○ Zieltabelle ○ Geheime Spalte ○ Filterdatensatz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das mit dieser Gruppe verwendet werden soll. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist nur sichtbar, wenn **Autogen-Modul** nicht ausgewählt ist. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über Modulzugriffsrichtlinien **Hinweis:** Sie können die Modulzugriffsrichtlinien für Ihre geheime Gruppe mithilfe der Schaltfläche **Instanzzugriff verwalten** überprüfen.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

Hinweis:
Nach der Erstellung ist eine geheime Gruppe standardmäßig inaktiv.

6. Nach dem Speichern des Datensatzes werden möglicherweise zusätzliche Felder angezeigt, je nachdem, wie Sie Ihre Gruppe konfiguriert haben.

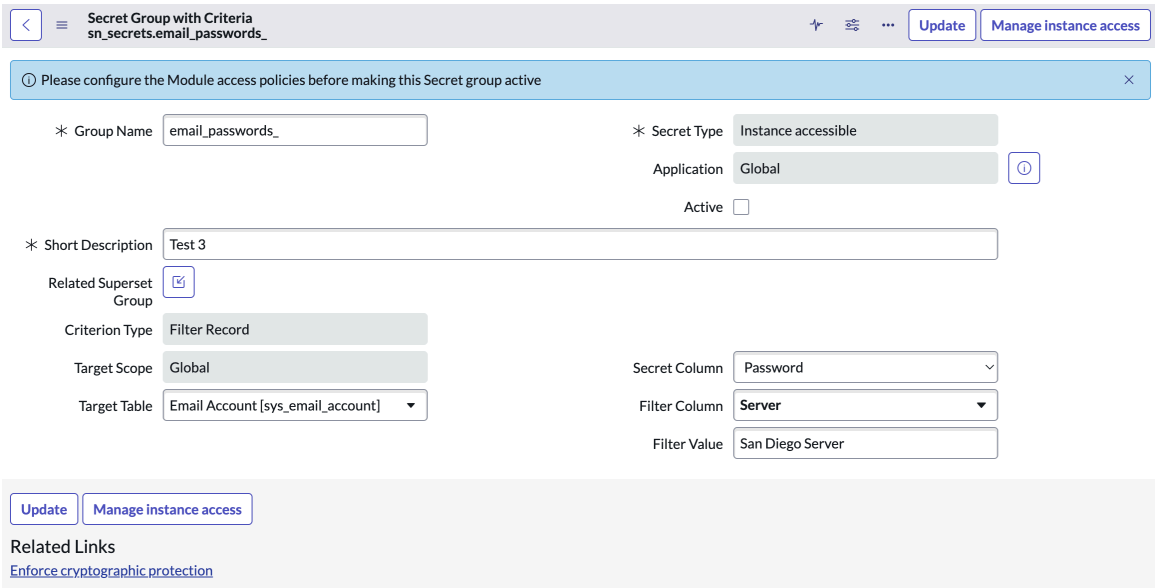
Zusätzliche geheime Gruppenfelder

Feld	Beschreibung
Zielbereich	Bereich, der von den dieser Gruppe zugewiesenen Geheimnissen gemeinsam verwendet wird. Dieses Feld ist nur verfügbar, wenn Sie im Feld **Kriterientyp** die Option Umfang auswählen.
Zielpaket	Paket, das von den dieser Gruppe zugewiesenen Geheimnissen gemeinsam genutzt wird. Dieses Feld ist nur verfügbar, wenn Sie im Feld **Kriterientyp** die Option Paket auswählen.
Zieltabelle	Tabelle, die von den dieser Gruppe zugewiesenen Geheimnissen gemeinsam verwendet wird. Dieses Feld ist nur verfügbar, wenn Sie im Feld **Kriterientyp** die Option Tabelle oder Geheime Spalte auswählen.
Zielbereich	Anwendungsbereich der im Feld Zieltabelle ausgewählten **Tabelle**. Dieses Feld ist nur sichtbar, wenn Sie im Feld **Kriterientyp**die Option Tabelle, Filterspalte oder Geheime Spalte auswählen.
Geheime Spalte	Tabellenspalte, die die pasword2-Geheimnisse enthält, die Sie in diese Gruppe aufnehmen. Die in dieser Liste verfügbaren Felder werden durch die im Feld Zieltabelle ausgewählte **Tabelle** bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn in der Auswahltabelle keine Spalten vorhanden sind, die Geheimnisse enthalten, wird in diesem Feld nur „ Keine“ als Auswahl angezeigt.
Spalte filtern	Die Spalte in der unter Zieltabelle ausgewählten **Tabelle**, die Sie als Filter verwenden möchten. Dieses Feld darf kein Passwort2-Feld sein.
Filterwert	Der Wert, den Sie als Filter verwenden möchten. Dieser **Filter** gilt für das Feld, das im Feld Filterspalte ausgewählt wird.

Example: Eine über die Instanz zugängliche Gruppe, die alle E-Mail-Account-Passwörter für einen E-Mail-Server enthält



Nächste Maßnahme

Nach dem Erstellen Ihrer Gruppe werden alle neuen Datensätze, die den Kriterien entsprechen, verschlüsselt. Um vorhandene Datensätze mit diesem kryptografischen Gruppenmodul zu verschlüsseln, müssen Sie einen Sicherheitsauftrag ausführen. Details finden Sie unter Führen Sie Sicherheitsaufträge für die Geheimnisverwaltung aus.

Vom Client zugängliche Gruppen benötigen einen vom Kunden bereitgestellten öffentlichen Schlüssel, um Ihre geheimen Schlüssel zu verschlüsseln. Schritte zum Hochladen dieses Schlüssels finden Sie unter Laden Sie einen öffentlichen Schlüssel für die Geheimnisverwaltung hoch.

Laden Sie einen öffentlichen Schlüssel für die Geheimnisverwaltung hoch

Laden Sie einen öffentlichen Schlüssel für hoch, um Ihre geheimen Schlüssel zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**, und öffnen Sie den geheimen Gruppendatensatz.
2. Klicken Sie im Datensatz auf die Schaltfläche **Clientseitigen Zugriff verwalten**.
   Ein neuer Identitätsgruppendatensatz wird geöffnet.
3. Klicken Sie auf die Schaltfläche **Identitätsschlüssel** hochladen.
   Das Fenster **„Identität des öffentlichen Schlüsselzertifikats importieren** “ wird angezeigt.
4. Geben Sie einen Alias für Ihren Schlüssel in das Feld **Identitätsschlüssel-Alias** ein.
5. Klicken Sie auf die Schaltfläche **Importieren**, um den Schlüssel aus Ihrer lokalen Umgebung hochzuladen.
6. Klicken Sie auf die Schaltfläche **OK**.
   Das Feld **Gruppenmodulschlüssel** verwendet den Identitätsschlüssel-Aliasnamen.
7. Wählen Sie **Absenden** aus, um den Datensatz der Identitätsgruppe zu speichern.

Führen Sie Sicherheitsaufträge für die Geheimnisverwaltung aus

Planen Sie einen Geheimnisverwaltungsauftrag, um Verschlüsselungsaufgaben für Geheimnisfelder in Ihrer Instanz auszuführen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin, security_admin und sn_secrets.admin

Um diese Schritte auszuführen, müssen Sie eine Erhöhung auf die Rolle security_admin durchführen. Weitere Informationen zu diesem Vorgang finden Sie unter Auf eine privilegierte Rolle erweitern

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen**.
2. Im **Feld Welche Art von Sicherheitsauftrag möchten Sie erstellen?** Wählen Sie in der Eingabeaufforderung **Geheimnisverwaltungsauftrag**aus.
3. Füllen Sie die Felder des Formulars aus.

Formular „Geheimnisverwaltungsauftrag“.

Feld	Beschreibung
Name	Name des Sicherheitsauftrags
Status	Der Anfangsstatus des Auftrags ist „Neu“. Nachdem die Aufgabe wie geplant ausgeführt wurde, wird der Status entsprechend aktualisiert
Zeitfensterstart	Startzeit für die Aufgabe im 24-Stunden-Format. Die Ausführung der Aufgabe beginnt zum ausgewählten Zeitpunkt.
Zeitfensterende	Endzeit für die Aufgabe im 24-Stunden-Format. Wenn die Aufgabe bis zu diesem Zeitpunkt nicht abgeschlossen ist, wird sie während des nächsten angegebenen Verarbeitungsfensters fortgesetzt, bis die Aufgabe abgeschlossen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Durchsetzungsebene	Ob die Aufgabe alle Tabellen oder eine Auswahl bestimmter Tabellen oder Felder betrifft. Wählen Sie aus folgenden Möglichkeiten aus: ○ Alle Tabellen ○ Bestimmte Tabellen ○ Bestimmte Felder ○ Bestimmte Pakete **⚠ Warnung:** Die Auswahl der Option **Alle Tabellen** kann sich auf die Instanzleistung auswirken. Erwägen Sie die Planung außerhalb der Spitzenzeiten.
Pakete	Die Pakete, die in diesen Job aufgenommen werden sollen. Die Verschlüsselung wird auf ausgewählte Pakete angewendet. Diese Option wird nur angezeigt, wenn das Feld **Durchsetzungsebene** auf **Bestimmte Pakete**festgelegt ist
Tabellen	Die Tabellen, die in diesen Auftrag aufgenommen werden sollen. Die Verschlüsselung wird auf alle zutreffenden Felder in den ausgewählten Tabellen angewendet. Diese Option wird nur angezeigt, wenn **Durchsetzungsebene** auf **Spezifische Tabellen**festgelegt ist
Felder	Die Tabellen, die in diesen Auftrag aufgenommen werden sollen. Die Verschlüsselung wird auf alle ausgewählten Felder angewendet. Diese Option wird nur angezeigt, wenn **Durchsetzungsebene** auf **Bestimmte Felder**festgelegt ist
Auftragsmodus	Wählen Sie aus folgenden Möglichkeiten aus: **Password2 an Geheimnisverwaltung** Verschlüsseln Sie alle password2-Felder in Ihren geheimen Gruppen mit den kryptografischen Modulen, die in der Modulzugriffsrichtlinie jeder Gruppe definiert sind. **Geheimnisverwaltung an Password2** Verschlüsseln Sie Daten in Ihren geheimen Gruppen erneut mit Passwort2-Verschlüsselung. Weitere Informationen zu diesem Verschlüsselungstyp finden Sie unter Password2-Verschlüsselung mit KMF. **Durchsetzung geheimer Gruppen** Fragt alle Daten ab, die mit der im Feld **Geheime**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Gruppe ausgewählten Gruppe übereinstimmen müssen. Wenn sich alle von der Abfrage gefundenen Daten bereits in der Gruppe befinden, nimmt die Aufgabe keine Änderungen vor. Wenn die Abfrage Daten findet, die sich noch nicht in der Gruppe befinden, verschlüsselt der Auftrag diese Daten innerhalb der geheimen Gruppe erneut. **Hinweis:** Wenn die in dieser Abfrage gefundenen Daten bereits verschlüsselt sind und Ihre Instanzen diese Daten nicht entschlüsseln können, werden sie nicht verschlüsselt und der geheimen Gruppe hinzugefügt.
Geheimnisgruppe	Geheimnisgruppe, die die zu verschlüsselnden Geheimnisse enthält. Dieses Feld ist nur verfügbar, wenn **Geheime Gruppe** im Feld **Auftragsmodus** ausgewählt ist.
Neueingabe von Daten erzwingen	
Zusammenfassung	Zeigt Informationen zum Fortschritt des Auftrags an. Die Zusammenfassung zeigt auch Datensätze an, die vom Job nicht verschlüsselt werden konnten.

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Der Job fragt alle Daten ab, die der ausgewählten geheimen Gruppe entsprechen müssen. Wenn sich alle von der Abfrage gefundenen Daten bereits in der Gruppe befinden, nimmt die Aufgabe keine Änderungen vor. Wenn die Abfrage Daten findet, die sich noch nicht in der Gruppe befinden, verschlüsselt der Auftrag diese Daten innerhalb der geheimen Gruppe erneut. (Wenn die Instanz sie entschlüsseln kann, was bei clientseitig verschlüsselten Geheimnissen möglicherweise nicht der Fall ist).

ServiceNow Vault

Verwenden Sie die ServiceNow Vault-Produktreihe von Datensicherheitstools, um vertrauliche Daten während ihres gesamten Lebenszyklus vor unbefugtem Zugriff, Beschädigung oder Diebstahl zu schützen. Wenden Sie Schutzmaßnahmen wie Verschlüsselung, Geheimnisverwaltung und Datenschutz zur Schwärzung und Prüfung vertraulicher Informationen an. Die Homepage von ServiceNow Vault stellt einen zentralen, gut erreichbaren Ausgangspunkt dar, um nach ServiceNow Vault-Datensicherheitsprodukten zu suchen und zu ihnen navigieren.

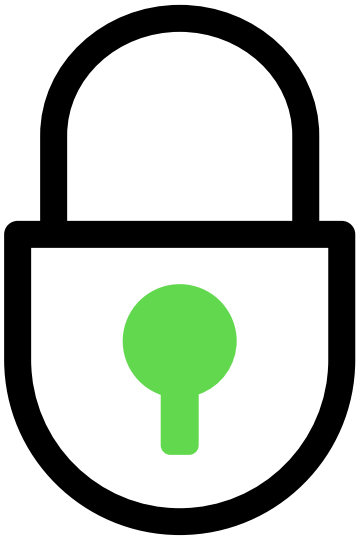
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Vault ist ein kostenpflichtiges Plugin, das von ServiceNow-Mitarbeitern in Ihrer Produktionsinstanz aktiviert werden muss. ServiceNow Vault enthält die nachfolgend aufgelisteten Komponenten.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste **Alle Anwendungen** in Ihrer Instanz aktivieren.

ServiceNow Vault-Komponenten

Verschlüsselung



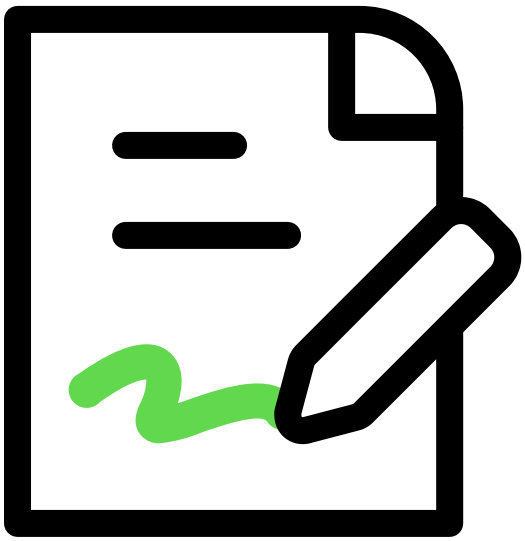
Key Management and Column Level Encryption ist eine Suite hochgradig konfigurierbarer Verschlüsselungsmodule

Geheimnisverwaltung

Lösung zum Ersetzen von hartcodierten Geheimnissen wie Passwörtern, Zertifikaten und API-Schlüsseln auf der -Plattform durch die Verwahrung von Geheimnissen durch den Kunden.

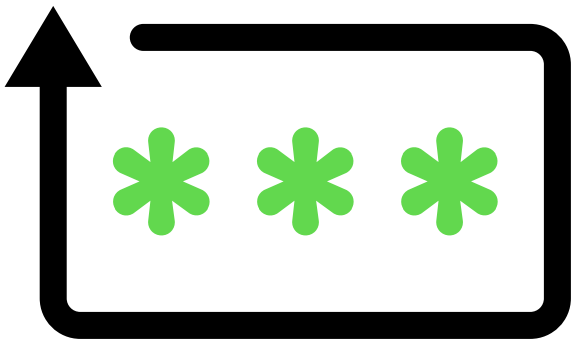
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur



Tragen Sie zur Erhöhung der Sicherheit bei, indem Sie sensible Anwendungskonfigurationsdaten und Skripts validieren, bevor sie verwendet werden.

Datenschutz



Verwenden Sie das Plugin „Data Privacy“, um personenbezogene Daten aus Benutzerdaten zu entfernen, wenn diese von einer Produktionsinstanz in eine Nicht-Produktionsinstanz migriert werden.

Daten-Discovery

Mit dem Plugin „Data Discovery“ können Sie personenbezogene Daten aus Benutzerdaten ermitteln. Die Daten können dann für weitere Sicherheitsmaßnahmen klassifiziert werden.

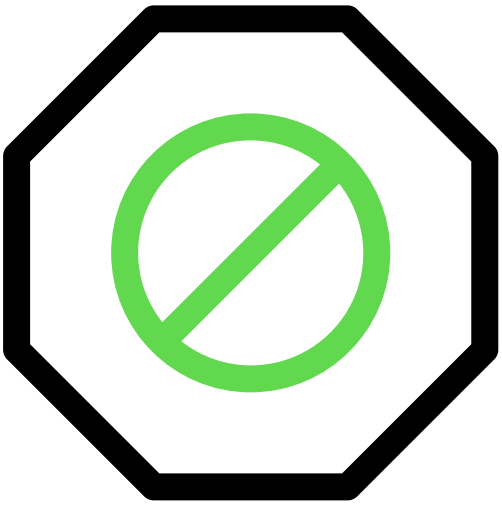
Protokolle

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbessern Sie Sicherheit, Leistung und Benutzer-Experience, indem Sie [qa: BEGIN review][End]ServiceNow-Protokolldaten mit dem Log Export Service in Enterprise Log Analytics importieren.

Zero Trust-Zugriff



[qa: BEGIN review][End]ServiceNow-Sitzungszugriff ermöglicht Organisationen, Benutzerberechtigungen in einer Websitzung dynamisch zu reduzieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

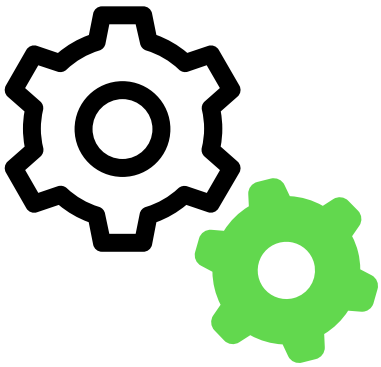
Plattform-Datenschutz

Mit Privacy können Sie vertrauliche Daten in der Instanz maskieren.

Sys-Sicherheits-ACL

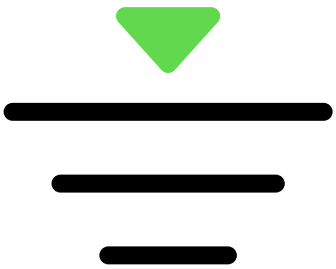
Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Benutzern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Datenklassifizierung



Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

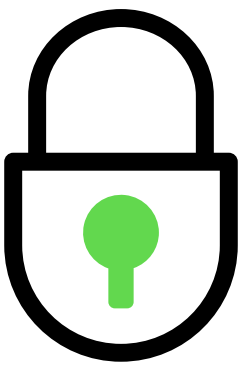
Datenfilterung



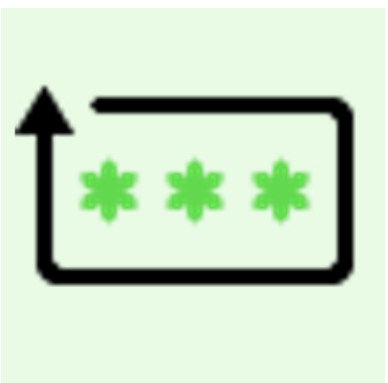
Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

Domain Separation

Datenschutz



Daten-Discovery



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit der ServiceNow -Plattform können Service Provider (SPs) ihren Kunden ein schnelleres Onboarding bieten, die Compliance erfüllen und ihre Daten durch Domänentrennung schützen.

Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren.

Identifizieren Sie mithilfe der Datenerkennung vertrauliche Daten innerhalb einer Instanz, um sie zu klassifizieren, zu schützen oder Berichte über sie zu erstellen.

Zugriffskontrolllistenregeln

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Benutzern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Erkunden

Erfahren Sie mehr über ACL.

Konfigurieren

Konfigurieren Sie die ACL.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz

Ruft Details zu Contextual Security Manager ab.

Erweitert

Erfahren Sie mehr über erweiterte ACL.

Durchsuchen von Zugriffssteuerungslisten

Erkunden Sie Zugriffssteuerungslisten (ACLs).

Komponenten von ACLs

Alle Regeln der Zugriffskontrollliste geben Folgendes an:

- Das *Objekt* und der *Vorgang*, die gesichert werden
- Die für den Zugriff auf das Objekt erforderlichen *Berechtigungen*

Das *Objekt* ist das Ziel, für das der Zugriff gesteuert werden muss. Jedes Objekt besteht aus einem Typ und einem Namen, der eine bestimmte Tabelle, ein bestimmtes Feld oder einen bestimmten Datensatz eindeutig identifiziert.

Alle diese Einträge geben beispielsweise ein Objekt an:

Typ	Name	Objekt gesichert
record	[incident].[--Keine--]	Die Incident-Tabelle.
record	[incident].[aktiv]	Das Feld Aktiv in der Incident-Tabelle.
REST_Endpunkt	user_role_inheritance	Der Datensatz für die Scripted REST API user_role_inheritance.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder *Vorgang* beschreibt eine gültige *Aktion*, die das System für das angegebene Objekt ausführen kann. Einige Objekte, z. B. Datensätze, unterstützen mehrere Vorgänge, während andere Objekte, z. B. ein REST_Endpoint, nur einen Vorgang unterstützen.

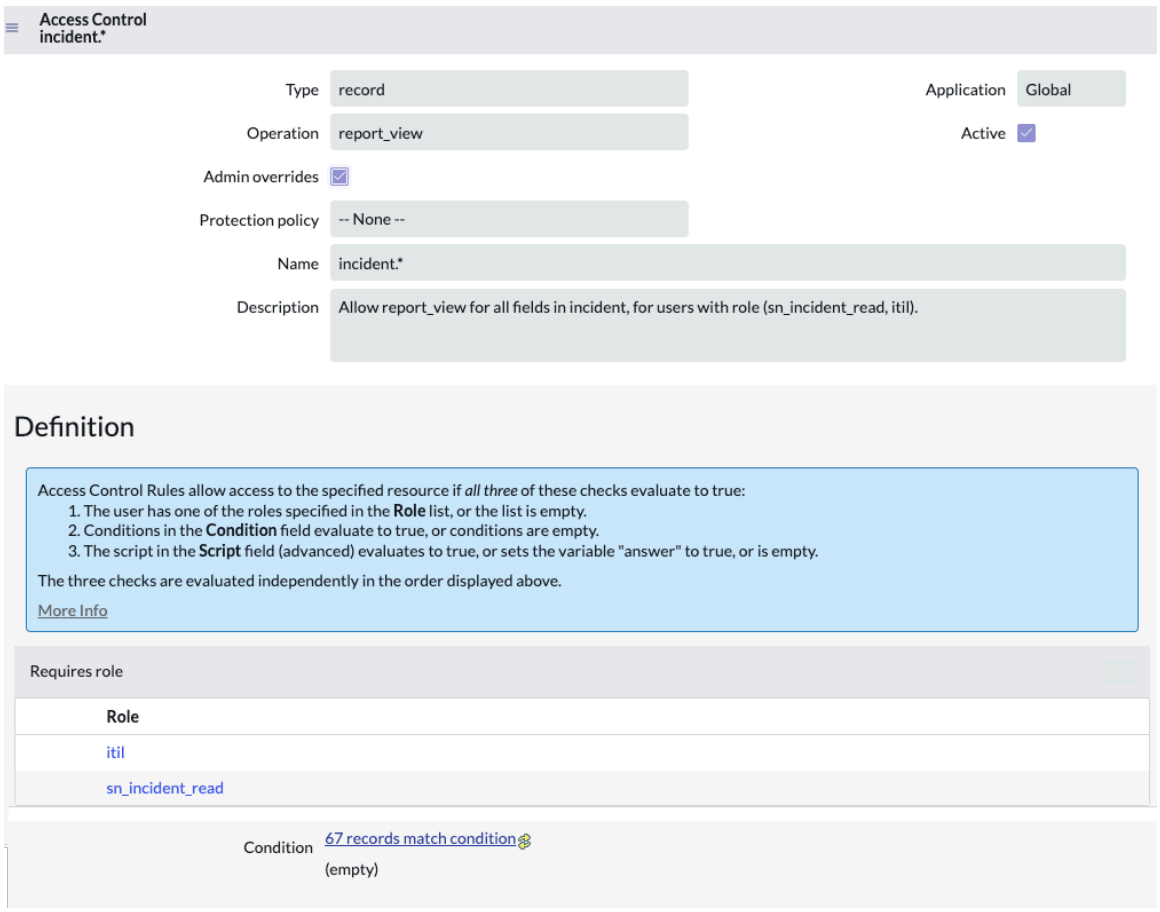
Alle diese Einträge geben beispielsweise einen Vorgang an:

Typ	Name	Vorgang	Vorgang gesichert
record	[incident].[--Keine--]	Erstellen	Erstellen von Datensätzen in der Incident-Tabelle.
record	[incident].[aktiv]	write	Das Feld Aktiv in der Incident-Tabelle wird aktualisiert.
REST_Endpunkt	user_role_inheritance	ausführen	Ausführen der geskripteten REST-API user_role_inheritance.

Die *Berechtigungen* geben an, wann jemand auf das benannte Objekt und den Vorgang zugreifen kann. Sicherheitsadministratoren können Berechtigungsanforderungen angeben, indem sie Folgendes hinzufügen:

- Eine oder mehrere Benutzerrollen für die Liste **„Erfordert Rollen“**
- Eine oder mehrere Bedingungen.
- Ein Skript, das als „true“ oder „false“ ausgewertet wird oder die `Antwortvariable` auf „true“ oder „false“ setzt.

Um Zugriff auf ein Objekt und einen Vorgang zu erhalten, muss ein Benutzer alle in einer Zugriffssteuerung aufgeführten Berechtigungen übergeben. Diese Zugriffssteuerung schränkt beispielsweise den Zugriff zum Anzeigen von Vorgängen in der Incident-Tabelle ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um einen Datensatz in der Incident-Tabelle zu aktualisieren, muss ein Benutzer über die aufgelisteten Rollen verfügen und der Datensatz muss die Bedingung erfüllen.

Berechtigungstyp	Anforderung	Beschreibung
Erfordert Rolle	**Erfordert Rolle**:itil	Lassen Sie nur Benutzer mit der Rolle itil zu, Incidents zu aktualisieren.
Bedingung	[Incident-Status] [ist nicht] [Geschlossen]	Lassen Sie nur Aktualisierungen für aktive Incident-Datensätze zu.

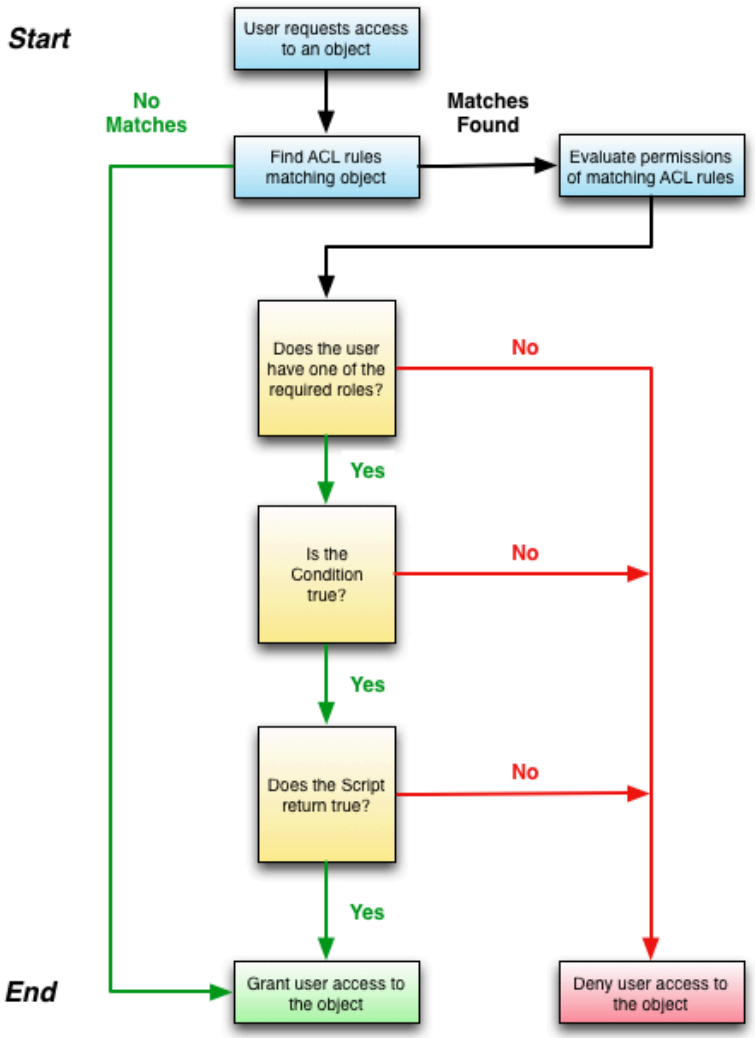
ACL-Auswertungsprozess

Eine ACL-Regel gewährt einem Benutzer nur dann Zugriff auf ein Objekt, wenn der Benutzer alle für die entsprechende ACL-Regel erforderlichen Berechtigungen erfüllt.

- Die Bedingung muss als „ *true*“ ausgewertet werden.
- Das Skript muss als „ *true* “ ausgewertet werden oder eine Antwortvariable mit dem Wert „ *true*“ zurückgeben.
- Der Benutzer muss eine der Rollen in der Liste der erforderlichen Rollen haben. Wenn die Liste leer ist, wird diese Bedingung als „ *true*“ ausgewertet.
- [Nur Datensatz-ACL-Regeln] Die übereinstimmenden ACL-Regeln auf Tabellenebene und Feldebene müssen beide als „ *true*“ ausgewertet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Bewertungsberechtigungen



Immer wenn eine Sitzung Daten anfordert, sucht das System nach Zugriffskontrollregeln, die dem angeforderten Objekt und Vorgang entsprechen. Wenn eine übereinstimmende Zugriffskontrollregel vorhanden ist, wertet das System aus, ob der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf das Objekt und den Vorgang verfügt. Wenn eine Zugriffskontrollregel mehr als eine Berechtigung angibt, muss der Benutzer alle Berechtigungen erfüllen, um Zugriff auf das Objekt und den Vorgang zu erhalten. Wenn eine Berechtigungsprüfung fehlschlägt, kann der Benutzer nicht auf das übereinstimmende Objekt und den übereinstimmenden Vorgang zugreifen.

Wenn ein Benutzer die Berechtigungen der ersten Übereinstimmungsregel nicht erfüllt, wertet das System die Berechtigungen der nächsten übereinstimmenden Zugriffskontrollregel aus, wie in der Verarbeitungsreihenfolge der Zugriffskontrolle angegeben. Wenn der Benutzer die Berechtigungen einer übereinstimmenden Zugriffskontrollregel nicht erfüllt, verweigert das System den Zugriff auf das angeforderte Objekt und den angeforderten Vorgang.

Hinweis:
Wenn für das angeforderte Objekt und den angeforderten Vorgang keine übereinstimmenden Zugriffskontrollregeln vorhanden sind, gewährt das System dem Benutzer Zugriff darauf. In der Praxis kommt es selten vor, dass das System keine übereinstimmenden Regeln findet, da das System über eine Reihe von Standardzugriffskontrollregeln verfügt, die alle Datensatzvorgänge schützen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Auswirkungen der Verweigerung des Zugriffs auf ein Objekt hängen von der ACL-Regel ab, die der Benutzer nicht bestanden hat. Beispiel: Wenn die ACL-Regel eines Lesevorgangs fehlschlägt, kann der Benutzer das Objekt nicht sehen. Abhängig vom gesicherten Objekt blendet die ACL-Regel ein Feld in einem Formular aus, blendet Zeilen in einer Liste aus oder verhindert, dass ein Benutzer auf eine UI-Seite zugreift. Die folgende Tabelle enthält eine vollständige Liste der Ergebnisse einer fehlgeschlagenen ACL-Regel für einen bestimmten Vorgang und Objekttyp.

ACL-Prüfungen vor und nach der Abfrage

Ihre Instanz überprüft ACL-Regeln sowohl vor als auch nach einer Abfrage durch einen Benutzer. Da vor und nach einer Abfrage unterschiedliche Informationen verfügbar sind, können die Ergebnisse unterschiedlich sein.

ACL-Prüfung vor der Abfrage

Bevor Ihre Instanz eine Datenbankabfrage ausführt, überprüft sie die ACL-Regeln für jedes Feld in der abgefragten Tabelle, um zu bestimmen, auf welche Felder ein Benutzer zugreifen darf. Diese Prüfung betrachtet nur die Rollen des Benutzers und prüft, ob diese Rollen den Zugriff auf Felder ermöglichen. Da diese Prüfung vor der Abfrage ausgeführt wird, hat die ACL keinen Zugriff auf die Datensätze in der Tabelle und kann diese Daten daher nicht berücksichtigen. Skripts und Bedingungen, die von der Kenntnis des Inhalts eines Datensatzes abhängig sind, werden nicht ausgewertet.

Wenn der Benutzer zu diesem Zeitpunkt keinen Lesezugriff hat, wird dem Benutzer der Wert für das Feld nicht angezeigt.

ACL-Prüfung nach der Abfrage

Nach der Abfrage überprüft Ihre Instanz jeden von der Abfrage zurückgegebenen Datensatz. Während dieser Prüfung gibt es einen Kontext für die ACL, sodass die Rollen-, Bedingungs- und Skriptteile der ACL ausgewertet werden. Wenn der Benutzer zu diesem Zeitpunkt keinen Lesezugriff hat, wird dem Benutzer der Wert für das Feld nicht angezeigt. Dem Benutzer wird jedoch die Feldbezeichnung angezeigt, wenn seine Rollen den Zugriff auf das Feld zulassen.

Vorgang	Ergebnisse des Fehlschlagens einer ACL-Regel für das Objekt
ausführen	Benutzer können keine Skripts für einen Datensatz oder eine UI-Seite ausführen.
Erstellen	Benutzer können die **neue** UI-Aktion in Formularen nicht sehen. Der Benutzer kann auch keine Datensätze mithilfe von API-Protokollen wie Webservices in eine Tabelle einfügen. Eine **Erstellungs** -ACL mit einer Bedingung, die erfordert, dass ein Feld einen bestimmten Wert enthält, wird immer als „falsch“ ausgewertet. Felder in neuen Datensätzen werden als leer betrachtet, bis der Datensatz gespeichert wird.
gelesen	Anwender kann das Objekt in Formularen oder Listen nicht sehen. Der Benutzer kann Datensätze auch nicht über API-Protokolle wie Webservices abrufen.
write	Benutzer sehen in Formularen und Listen ein schreibgeschütztes Feld und können Datensätze nicht mit API-Protokollen wie Webservices aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang	Ergebnisse des Fehlschlagens einer ACL-Regel für das Objekt
löschen	Benutzer können die UI-Aktion **„Löschen** “ in Formularen nicht sehen. Der Benutzer kann auch keine Datensätze aus einer Tabelle entfernen, indem er API-Protokolle wie Webservices verwendet.
edit_task_relations	Anwender kann keine Beziehungen zwischen Aufgabentabellen definieren.
edit_ci_relations	Benutzer kann keine Beziehungen zwischen Konfigurationselementtabellen [cmdb_ci] definieren.
save_as_template	Wird verwendet, um die Felder zu steuern, die beim Erstellen einer Vorlage gespeichert werden sollen.
add_to_list	Benutzer können bestimmte Spalten in der Listenmechanik nicht anzeigen oder personalisieren.
list_edit	Anwender kann keine Datensätze (Zeilen) aus einer Liste aktualisieren.
report_on	Anwender kann keinen Bericht in der ACL-Tabelle erstellen. Weitere Informationen finden Sie unter Berichterstellung mit einer ACL-Regel einschränken .
report_view	Benutzer können den Inhalt eines Berichts in der ACL-Tabelle oder im ACL-Feld nicht anzeigen. Weitere Informationen finden Sie unter Reporting .
personalize_choices	Benutzer kann nicht mit der rechten Maustaste auf ein Listenfeld klicken und Auswahlmöglichkeiten **konfigurieren**auswählen.

ACL-Übereinstimmungsanforderungen für -Objekte

Objekttyp	Übereinstimmende ACL-Regeln für Zugriff auf Objekt erforderlich	Vorhandene Platzhalter-ACL-Regeln
Vom Client aufrufbare Skripteinbindungen Prozessoren	Benutzer müssen die Berechtigungen von zwei ACL-Regeln erfüllen: 1. Alle Platzhalter-ACL-Regeln für das Objekt (falls eine ACL-Regel für den Vorgang vorhanden ist). 2. Die erste ACL-Regel, die dem Namen des Objekts entspricht (falls eine ACL-Regel für den Vorgang vorhanden ist).	Standardmäßig gibt es keine Platzhalterregeln (*) für diese Objekttypen. Wenn Sie eine Platzhalter-ACL-Regel für eines dieser Objekte erstellen, gilt die ACL-Regel für alle Objekte dieses Typs.
UI-Seiten Datensatz	Benutzer müssen die Berechtigungen von zwei ACL-Regeln erfüllen: 1. Die erste ACL-Regel, die dem Feld des Datensatzes entspricht (falls eine ACL-Regel für den Vorgang vorhanden ist).	Standardmäßig gibt es Platzhalter-Tabellenregeln (*) für die Vorgänge Erstellen, Lesen, Schreiben und Löschen und Platzhalter-Feldregeln (*.*) für die Vorgänge „personalize_choices“, „create“ und „save_as_template“. Wenn Sie eine Tabelle erstellen, erstellen Sie ACL-Regeln für die Tabelle, es sei denn, Sie möchten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objekttyp	Übereinstimmende ACL-Regeln für Zugriff auf Objekt erforderlich	Vorhandene Platzhalter-ACL-Regeln
	2. Die erste ACL-Regel, die der Tabelle des Datensatzes entspricht (falls eine ACL-Regel für den Vorgang vorhanden ist).	die bereitgestellten Platzhalter-ACL-Regeln verwenden.

Hinweis:
Die Eigenschaft Security Manager Standardverhalten (`glide.sm.default_mode`) bestimmt, ob Benutzer auf Objekte zugreifen können, die nur mit ACL-Regeln der Platzhaltertabelle übereinstimmen. Wenn diese Eigenschaft auf *Zugriff verweigern*festgelegt ist, können nur Administratoren auf Objekte zugreifen, die den ACL-Regeln der Platzhaltertabelle entsprechen.

Hinweis:
Die ACL-Regel für Platzhalterfelder (*.*) für den Erstellungsvorgang verwendet dieselben Berechtigungen wie der Schreibvorgang. Dies bedeutet, dass die Erstellungsberechtigungen mit den Schreibberechtigungen identisch sind, es sei denn, Sie definieren eine explizite ACL-Regel für den Erstellungsvorgang.

Mehrere ACL-Regeln am selben Punkt in der Verarbeitungsreihenfolge

Wenn zwei oder mehr Regeln an derselben Stelle in der Verarbeitungsreihenfolge übereinstimmen, muss der Benutzer eine der ACL-Regelberechtigungen übergeben, um auf das Objekt zugreifen zu können. Wenn Sie beispielsweise zwei Feld-ACL-Regeln für `incident.number`erstellen, hat ein Benutzer, der eine Regel übergibt, Zugriff auf das Nummernfeld, unabhängig davon, ob der Benutzer eine andere Feld-ACL-Regel an derselben Stelle in der Verarbeitungsreihenfolge durchlaufen hat.

Erforderliche Rolle

Normale Administratorbenutzer können Zugriffskontrollregeln anzeigen und debuggen. Um jedoch Zugriffskontrollregeln zu erstellen oder vorhandene zu aktualisieren, müssen Administratoren die Berechtigungen für die Rolle security_admin erhöhen. Siehe Führen Sie eine Erhöhung auf eine privilegierte Rolle durch für Anweisungen.

ACL-Regeln in bereichsbezogenen Anwendungen

Sie können ACL-Regeln für Objekte im selben Bereich wie die ACL-Regel erstellen. Sie können ACL-Regeln auch für Tabellen mit mindestens einem Feld erstellen, das sich im selben Bereich wie die ACL-Regel befindet.

Für Tabellen, die sich in einem anderen Bereich als der ACL-Regeldatensatz befinden, sind die Regeltypen beschränkt.

- Sie können eine ACL-Regel für jede Tabelle, UI-Seite oder ein anderes Objekt erstellen, das sich im selben Bereich wie die ACL-Regel befindet.
- Sie können eine ACL für ein Feld erstellen, das sich im selben Bereich wie die ACL-Regel befindet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

  - Wenn sich die Tabelle im selben Bereich befindet, können Sie ein Skript zum Auswerten von Berechtigungen verwenden.
  - Wenn sich die Tabelle in einem anderen Bereich befindet, können Sie kein Skript zum Auswerten von Berechtigungen verwenden.
- Sie können keine ACL-Regeln für Objekte erstellen oder ändern, die sich in einem anderen Bereich befinden als die Anwendung, die Sie in der Anwendungsauswahl ausgewählt haben. Dies schließt das Hinzufügen einer Rolle zu einer ACL in einem anderen Bereich ein.
- Sie können Platzhalter-Tabellenregeln (*) nur im globalen Bereich erstellen.
- Sie können Platzhalter-Feldregeln (*) nur für Tabellen erstellen, die sich im selben Bereich wie die ACL-Regel befinden.

ACL_Regeltypen

Erstellen Sie ACL-Regeln für verschiedene Komponenten des Systems.

Datensatz-ACL-Regeln

Datensatz-ACL-Regeln bestehen aus Tabellen- und Feldnamen.

- Der Tabellenname ist die Tabelle, die Sie sichern möchten. Wenn andere Tabellen aus dieser Tabelle erweitert werden, wird die Tabelle als übergeordnete Tabelle betrachtet. ACL-Regeln für übergeordnete Tabellen gelten für jede Tabelle, die die übergeordnete Tabelle erweitert.
- Der Feldname ist das Feld, das Sie sichern möchten. Einige Felder sind aufgrund der Tabellenerweiterung Teil mehrerer Tabellen. ACL-Regeln für Felder in einer übergeordneten Tabelle gelten für jede Tabelle, die die übergeordnete Tabelle erweitert.

ACL-Regeln können die folgenden Datensatzvorgänge sichern:

Vorgang	Beschreibung
Erstellen	Ermöglicht Benutzern das Einfügen neuer Datensätze (Zeilen) in eine Tabelle.
gelesen	Ermöglicht Benutzern das Anzeigen von Datensätzen aus einer Tabelle.
write	Ermöglicht Benutzern das Aktualisieren von Datensätzen in einer Tabelle.
löschen	Ermöglicht Benutzern das Entfernen von Datensätzen aus einer Tabelle oder das Löschen einer Tabelle.
edit_task_relations	Ermöglicht Benutzern das Erweitern der Aufgabentabelle [task].
edit_ci_relations	Ermöglicht Benutzern das Erweitern der Tabelle „Konfigurationselement“ [cmdb_ci].
save_as_template	Ermöglicht Benutzern das Speichern eines Datensatzes als Vorlage.
add_to_list	Verhindert, dass Benutzer bestimmte Spalten in der Listenmechanik anzeigen oder personalisieren. **Hinweis:** Bedingungen und Skripts werden nicht unterstützt.
list_edit	Ermöglicht Benutzern das Aktualisieren von Datensätzen (Zeilen) aus einer Liste.
report_on	Ermöglicht Benutzern das Erstellen von Berichten zu Tabellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

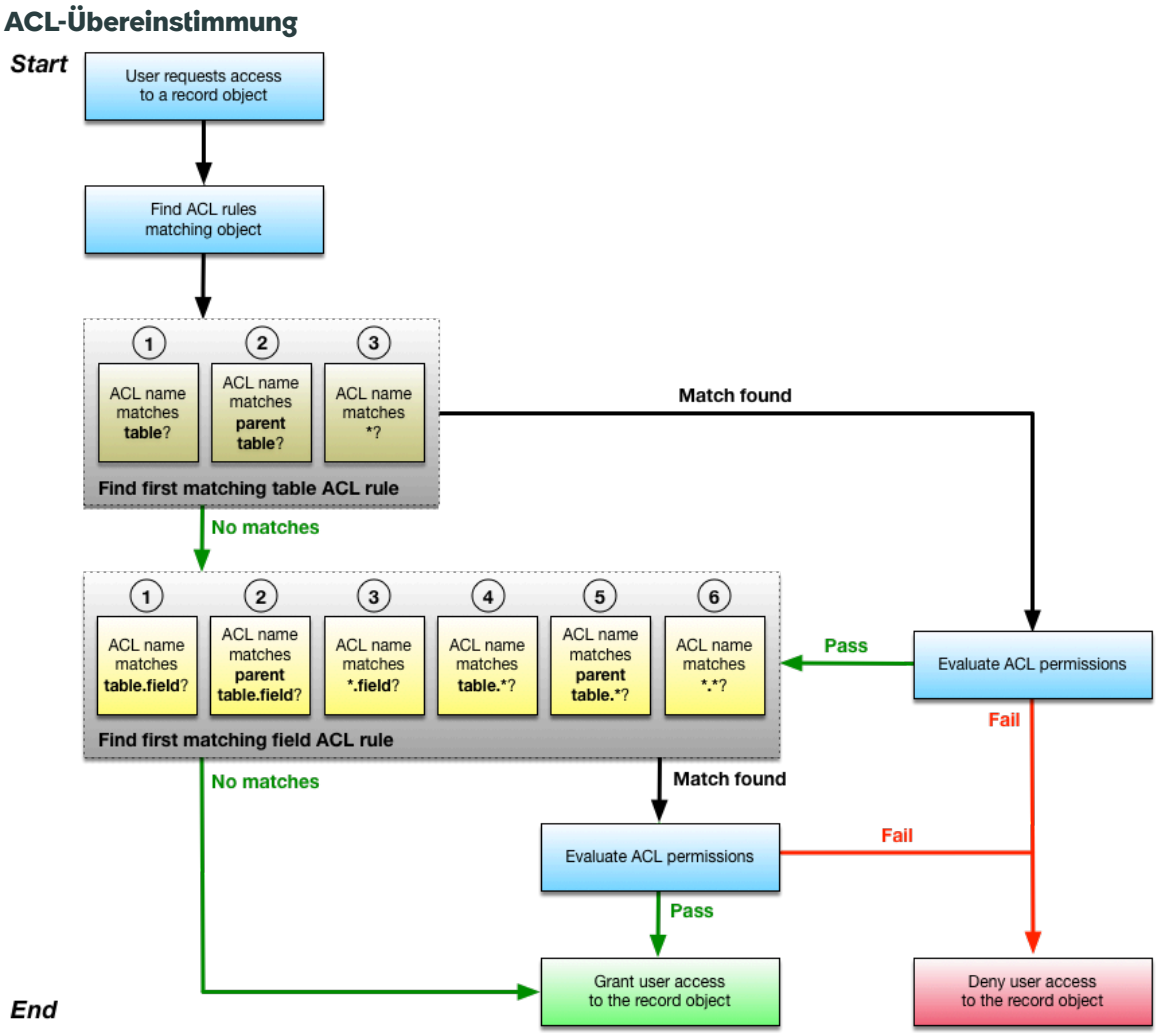
Vorgang	Beschreibung
report_view	Ermöglicht Benutzern das Melden von Feld-ACLs.
personalize_choices	Ermöglicht Benutzern das Konfigurieren der Tabelle oder des Felds.

Datensatz-ACL-Regeln werden in der folgenden Reihenfolge verarbeitet:

- Ordnen Sie das Objekt den ACL-Regeln der Tabelle zu.
- Ordnen Sie das Objekt den Feld-ACL-Regeln zu.

Diese Verarbeitungsreihenfolge stellt sicher, dass Benutzer Zugriff auf spezifischere Objekte erhalten, bevor sie Zugriff auf allgemeinere Objekte erhalten. Ein Benutzer muss sowohl Tabellen- als auch Feld-ACL-Regeln übergeben, um auf ein Datensatzobjekt zuzugreifen.

- Wenn ein Benutzer eine Tabellen-ACL-Regel nicht erfüllt, wird dem Benutzer der Zugriff auf alle Felder in der Tabelle verweigert, auch wenn der Benutzer eine Feld-ACL-Regel übergibt.
- Wenn ein Benutzer eine Tabellen-ACL-Regel übergibt, aber eine Feld-ACL-Regel nicht erfüllt, kann der Benutzer nicht auf das von der Feld-ACL-Regel beschriebene Feld zugreifen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozessor-ACL-Regeln

Prozessor-ACL-Regeln geben den Prozessor an, den Sie sichern möchten. Um eine Liste der verfügbaren Prozessoren zu erhalten, navigieren Sie zu **Systemdefinition** > **Prozessoren**.

Standardmäßig ist eine ACL-Regel für den EmailClientProcessor enthalten, um den E-Mail-Client auf Benutzer mit der itil-Rolle zu beschränken.

Prozessor-ACL-Regeln berücksichtigen die Star-Regel (*), wenn sie keine spezifischere ACL für diese Ressourcen finden können.

Tabellen-ACL-Regeln

Der Benutzer muss zuerst die Tabellen-ACL-Regel übergeben. Da das Basissystem Tabellen-ACL-Regeln des Typs START (*) enthält, die mit jeder Tabelle übereinstimmen, muss der Benutzer immer mindestens eine Tabellen-ACL-Regel übergeben. Das Basissystem enthält zusätzliche Tabellen-ACL-Regeln, um den Zugriff auf bestimmte Tabellen zu steuern.

Tabellen-ACL-Regeln werden in der folgenden Reihenfolge verarbeitet:

1. Ordnen Sie den Tabellennamen zu. Beispiel: Incident.
2. Entspricht dem Namen der übergeordneten Tabelle. Beispiel: Aufgabe.
3. Entspricht einem beliebigen Tabellennamen (*). Beispiel: *.

Wenn ein Benutzer alle Tabellen-ACL-Regeln nicht erfüllt, kann der Benutzer auf keine Felder in der Tabelle zugreifen. Wenn ein Benutzer eine Tabellen-ACL-Regel übergibt, wertet das System die Feld-ACL-Regeln aus.

Feld-ACL-Regeln

Nachdem ein Benutzer eine Tabellen-ACL-Regel übergeben hat, werden Feld-ACL-Regeln in der folgenden Reihenfolge verarbeitet:

1. Ordnen Sie die Tabelle und den Feldnamen zu. Beispiel: incident.number.
2. Ordnen Sie die übergeordnete Tabelle und den Feldnamen zu. Beispiel: task.number.
3. Eine beliebige Tabelle (*) und einen beliebigen Feldnamen abgleichen. Beispiel: *.number.
4. Ordnen Sie die Tabelle und ein beliebiges Feld (*) zu. Beispiel: incident.*.
5. Ordnen Sie die übergeordnete Tabelle und ein beliebiges Feld (*) zu. Beispiel: task.*.
6. Eine beliebige Tabelle (*) und ein beliebiges Feld (*) abgleichen. Beispiel: *.*.

Ein Benutzer muss die Tabellen-ACL-Regel übergeben, um Zugriff auf die Felder der Tabelle zu erhalten. Beispielsweise muss der Benutzer zuerst die Tabellen-ACL-Regel für die Incident-Tabelle übergeben, um in der Incident-Tabelle auf das Feld **Nummer** zugreifen zu können.

Die erste erfolgreiche Feld-ACL-Auswertung stoppt die ACL-Regelverarbeitung auf Feldebene. Wenn ein Benutzer eine Feld-ACL-Regel übergibt, beendet das System die Suche nach anderen übereinstimmenden Feld-ACL-Regeln. Wenn ein Benutzer beispielsweise das Feld ACL-Regel für incident.number übergibt, beendet das System die Suche nach anderen ACL-Regeln, die das Feld **Nummer** in der Incident-Tabelle sichern.

Der Zugriff auf Abfrageinformationen abgeleiteter Daten ist für geschützte Felder eingeschränkt, sodass die Rückgabe von Vorhersageinformationen verhindert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Regeln der UI-Seite

ACL-Regeln für UI-Seiten geben die zu sichernde UI-Seite an. Um eine Liste der verfügbaren UI-Seiten zu erhalten, navigieren Sie zu **System-UI** > **UI-Seiten**. Verwenden Sie beim Definieren einer ACL-Regel für eine UI-Seite den vollständigen Seitennamen. Beispiel: **x_myapp_mypage**.

Hinweis:
Sie können das STERN-Zeichen (*) im Feld **Name** in ACLs vom Typ **„ui_page** “ verwenden, um beliebige UI-Seiten abzugleichen.

ACL-Regeln für UI-Seiten berücksichtigen die STERN-Regel (*), wenn sie keine spezifischere ACL für diese Ressourcen finden können. Wenn Sie beispielsweise eine UI-Seite mit dem Namen „mysecretpage“ haben, aber keine ACL für diese UI-Seite definieren, wird für die Zugriffsprüfung die STERN-Regel (*) für den UI-Seitenprozessor verwendet.

ACL-Regeln können den folgenden UI-Seitenvorgang absichern:

Vorgang	Beschreibung
gelesen	Ermöglicht Benutzern das Anzeigen der UI-Seite.

Vom Client aufrufbare ACL-Regeln für Skripteinbindungen

ACL-Regeln für Skripteinbindungen geben die vom Client aufrufbare Skripteinbindung an, die gesichert werden soll. Um eine Liste der verfügbaren Skripteinbindungen zu erhalten, navigieren Sie zu **Systemdefinition** > **Skripteinbindungen**. Sie können die Liste personalisieren, um die Spalte *„Aufrufbarer Client“ anzuzeigen*.

Das Basissystem enthält keine ACL-Regeln für vom Client aufrufbare Skripteinbindungen.

ACL-Regeln für vom Client aufrufbare Skripteinbindungen berücksichtigen die STERN-Regel (*), wenn sie keine spezifischere ACL für diese Ressourcen finden können.

ACL-Steuerung von Funktionsfeldern

Bei der Auswertung des Zugriffs auf ein Funktionsfeld überprüft das System nicht nur den Zugriff auf das Funktionsfeld selbst, sondern auch den Zugriff auf die beitragenden Felder der Funktion. Beitragende Felder werden als Argumente in einer bestimmten Funktionsdefinition verwendet.

Weitere Informationen zu Funktionsfeldern finden Sie unter Funktionsfeld .

In Rome und früheren Versionen überprüft das System einfach den Zugriff auf das Funktionsfeld selbst (wie bei jedem anderen Feld). Wenn die ACLs in diesem Feld den Zugriff zulassen, erhält der Benutzer den resultierenden Wert, unabhängig davon, ob er Zugriff auf die beitragenden Felder hat.

In Washington DC und höher erfordert das System auch Zugriff auf alle beitragenden Felder, um den Zugriff auf das Funktionsfeld zu ermöglichen. Wenn eine oder mehrere der beitragenden Feld-ACLs den Zugriff verweigern, verweigert auch das Funktionsfeld den Zugriff.

Die einzigen von der neuen Anforderung betroffenen Vorgänge sind „read“ und „report_view“. Für report_view gelten eigene zusätzliche Anforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang	Beschreibung
Lesevorgang	Ein Benutzer hat nur dann Lesezugriff auf ein Funktionsfeld, wenn beide der folgenden Bedingungen zutreffen: • Der Benutzer hat Lesezugriff auf das Funktionsfeld. • Der Benutzer hat Lesezugriff auf alle in der Funktion verwendeten beitragenden Felder.
report_view-Vorgang	Ein Benutzer hat nur dann report_view-Zugriff auf ein Funktionsfeld, wenn alle der folgenden Bedingungen zutreffen: • Der Benutzer hat report_view-Zugriff auf das Funktionsfeld. • Der Benutzer hat report_view-Zugriff auf jedes der beitragenden Felder. • Es gibt eine ACL mit nur Lesezugriff ohne Bedingungen und ohne Skript, und der Benutzer hat diese Rolle. • Der Benutzer hat nur über die Rolle Lesezugriff auf die beitragenden Felder, sodass nur ACLs ohne Bedingung oder Skript dies zulassen können.

Beispiele

Gegeben:

- Tabelle: Gehalt
- Spalten: Basis, Bonus, Summe (in diesem Beispiel sind alle Ganzzahlen)
- Funktionsfeld: Die Gesamtsummenspalte wird als Funktionsfeld mit der Funktionsdefinition `glidefunction:add(base,bonus)`markiert.
- Beitragende Felder: Basis und Bonus, da sie in der Funktionsdefinition verwendet werden
- Rollen: „salary_admin“, „bonus_admin“.

Beispiel 1: Alle Felder erlauben den Zugriff

ACLs	Ergebnis
insgesamt, Basis, Bonus: read und report_view für Rolle „salary_admin“, ohne Bedingungen oder Skripts	Einem Benutzer mit der Rolle „salary_admin“ wird Lese- und report_view-Zugriff auf „Gesamt“ gewährt, da er über die erforderliche Rolle verfügt.

Beispiel 2: Beitragendes Feld verweigert Lesezugriff

ACLs	Ergebnis
• gesamt, Basis: read und report_view für Rolle „salary_admin“, ohne Bedingungen oder Skripts	Einem Benutzer mit der Rolle „salary_admin“ wird der Lese- und report_view-Zugriff auf „total“ verweigert, da Bonus den Lesezugriff auf seine Rolle verweigert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel 2: Beitragendes Feld verweigert Lesezugriff (Fortsetzung)

ACLs	Ergebnis
• Bonus: report_view für Rolle „salary_admin“ , ohne Bedingungen oder Skripts • Bonus: Lesezugriff für die Rolle „bonus_admin“, ohne Bedingungen oder Skripts	

Beispiel 3: Beitragendes Feld ACL hat Skript

ACLs	Ergebnis
• gesamt, Basis: read und report_view für Rolle „salary_admin“, ohne Bedingungen oder Skripts • Bonus: report_view für Rolle „bonus_admin“, ohne Bedingungen oder Skripts • Bonus: Lesezugriff für die Rolle „salary_admin“ mit einem Skript (beachten Sie, dass es keine Rolle spielt, was im Skript enthalten ist, nur dass es vorhanden ist.)	Einem Benutzer mit der Rolle „salary_admin“ wird Lesezugriff auf „Gesamt“ gewährt, da er die erforderliche Rolle für alle Felder hat. Dem gleichen Benutzer mit „salary_admin“ wird jedoch der Zugriff auf „report_view“ verweigert, da die Lese-ACL mit dem Skript den Zugriff für diesen Fall standardmäßig verweigert, obwohl er über die erforderliche Rolle verfügt.

Sicherheits-Jump-Start – Plugin „ACL-Regeln“.

Das Plugin „Security Jump-Start Access Control Level (ACL Rules)“ wird automatisch auf allen neuen Instanzen installiert. Verwenden Sie dieses Plugin, um schnell mehrere Systemtabellen zu sichern und den Produktionsstartprozess für Ihre Organisation zu beschleunigen.

Dieses Plugin ist nicht für vorhandene Instanzen gedacht, da es den Sicherheitszugriff auf Tabellen ändern kann, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator dieses Plugin unbedingt in einer vorhandenen Instanz installieren möchte, wird empfohlen, es zuerst in einer Testinstanz gründlich zu testen. Dadurch wird die Kompatibilität mit der aktuellen Implementierung der Organisation sichergestellt.

Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die von diesem Plugin bereitgestellt werden, kann er manuell eine oder mehrere in einer vorhandenen Instanz erstellen, indem er die Liste der ACLs als Richtlinie verwendet.

Die folgenden ACLs sind in diesem Plugin enthalten. Wählen Sie das Symbol in einer Kopfzeile aus, um diese Spalte in aufsteigender oder absteigender Reihenfolge zu sortieren. Die Betriebstaste lautet wie folgt:

- R = lesen
- W = schreiben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- D = löschen
- C = erstellen

Name	Vorgang	Beschreibung
cmdb_ci	WCD	„asset“- oder „itil“-Rolle, die zum Schreiben/Erstellen/Löschen von Konfigurationselement-Datensätzen erforderlich ist
cmn_department	WD	Rolle „user_admin“ zum Schreiben/Löschen von Abteilungsdatensätzen erforderlich
cmn_location	WC	Rolle „user_admin“ zum Schreiben/Erstellen von Standortdatensätzen erforderlich
core_company	WD	Rolle „user_admin“ zum Schreiben/Löschen von Unternehmensdatensätzen erforderlich
kb_knowledge	Erstellen	Wissensrolle, die zum Erstellen von Wissensdatensätzen erforderlich ist
ldap_ou_config	RWCD	Rolle user_admin zum Lesen/Schreiben/Erstellen/Löschen von LDAP-OU-Definitionsdatensätzen erforderlich
ldap_server_config	RWCD	Rolle „user_admin“ zum Lesen/Schreiben/Erstellen/Löschen von LDAP-Server-Datensätzen erforderlich
process_guide	WCD	Administratorrolle, die zum Schreiben/Erstellen/Löschen von Prozessleitfaden-Datensätzen erforderlich ist
process_step	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Prozessschritt-Datensätzen erforderlich
sc_category	Erstellen	Rolle „catalog_admin“ zum Erstellen von Servicekatalog-Kategoriedatensätzen erforderlich
sc_category	löschen	Rolle „catalog_admin“ zum Löschen von Servicekatalog-Kategoriedatensätzen erforderlich
sc_category	write	Rolle „catalog_admin“ zum Schreiben in Servicekatalog-Kategoriedatensätze erforderlich
Katalogelement	write	Rolle „catalog_admin“ zum Schreiben in Katalogelementdatensätze erforderlich
Katalogelement	löschen	Rolle „catalog_admin“ zum Löschen von Katalogelementdatensätzen erforderlich
Katalogelement	Erstellen	Rolle „catalog_admin“ zum Erstellen von Katalogelementdatensätzen erforderlich
sysevent_email_action	gelesen	Alle Benutzer können E-Mail-Benachrichtigungsdatensätze lesen (für Abonnementzwecke).
sysevent_register	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Ereignisregistrierungsdatensätzen erforderlich
sysevent_script_action	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Skriptaktionsdatensätzen erforderlich
syslog	RWCD	Administrator zum Lesen/Schreiben/Erstellen/Löschen von Protokolleintragsdatensätzen erforderlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
Sysrule	RWCD	Administrator zum Lesen/Schreiben/Erstellen/Löschen von Regeldatensätzen (E-Mail-Benachrichtigungen, Aktionen für eingehende E-Mails, Genehmigungsregeln usw.) erforderlich
Sysrule	gelesen	alle Benutzer können E-Mail-Benachrichtigungsdatensätze für lesen (abonnementbasierte Benachrichtigungen)
sys_app_application	WCD	Administrator zum Schreiben/Erstellen/Löschen von Anwendungsdatensätzen erforderlich
sys_app_category	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Anwendungskategorie-Datensätzen erforderlich
sys_app_module	WCD	Administrator zum Schreiben/Erstellen/Löschen von Moduldatensätzen erforderlich
sys_audit	RWCD	Administrator zum Lesen/Schreiben/Erstellen/Löschen von Audit-Datensätzen erforderlich
sys_dictionary	RWC	Rolle „personalize_dictionary“ erforderlich zum Lesen/Schreiben/ Erstellen von Wörterbuchdatensätzen
sys_dictionary.*	gelesen	Die Rolle „personalize_dictionary“ kann Dictionary-Felder lesen
sys_documentation	löschen	Rolle „personalize_dictionary“ erforderlich, um Feldbezeichnungsdatensätze zu löschen
sys_documentation	Erstellen	Rolle „personalize_dictionary“ erforderlich, um Feldbezeichnungsdatensätze zu erstellen
sys_documentation	write	Rolle „personalize_dictionary“ erforderlich, um in Feldbezeichnungsdatensätzen zu schreiben
sys_anzeige	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Anzeigedatensätzen erforderlich
sys_anzeige_count	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Zählerdatensätzen erforderlich
sys_group_has_role	gelesen	itil-Rolle zum Anzeigen von Gruppenrollendatensätzen erforderlich
sys_home	WCD	Rolle „itil_admin“ zum Schreiben/Erstellen/Löschen von Datensätzen im Abschnitt „Willkommensseite“ erforderlich
sys_installation_exit	WCD	-Administratorrolle zum Schreiben/Erstellen/Löschen von Installations-Exit-Datensätzen erforderlich
sys_job	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Sys-Auftragsdatensätzen erforderlich
sys_nav_link	WCD	Administratorrolle, die zum Schreiben/Erstellen/Löschen von Navigationslink-Datensätzen erforderlich ist
sys_perpektive	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Menülistendatensätzen erforderlich
sys_portal	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Portaldatensätzen erforderlich
sys_portal_page	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Homepage-Datensätzen erforderlich
sys_portal_preferences	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Portaleinstellungsdatensätzen erforderlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_processor	WC	Administratorrolle zum Schreiben/Erstellen von Prozessordatensätzen erforderlich
sys_properties	WC	Administratorrolle zum Schreiben/Erstellen von Systemeigenschaften-Datensätzen erforderlich
sys_properties_category	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Eigenschaftskategorie-Datensätzen erforderlich
sys_report	löschen	Rollen, die Berichtsdatensätze löschen können (Schränkt das Löschen über die Berichts-UI nicht ein)
sys_report	write	Rollen, die in Berichtsdatensätze schreiben können (Schränkt die Bearbeitung über die Berichts-UI nicht ein)
sys_report	gelesen	Benutzer können ihre eigenen Berichtsdatensätze, die ihrer Gruppe und GLOBALE Datensätze lesen (hat keine Auswirkungen auf die Anzeige über die Berichts-UI).
sys_report	gelesen	Rollen, die Berichtsdatensätze lesen können (Schränkt die Anzeige über die Berichts-UI nicht ein)
sys_reportroles	gelesen	Administratorrolle zum Lesen von Berichtsrollen-Datensätzen erforderlich
sys_script	WCD	Administratorrolle, die zum Schreiben/Erstellen/Löschen von Business Rule-Datensätzen erforderlich ist
sys_script_ajax	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von AJAX-Skriptdatensätzen erforderlich
sys_script_client	WCD	Administratorrolle, die zum Schreiben/Erstellen/Löschen von Client-Skript-Datensätzen erforderlich ist
sys_script_include	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Skripteinbindungsdatensätzen erforderlich
sys_security_acl	write	-Administratorrolle, die zum Schreiben in Zugriffssteuerungsdatensätze erforderlich ist
sys_security_acl_role	Erstellen	Administratorrolle, die zum Erstellen von Zugriffsrollendatensätzen erforderlich ist
sys_security_acl_role	löschen	Administratorrolle zum Löschen von Zugriffsrollendatensätzen erforderlich
sys_security_acl_role	write	Administratorrolle, die zum Schreiben in Zugriffsrollendatensätze erforderlich ist
sys_security_operation	löschen	-Administratorrolle zum Löschen von Sicherheitsvorgangsdatensätzen erforderlich
sys_security_operation	Erstellen	-Administratorrolle, die zum Erstellen von Sicherheitsvorgangsdatensätzen erforderlich ist
sys_security_operation	write	-Administratorrolle, die zum Schreiben in Sicherheitsvorgangsdatensätze erforderlich ist
sys_security_type	write	-Administratorrolle, die zum Schreiben in Sicherheitstyp-Datensätze erforderlich ist
sys_security_type	Erstellen	-Administratorrolle, die zum Erstellen von Sicherheitstyp-Datensätzen erforderlich ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_security_type	löschen	-Administratorrolle zum Löschen von Sicherheitstyp-Datensätzen erforderlich
sys_status	Erstellen	-Administratorrolle, die zum Erstellen von Systemstatusdatensätzen erforderlich ist
sys_status	löschen	-Administratorrolle zum Löschen von Systemstatusdatensätzen erforderlich
sys_status	write	-Administratorrolle, die zum Schreiben in Systemstatusdatensätze erforderlich ist
sys_template	write	Rolle „template_editor“ zum Schreiben in Vorlagendatensätze erforderlich
sys_template	Erstellen	Rolle „emplate_editor“ zum Erstellen von Vorlagendatensätzen erforderlich
sys_template	löschen	Rolle „template_editor“ zum Löschen von Vorlagendatensätzen erforderlich
sys_template	gelesen	Rolle „template_editor“ zum Lesen von Vorlagenrollen-Datensätzen erforderlich
sys_ui_action	Erstellen	-Administratorrolle, die zum Erstellen von UI-Aktionsdatensätzen erforderlich ist
sys_ui_action	löschen	-Administratorrolle zum Löschen von UI-Aktionsdatensätzen erforderlich
sys_ui_action	write	Administratorrolle zum Schreiben in UI-Aktionsdatensätze erforderlich
sys_ui_action_view	write	Administratorrolle zum Schreiben in UI-Ansichtsaktionsdatensätze erforderlich
sys_ui_action_view	Erstellen	-Administratorrolle, die zum Erstellen von UI-Ansichtsaktionsdatensätzen erforderlich ist
sys_ui_action_view	löschen	Administratorrolle zum Löschen von UI-Ansichtsaktionsdatensätzen erforderlich
sys_ui_policy	Erstellen	Administratorrolle, die zum Erstellen von UI-Richtliniendatensätzen erforderlich ist
sys_ui_policy	löschen	Administratorrolle zum Löschen von UI-Richtliniendatensätzen erforderlich
sys_ui_policy	write	Administratorrolle zum Schreiben in UI-Richtliniendatensätze erforderlich
sys_ui_policy_action	Erstellen	Administratorrolle, die zum Erstellen von Datensätzen für UI-Richtlinienaktionen erforderlich ist
sys_ui_policy_action	löschen	-Administratorrolle zum Löschen von UI-Richtlinienaktionsdatensätzen erforderlich
sys_ui_policy_action	write	Administratorrolle zum Schreiben in UI-Richtlinienaktionsdatensätze erforderlich
sys_ui_script	write	Administratorrolle zum Schreiben in UI-Skriptdatensätze erforderlich
sys_ui_script	löschen	Administratorrolle zum Löschen von UI-Skriptdatensätzen erforderlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_ui_script	Erstellen	Administratorrolle, die zum Erstellen von UI-Skriptdatensätzen erforderlich ist
sys_user	write	Benutzer ohne Rolle können nur ihren eigenen Benutzerdatensatz aktualisieren
sys_user_grmember	löschen	Rolle „user_admin“ zum Löschen von Gruppenmitgliedsdatensätzen erforderlich
sys_user_grmember	write	Rolle „user_admin“ zum Schreiben in Gruppenmitgliedsdatensätze erforderlich
sys_user_group	Erstellen	Nur itil und höher können Gruppendatensätze erstellen
sys_user_group	write	Nur itil und höher können in Gruppendatensätze schreiben
sys_user_has_role	gelesen	itil-Rolle zum Anzeigen von Benutzerrollendatensätzen erforderlich
sys_user_role	Erstellen	Administratorrolle, die zum Erstellen von Rollendatensätzen erforderlich ist
sys_user_role	löschen	Administratorrolle zum Löschen von Rollendatensätzen erforderlich
sys_user_role	write	Administratorrolle zum Schreiben in Rollendatensätze erforderlich
sys_user_role_contains	gelesen	itil-Rolle erforderlich, um Datensätze der enthaltenen Rolle anzuzeigen
sys_user_role_contains	write	Administratorrolle, die zum Schreiben in Datensätze der enthaltenen Rolle erforderlich ist
sys_user_token	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Benutzer-Token-Datensätzen erforderlich

Hinweis:
Weitere Informationen zu diesem Plugin finden Sie unter Sicherheits-Jump-Start (ACL-Regeln) (Härtung der Instanzsicherheit) in Einstellungen für die Härtung der Instanzsicherheit.

Konfigurieren einer ACL-Regel

Konfigurieren Sie eine benutzerdefinierte ACL-Regel, um den Zugriff auf neue Objekte zu sichern oder das Standardsicherheitsverhalten zu ändern.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Um ACL-Regeln zu erstellen, müssen Sie die Berechtigungen für die Rolle „security_admin“ erhöhen.

Für Tabellen, die sich in einem anderen Bereich als der ACL-Regeldatensatz befinden, sind die Regeltypen beschränkt. Damit Scope Master-Tabellen den Bereich ableiten und bereichsbezogene ACLS ausführen, legen Sie die Eigenschaft *glide.enforce_security_scope.<scope_name>* auf **true**fest. Dadurch wird sichergestellt, dass ACLs im globalen Bereich nicht übereinstimmen, wenn bereichsspezifische ACLs in der entsprechenden Tabelle erstellt werden. Beispiele hierfür sind die Sicherung von Daten in gemeinsam genutzten Anwendungstabellen im globalen Bereich, z. B. sys_attachment- oder sys_question_answer-Tabellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Rollen mit erhöhten Berechtigungen auf die Rolle „security_admin“.
2. Navigieren zu **Systemsicherheit** > **Zugriffssteuerung (ACL)**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie das Formular aus.

Zugriffssteuerungsfelder

Feld	Beschreibung
Typ	Wählen Sie aus, welche Art von Objekt diese ACL-Regel sichert. Der Typ des Objekts bestimmt, wie das Objekt benannt wird und welche Vorgänge verfügbar sind. Dieses Feld wird schreibgeschützt, nachdem die ACL-Regel erstellt wurde. Wenn Sie den Typ ändern möchten, müssen Sie die ACL löschen und eine neue mit dem richtigen Typ erstellen.
Vorgang	Wählen Sie den Vorgang aus, den diese ACL-Regel sichert. Jeder Objekttyp verfügt über eine eigene Liste von Vorgängen. Eine ACL-Regel kann nur einen Vorgang sichern. Um mehrere Vorgänge abzusichern, erstellen Sie für jeden eine separate ACL-Regel.
Admin-Aufhebungen	Aktivieren Sie diese Checkbox, damit Benutzer mit der Administratorrolle automatisch die Berechtigungsprüfung für diese ACL-Regel durchlaufen. Admin-Benutzer übergeben unabhängig von den geltenden Skript- oder Rollenbeschränkungen. Die Rolle „ **Niemand** “, die nur von Mitarbeitern von ServiceNow zugewiesen werden kann, hat jedoch Vorrang vor der Überschreibungsoption des Administrators. Wenn einer ACL die Rolle **niemand** zugewiesen ist, können Administratoren nicht auf die Ressource zugreifen, auch wenn **Administratorüberschreibungen** ausgewählt sind. Weitere Informationen finden Sie unter Basissystemrollen. Deaktivieren Sie diese Checkbox, wenn Administratoren die in dieser ACL-Regel definierten Berechtigungen erfüllen müssen, um Zugriff auf das gesicherte Objekt zu erhalten. Da Administratoren Rollenprüfungen immer bestehen (siehe Beschreibung des Felds „ **Erfordert Rolle** “), verwenden Sie den Bedingungsgenerator oder das **Skriptfeld**, um eine Berechtigungsprüfung zu erstellen, die Administratoren bestehen müssen.
Aktiv	Aktivieren Sie diese Checkbox, um diese ACL-Regel durchzusetzen.
Erweitert	Aktivieren Sie diese Checkbox, um das Feld **Skript** anzuzeigen. **Wichtig:** Wenn sich im Feld Skript ein **Skript** befindet. Dieses Skript wird auch dann ausgeführt, wenn das Feld nicht im Formular angezeigt wird.
Name	Geben Sie den Namen des zu sichernden Objekts ein, entweder den Datensatznamen oder die Tabellen- und Feldnamen. Je spezifischer der Name, desto spezifischer die ACL-Regel. Sie können das Platzhalterzeichen Sternchen (*) anstelle eines Datensatz-, Tabellen- oder Feldnamens verwenden, um alle Objekte auszuwählen, die einem Datensatztyp, allen Tabellen oder allen Feldern entsprechen. Sie können ein Platzhalterzeichen und eine Textsuche nicht kombinieren. Beispiel: inc* ist kein gültiger ACL-Regelname, aber incident.* und *.number sind gültige ACL-Regelnamen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Klicken Sie auf das blaue Dreieck, um den Datensatznamen oder die Tabellen- und Feldnamen des zu sichernden Objekts manuell einzugeben. Verwenden Sie diese Option, um ein Objekt zu sichern, das nicht in der Dropdown-Liste angezeigt wird.
Beschreibung	Geben Sie eine Beschreibung des Objekts oder der Berechtigungen ein, die diese ACL-Regel sichert.
Erfordert Rolle	Verwenden Sie diese Liste, um die Rollen anzugeben, die ein Benutzer für den Zugriff auf das Objekt haben muss. Wenn Sie mehrere Rollen auflisten, kann ein Benutzer mit einer der aufgelisteten Rollen auf das Objekt zugreifen. Die Liste „ *Erfordert Rolle* “ wird als zugehörige Liste angezeigt. **Hinweis:** Benutzer mit der Administratorrolle bestehen diese Berechtigungsprüfung immer, da die Administratorrolle Benutzern automatisch alle anderen Rollen gewährt.
Bedingung	Verwenden Sie diesen Bedingungsgenerator , um die Felder und Werte auszuwählen, die erfüllt sein müssen, damit Benutzer auf das Objekt zugreifen können.
Skript	Geben Sie ein benutzerdefiniertes Skript ein, das die für den Zugriff auf das Objekt erforderlichen Berechtigungen beschreibt. Das Skript kann die Werte der *aktuellen* und *vorherigen* globalen Variablen in Business Rules sowie Systemeigenschaften verwenden. Das Skript muss auf eine von zwei Arten eine True- oder False-Antwort generieren: ○ eine *Antwortvariable* zurückgeben, die auf den Wert true oder false festgelegt ist ○ als „true“ oder „false“ auswerten In beiden Fällen erhalten Benutzer nur dann Zugriff auf das Objekt, wenn das Skript „true“ ergibt und der Benutzer die Bedingungen der ACL-Regel erfüllt. Sowohl die Bedingungen als auch das Skript müssen als „wahr“ ausgewertet werden, damit ein Benutzer auf das Objekt zugreifen kann. **Hinweis:** Wenn sich das ausgewertete Element in einer zugehörigen Liste befindet, verweist **aktuell** auf das Element, auf dem sich die zugehörige Liste befindet, nicht auf das aktuelle Element, für das die ACL gilt. Wenn sich das Element, für das Sie die ACL auswerten, jedoch nicht in einer zugehörigen Liste befindet, verweist **current** auf das tatsächliche Element.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

Sichere Datensätze in einer eingebetteten Liste

Um Sicherheit auf die Datensätze in eingebetteten Listen anzuwenden, beschränken Sie das Bearbeiten und Löschen von Datensätzen in eingebetteten Listen auf bestimmte Rollen.

Vorbereitungen

Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerung (ACL)**.
2. Öffnen Sie den Datensatz **Schreiben** oder **Löschen** für die entsprechende Tabelle.
3. Fügen Sie im Abschnitt „Erfordert Rolle“ des Formulars die Rollen hinzu, die über Schreib- oder Löschberechtigungen für diese Tabelle verfügen.
4. Speichern Sie die Änderungen.
   Wenn Datensätze aus der zugeordneten Tabelle in einer eingebetteten Liste angezeigt werden, sind die Optionen zum Bearbeiten und Löschen nur für Benutzer mit den angegebenen Rollen verfügbar.

Contextual Security Manager

Contextual Security Manager schützt Ihre Daten durch die Steuerung der Lese-, Schreib-, Erstellungs- und Löschberechtigung.

Hauptvorteile

Contextual Security Manager erkennt die Systemtabellenhierarchie, sodass Sie spezifische Sicherheitsregeln für ein Feld basierend auf der Position in der Hierarchie erstellen können, an der es angezeigt wird. Zu den Vorteilen von Contextual Security Manager gehören:

- **Kontextabhängige Sicherheit**: Sichern Sie einen Datensatz basierend auf dem Inhalt des Datensatzes.
- **Hierarchische Sicherheit**: Wenden Sie Sicherheitsregeln auf eine beliebige Ebene in der Objekthierarchie an.

Sichern von Feldern und Tabellen

Mit dem veralteten Simple Security Manager konnten Sie Felder und Tabellen sichern, indem Sie dem entsprechenden Dictionary-Eintrag Rollen hinzufügen. Mit dem Contextual Security Manager werden diese Wörterbuchrollen nicht mehr getestet. Stattdessen sucht das System nach ACL-Regeln für Felder und Tabellen.

> ⚠ **Warnung:**
> Nachdem Sie den Contextual Security Manager installiert haben, müssen Sie Felder und Tabellen über ACL-Regeln sichern. Auch wenn Sie das Formularlayout des Wörterbuchformulars konfigurieren und einem Wörterbucheintrag Rollen hinzufügen, werden die Rechte nicht geändert.

Kontextbezogene Sicherheit und Rollen

Sie können Benutzern oder Gruppen Rollen gewähren. Nach der Installation von Contextual Security Manager wird das Feld „ **Rollen** “ im Benutzerdatensatz jedoch nicht mehr überprüft und in Ihren Benutzer- und Gruppenformularen angezeigt. Stattdessen müssen Sie Rollen der zugehörigen Liste „Rollen“ und nicht dem Benutzer- oder Gruppendatensatz hinzufügen.

Anwendungen und Module enthalten Listen der Rollen, die erforderlich sind, um sie anzuzeigen. Um beispielsweise die Systemdefinitionsanwendung anzuzeigen, ist die Administratorrolle erforderlich. Sicherheitsrechte für Anwendungen und Module werden weiterhin mithilfe von Rollen-Arrays definiert.

Sowohl Katalogelemente als auch Katalogvariablen enthalten Listen der Rollen, die zum Anzeigen erforderlich sind. Sicherheitsrechte für Katalogelemente und Katalogvariablen werden weiterhin über diese Rollen-Arrays definiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unter dem Contextual Security Manager erbt eine Gruppe weiterhin automatisch jede Rolle, die der Gruppe zugewiesen wurde, wenn die Kennzeichnung für Erbungen für die Rolle auf *true*gesetzt ist.

Contextual Security Manager wird aktiviert

Contextual Security Manager ist im Basissystem aktiv. Wenn in der Tabelle „Benutzerrollen“ viele doppelte Einträge vorhanden sind, müssen Sie möglicherweise ein Upgrade auf Contextual Security: Role Management V2 durchführen, um doppelte Rollen zu entfernen. Zu den Plugins gehören:

Kontextabhängige Sicherheit: Rollenverwaltung [com.glide.role_management]

Bietet kontextbezogene Sicherheitsfunktionen. Dieses Plugin wird automatisch installiert.

Kontextabhängige Sicherheit: Rollenverwaltung V2 [com.glide.role_management.inh_count]

Verhindert doppelte Einträge, die durch geerbte Rollen in der Tabelle „Benutzerrollen“ [sys_user_has_role] verursacht werden. Dieses Plugin wird automatisch in neuen Instanzen installiert und kann für Upgrades aktiviert werden. Das Plugin „Contextual Security: Role Management Enhancements“ ist eine frühere Version dieses Plugins. Das Plugin „Role Management Enhancements“ enthält nicht das Skript RoleManagementVerify(). Dieses Skript gibt eine Liste der Änderungen zurück, die bei einem Upgrade durchgeführt werden, sodass Sie die vom Plugin vorgenommenen Änderungen überwachen können.

Hinweis:
Nach der Aktivierung von Role Management V2 müssen Sie die Systemeigenschaft glide.role_management.v2.audit_roles festlegen, damit die Tabelle Audit-Rollen Audit-Datensätze im Zusammenhang mit Benutzerrollen erstellen kann. Weitere Informationen zum Festlegen dieser Eigenschaft und zur Tabelle „Audit-Rollen“ finden Sie unter:

- Aktivieren Sie Rollenaudits mit Contextual Security: Role Management V2.
- Plugin „Contextual Security: Role Management“. in Härtungseinstellungen für Instanzsicherheit.
- Audit-Benutzerrollen

Verhindern Sie doppelte Einträge mit Contextual Security: Role Management V2

Von anderen Rollen geerbte Rollen werden als einzelne Einträge in der Benutzerrollentabelle [sys_user_has_role] hinzugefügt, was möglicherweise dazu führt, dass eine Rolle doppelte Einträge aufweist. Contextual Security: Role Management V2 eliminiert diese doppelten Einträge und verhindert zukünftige Duplikate.

Beseitigen Sie doppelte Einträge durch Vererbungszählung

Kontextabhängige Sicherheit: Rollenverwaltung V2 verwendet die Spalte „Vererbungsanzahl“ (inh_count), um nachzuverfolgen, wie oft eine Rolle von einer anderen Rolle oder Gruppe geerbt wurde. In der Tabelle „Benutzerrollen“ [sys_user_has_role] kann ein Benutzer eine bestimmte Rolle nur einmal erben, wodurch doppelte Einträge vermieden werden. Die Spalte „Vererbungsanzahl“ (inh_count) ist schreibgeschützt und berechnet, wie oft der Benutzer eine Rolle erbt.

Aktivierungsänderungen

Contextual Security: Role Management V2 wird automatisch in neuen Instanzen installiert und kann für Upgrades aktiviert werden. Wenn diese Option aktiviert ist, ersetzt Contextual

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security: Role Management V2 sowohl Contextual Security als auch Contextual Security: Role Management Enhancements.

Wenn Contextual Security: Role Management V2 aktiviert ist, sind die folgenden Spalten veraltet, verbleiben jedoch aus Gründen der Abwärtskompatibilität in der Tabelle „Benutzerrollen“:

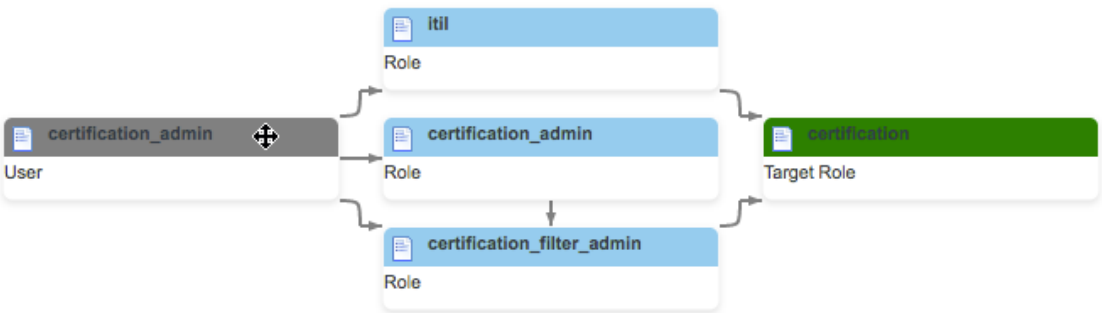
- gewährt_by (wird nur von Rollendelegierung verwendet)
- include_in_role
- include_in_role_instance

Warnung:
Wenn diese Spalten in benutzerdefinierten Skripts in Ihrer Instanz verwendet werden, führen Sie kein Upgrade auf Role Management V2 durch.

Visualisieren Sie die Rollenvererbung über die Rollenvererbungszuordnung

Die Rollenvererbungszuordnung zeigt eine visuelle Darstellung der geerbten Rollen an. Sie können diese Zuordnung verwenden, um die Rollen zu verstehen, die in der Spalte „Vererbungsanzahl“ (inh_count) dargestellt werden. Um die Rollenvererbungszuordnung anzuzeigen, konfigurieren Sie die Tabelle „Benutzerrollen“ [sys_user_has_role] so, dass die Spalte „Rollenvererbungszuordnung“ angezeigt wird.

Rollenvererbungskarte



Führen Sie ein Upgrade auf Contextual Security: Role Management V2 durch

Contextual Security: Role Management V2 wird automatisch in neuen Instanzen installiert. Sie können ein Upgrade von Contextual Security: Role Management auf Contextual Security: Role Management V2 durchführen, um doppelte Rollen in der Tabelle „Benutzerrollen“ zu entfernen und zukünftige Duplikate zu verhindern.

Vorbereitungen

Erforderliche Rolle: admin, security_admin

Sie müssen über die Administratorrolle und Führen Sie eine Erhöhung auf eine privilegierte Rolle durch verfügen, um die effektive Rolle security_admin zu erhalten.

Hinweis:
Vor dem Upgrade auf Contextual Security: Rolle: Management V2 müssen Sie die Tabelle Audit-Rollen aktivieren, um Audit-Datensätze im Zusammenhang mit Benutzerrollen zu erstellen. Weitere Informationen zum Festlegen der erforderlichen Systemeigenschaft finden Sie unter Aktivieren Sie Rollenaudits mit Contextual Security: Role Management V2.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt, wie Sie Ihre Rolle für die kontextbezogene Sicherheit aktualisieren und die zugehörigen Plugins aktivieren, die in der folgenden Tabelle beschrieben werden.

Plugins für Contextual Security: Role Management V2

Plugin	Beschreibung
Kontextabhängige Sicherheit: Rollenverwaltung V2 [com.glide.role_management.inh_count]	Verhindert doppelte Einträge in der Benutzerrollentabelle [sys_user_has_role]. Die Rolle security_admin oder ein Benutzer mit erhöhten Berechtigungen ist erforderlich, um das Plugin zu aktivieren, oder wenden Sie sich an Kundenservice und Support.
Kontextabhängige Sicherheit: Rollenverwaltung V2 REST API [com.glide.role_management.inh_count.rest_api]	Aktiviert die API-Funktionalität für die Rollenverwaltung.

Testen Sie vor dem Upgrade von Contextual Security: Role Management auf Contextual Security: Role Management V2 die Ergebnisse eines Upgrades, indem Sie das Skript ausführen. Das Skript gibt eine Liste der Änderungen zurück, die bei einem Upgrade durchgeführt werden. Wenn die Änderungen akzeptabel sind, installieren Sie das Plugin Contextual Security: Role Management V2. Wenn die Änderungen nicht akzeptabel sind, installieren Sie das Plugin „Contextual Security: Role Management V2“ nicht. Alternativ können Sie das Upgrade durchführen und dann die erforderlichen Änderungen manuell vornehmen.

Prozedur

1. Testen Sie die Auswirkungen eines Upgrades vor dem Upgrade, indem Sie das folgende Skript ausführen.

   a. Navigieren zu **Systemdefinition** > **Skripts – Hintergrund**.

   b. Führen Sie das folgende Skript im globalen Bereich aus.

   ```
   new RoleManagementVerify().verifyInheritedRoles();
   ```

   Bei großen sys_user_has_role-Tabellen kann die Ausführung bis zu mehrere Stunden dauern. Bearbeiten oder fügen Sie während dieser Zeit keine Benutzerrollen hinzu.
   Beispielergebnis basierend auf Testdaten:

   ```
   *** Script: 2016-12-01 19:58:54 Starting checking of inherited roles for all users...
   *** Script: User: itam, inherited roles to be ADDED: financial_mgmt_user
   *** Script: User: bernard.laboy, inherited roles to be DELETED:
    api_analytics_read,pa_viewer,rest_api_explorer,a123
   *** Script: User: bernard.laboy, inherited roles to be ADDED: dependency_views
   *** Script: Number of inherited-role records in sys_user_has role, current: 260, after
    re-calculation: 258
   *** Script: Number of users with discrepancies for inherited roles: 2
   *** Script: 2016-12-01 19:58:55 Finished checking of inherited roles for all users!
   ```

   c. Bewerten Sie die Skriptergebnisse, um festzustellen, ob die vorgeschlagenen Änderungen akzeptabel sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Aktivieren Sie das Plugin „Contextual Security: Role Management V2“.

> **Wichtig:**
> Die Rolle security_admin oder ein Benutzer mit erhöhten Berechtigungen ist erforderlich, um das Plugin zu aktivieren, oder wenden Sie sich an Kundenservice und Support.

   a. Navigieren zu **Systemdefinition** > **Plugins**.

   b. Suchen Sie nach dem Namen des Plugins, und klicken Sie darauf.

   c. Überprüfen Sie im System-Plugin-Formular die Plugin-Details, und klicken Sie dann auf den zugehörigen Link **Aktivieren/Aktualisieren**.

   d. Klicken Sie auf **Aktivieren**.

Ergebnisse

Nach der Aktivierung von Role Management V2 werden die im Skriptergebnis beschriebenen Änderungen übernommen. Die Spalte „Vererbungsanzahl“ (inh_count) in der Tabelle „Benutzerrollen“ ist schreibgeschützt und gibt automatisch an, wie oft der Benutzer eine Rolle übernimmt.

Aktivieren Sie Rollenaudits mit Contextual Security: Role Management V2

Legen Sie eine Systemeigenschaft fest, um die Tabelle Audit-Rollen zum Erstellen von Audit-Datensätzen im Zusammenhang mit Benutzerrollen zu aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn diese Option aktiviert ist, werden in der Tabelle „Audit-Rollen“ [sys_audit_role] Änderungen an Benutzerdatensätzen beibehalten. Weitere Informationen zu Rollenaudits finden Sie unter Audit-Benutzerrollen. Wenn das Plugin „Contextual Security: Role Management V2“ [com.glide.role_management.inh_count] installiert ist, müssen Sie eine Systemeigenschaft auf „ **true** “ festlegen, um die Rollenprüfung zu aktivieren.

Prozedur

1. Navigieren Sie zur Tabelle „Systemeigenschaften“ [sys_properties].
2. Fügen Sie die Systemeigenschaft `glide.role_management.v2.audit_roles` hinzu, und legen Sie sie auf **true**fest.

   Wenn das Plugin „Contextual Security: Role Management V2“ [**com.glide.role_management.inh_count**] installiert ist, kann die Tabelle „Audit-Rollen“ [sys_audit_role] Datensätze erstellen, wenn sich die Benutzerrollen ändern.

Überprüfen Sie die Formularübermittlung noch einmal

Wenn das System feststellt, dass der aktuelle Benutzer nicht in ein bestimmtes Feld (z. B. task.number) schreiben darf, rendert das System dieses Feld in einen schreibgeschützten Modus, weshalb in das Nummernfeld bei den meisten Incidents nicht geschrieben werden kann.

Wenn Sie das System so einstellen, dass die Werte eingehender Felder auf Bearbeitbarkeit überprüft werden, wendet das System dieselben Sicherheitsregeln auf den eingehenden Abschnitt einer Transaktion an. Wenn Sie beispielsweise einen Incident übermitteln, prüft das System vor der Veröffentlichung von Änderungen, ob in das Nummernfeld geschrieben werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie das System anweisen, eingehende Transaktionen nicht noch einmal zu überprüfen, können Sie in ein nominell schreibgeschütztes Feld schreiben, wenn dies die vom Client zurückgesendete Transaktion ist. In vielen Bereitstellungen ist dies tatsächlich ein wünschenswertes Verhalten, wenn Sie beispielsweise Client-Skripts verwenden, um nominell schreibgeschützte Felder als Reaktion auf Benutzerauswahlen in anderen, bearbeitbaren Feldern festzulegen.

Standardmäßige Deny-Eigenschaft

Die Standardverweigerungseigenschaft (glide.sm.default_mode) steuert das Standardverhalten des Sicherheitsmanagers, wenn die einzigen übereinstimmenden ACL-Regeln die ACL-Regeln der Platzhaltertabelle sind.

Eine Reihe von ACL-Regeln für Platzhaltertabellen für die häufigsten datensatzbasierten Vorgänge sind verfügbar: Lesen, Schreiben, Erstellen und Löschen. Eine erhebliche Anzahl von ACLs für den rollenbasierten Zugriff auf Systemtabellen ist ebenfalls verfügbar. Beispielsweise gibt es ACLs, die sys_script Zugriff auf die Rolle „business_rule_admin“ gewähren, da diese Rolle nachweislich in der Lage ist, Business Rules zu verwalten.

Verwenden Sie die Eigenschaft glide.sm.default_mode, um diese Vorgänge für alle Tabellen zu verweigern oder zuzulassen:

- **Zugriff verweigern**: Die ACL-Regeln der Platzhaltertabelle schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Benutzer hat die Administratorrolle oder erfüllt die Anforderungen einer anderen Tabellen-ACL-Regel. Andere Vorgänge wie report_on und personalize_choices sind von dieser Einstellung nicht betroffen.
- **Zugriff zulassen**: Die ACL-Regeln der Platzhaltertabelle ermöglichen das Lesen, Schreiben, Erstellen und Löschen von Vorgängen in allen Tabellen, es sei denn, es sind bestimmte Tabellen-ACL-Regeln vorhanden, um solche Vorgänge einzuschränken.

Sie können glide.sm.default_mode nicht auf **Zugriff zulassen** zurücksetzen, nachdem es auf Zugriff **verweigern**festgelegt wurde.

Hinweis:
Standardmäßig sind die ACL-Regeln der Platzhaltertabelle die einzigen ACL-Regeln, die den Wert der Eigenschaft glide.sm.default_mode überprüfen. Wenn Sie andere Vorgänge mit dieser Einstellung steuern möchten, erstellen Sie eigene ACL-Regeln, um nach diesem Eigenschaftswert zu suchen.

Weitere Informationen zu dieser Eigenschaft finden Sie unter Standardmäßig verweigern in Härtungseinstellungen für Instanzsicherheit.

Erweiterte ACL-Konfiguration

Sie können nicht nur neue ACLs erstellen oder vorhandene ACLs ändern, sondern auch andere Aspekte der ACL-Funktionalität konfigurieren.

Aufgabe	Beschreibung
Wenden Sie ACL-Skriptbedingungen auf Referenzfelder an	Aktivieren Sie eine Eigenschaft, damit Skriptbedingungen auf Referenzfelder angewendet werden können, wenn Sie den Zugriff auf die Daten steuern möchten, die ein Referenzfeld in einem Formular oder in einer Liste anzeigt. Wenn Sie diese Option aktivieren, kann dies Auswirkungen auf die Leistung Ihrer Instanz haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz)	Wenden Sie ACLs auf Aufrufe der `GlideAjax-` API an, damit das System nur die Daten abfragt, für die der aktuell verbundene Benutzer Zugriffsrechte hat.
Bewerten Sie die Administratorüberschreibung auf Zugriffsebene	ACL-Auswertung für Administratorüberschreibungen auf Zugriffsebene erzwingen. Standardmäßig bestehen Benutzer mit der Administratorrolle automatisch die Berechtigungsprüfung für diese ACL-Regel, wenn die Option Admin-Überschreibungen im ACL- Regelformularausgewählt ist.
Verwenden Sie ACL-Debugging- und Problembehandlungstools	Verwenden Sie Tools wie ACL-Watcher, Debugging auf Feldebene und Zugriff auf Ausgabenachrichten von ACL-Regeln, um Probleme bei ACLs zu beheben und zu debuggen.

Externen Benutzern Zugriff auf eine Tabelle bereitstellen

Um Benutzern mit nur der Rolle snc_external den Zugriff auf die Listenansicht einer Tabelle zu ermöglichen, müssen Sie eine Reihe von ACLs erstellen.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Führen Sie eine Erhöhung auf eine privilegierte Rolle durch.
2. Erstellen Sie eine ACL-Regel mit den folgenden Einstellungen:
   - **Typ**: ui_page
   - **Operation**: Lesen
   - **Name**: {table_name}_list
   - **Erforderliche Rolle**: snc_external
3. Fügen Sie in der standardmäßigen **Lese**-ACL für die Tabelle **snc_external** in die Liste „Erforderliche Rolle“ hinzu.
   Erstellen Sie die ACL, wenn sie nicht bereits vorhanden ist.
4. Verwenden Sie diese Einstellungen, um eine andere ACL zu erstellen:
   - **Typ**: ui_page
   - **Operation**: Lesen
   - **Name**: {table_name}
   - **Erforderliche Rolle**: snc_external
5. Verwenden Sie diese Einstellungen, um eine weitere ACL zu erstellen, um dem Benutzer Schreibzugriff für ein Feld in der Tabelle zu gewähren:
   - **Typ**: Datensatz
   - **Operation**: Erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Name**: {table_name} {column_name}
- **Erforderliche Rolle**: snc_external

Wiederholen Sie diesen Schritt für jedes Feld, auf das Sie dem Benutzer Schreibzugriff gewähren möchten. Verwenden Sie ein Sternchen * anstelle des Spaltennamens, um Zugriff auf alle Felder gleichzeitig bereitzustellen.

Wenden Sie ACL-Skriptbedingungen auf Referenzfelder an

Verwenden Sie die Systemeigenschaft `glide.sys_reference_row_check`, um geskriptete Bedingungen für Referenzfelder zu aktivieren.

Das Standardverhalten soll die Instanzleistung verbessern. Wenn Sie Skriptbedingungen für Referenzfelder aktivieren möchten, fügen Sie die folgende Systemeigenschaft hinzu.

Hinweis:
Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Add a system property.

Systemeigenschaft

Eigenschaft	Beschreibung
glide.sys_reference_row_check	Steuert, ob die Skriptbedingungen von Zugriffskontrollregeln für Referenzfelder einer Tabelle gelten. • Typ: Wahr | Falsch • Standardwert: **false** • Speicherort: Fügen Sie der Tabelle „Systemeigenschaften“ [sys_properties] eine Systemeigenschaft hinzu

Hinweis:
Wenn die Systemeigenschaft `glide.sys_reference_row_check` nicht vorhanden ist oder auf „falsch“ festgelegt wurde, werden die Skriptbedingungen für Zugriffskontrollregeln nicht angewendet. Das bedeutet, dass eine ACL, die geskriptete Bedingungen enthält, ihre Prüfung besteht, solange die anderen ACL-Kriterien erfüllt sind (z. B. Rollenanforderungen).

ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz)

Verwenden Sie eine Systemeigenschaft, um eine Validierung der Zugriffssteuerungslistenregel (ACL) durchzuführen, wenn auf serverseitige Datensätze (z. B. Tabellen) mit GlideAjax-APIs in einem Client-Skript zugegriffen wird.

Wenn Sie Zugriffskontrolllisten (ACLs) auf Aufrufe der `GlideAjax-` API anwenden, können Sie nur Daten abfragen, für die der aktuell verbundene Benutzer Zugriffsrechte hat. Wenn der Benutzer beispielsweise als ESS-Benutzer angemeldet ist, der keine Rechte zum Lesen der Tabelle cmn_location hat, schlägt jeder Aufruf der `GlideAjax-` API durch den Benutzer fehl.

Wenn Sie das System ohne ACL ausführen, die `GlideAjax-` Aufrufe überprüft, kann die API Informationen zurückgeben, auf die der aktuell angemeldete Benutzer ansonsten über die Benutzeroberfläche nicht zugreifen könnte.

Hinweis:
Legen Sie diese Eigenschaft in fest **Systemeigenschaften** > **Sicherheit**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Weitere Informationen zu dieser Eigenschaft finden Sie unter Aktivieren der AJAXGlideRecord-ACL-Überprüfung in Härtungseinstellungen für Instanzsicherheit.

Bewerten Sie die Administratorüberschreibung auf Zugriffsebene

Wenn Sie die ACL-Auswertung für Administratorüberschreibungen auf Zugriffsebene erzwingen möchten, können Sie eine Systemeigenschaft hinzufügen.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

ACLs werden kumulativ ausgewertet. Wenn in einem bestimmten Feld eine Anzahl von **ACLs** vorhanden ist und die Option „Administratorüberschreibungen“ für eines von ihnen auf „ **falsch** “ (nicht ausgewählt) festgelegt ist, werden die effektiven Administratorüberschreibungen für alle ACLs als „ **falsch**“ betrachtet. Dies führt dazu, dass Administratoren nicht einmal die ACL passieren können, in der die Überschreibung wirksam sein sollte.

Prozedur

Fügen Sie der Tabelle „Systemeigenschaften“ die folgende Eigenschaft hinzu:

Eigenschaft	Beschreibung
`glide.security.admin.override.accessterm`	Wertet die Überschreibungsbedingung des Administrators auf der Ebene der Zugriffsbedingung aus. • Typ: Wahr | Falsch • Standardwert: „ **true** “ für neue Instanzen, „ **false** “ für Upgrades • Speicherort: Fügen Sie der Tabelle „Systemeigenschaften `[sys_properties]` “ hinzu **Hinweis:** Wenn die Eigenschaft nicht in der Instanz definiert ist, wird der Wert als „false“ ausgewertet.

ACL-Debugging-Tools

Debugging auf Feldebene und Ausgabenachrichten für Zugriffs-ACL-Regeln sind verfügbar, um Sie bei der Problembehandlung und beim Debuggen von ACLs zu unterstützen. Der ACL-Konfigurationsbeobachter teilt Ihnen mit, welche zugehörigen ACLs vorhanden sind, wenn Sie eine ändern.

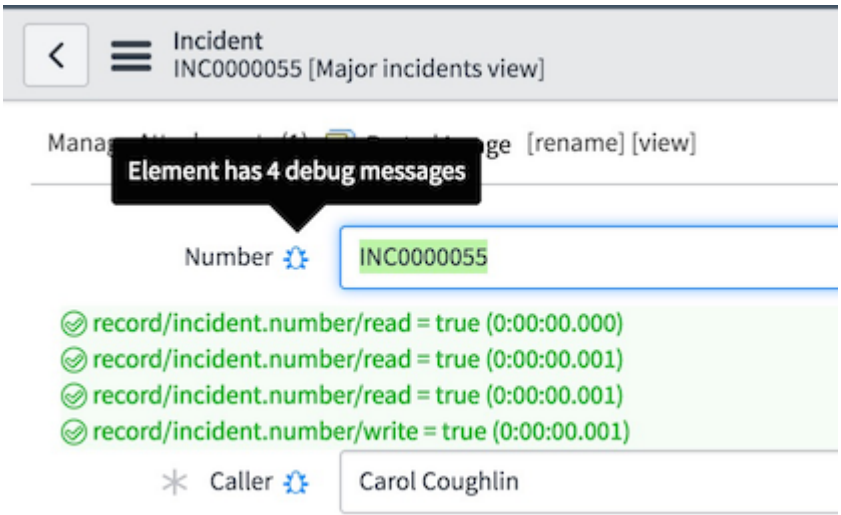
Debugging auf Feldebene

Wenn das Debugging aktiviert ist, wird neben jedem Feld mit einer ACL-Regel ein kleines Fehlersymbol ( ) angezeigt. Wenn Sie auf das Symbol klicken, werden die für das Feld

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

geltenden ACL-Regeln und die Auswertungsergebnisse aufgelistet. Aktivieren Sie das Debugging, indem Sie zu navigieren **Systemsicherheit** > **Debugging** > **Sicherheitsregeln debuggen**.

Sicherheit auf Feldebene bei einem Incident



Nachdem Sie das ACL-Debugging aktiviert haben, können Sie die Identität eines anderen Benutzers annehmen, um zu sehen, welche ACL-Regeln der Benutzer durchläuft und welche nicht. Wenn Sie die Identität eines Benutzers annehmen, können Sie nur das sehen, was dieser Benutzer sehen darf. Sie können beispielsweise keinen Datensatz anzeigen, den eine ACL dem Benutzer nicht anzeigen lässt. Um das Debugging zu erleichtern, ist der schreibgeschützte Zugriff auf bestimmte ACL-bezogene Tabellen standardmäßig aktiviert, auch wenn die Identität eines Benutzers angenommen wird, der keinen Lesezugriff auf die Tabellen hat. Um diese Funktionalität zu ändern, legen Sie die folgende Eigenschaft auf **false**fest.

Um das Debugging von ACL-Regeln zu aktivieren, navigieren Sie zu **Systemsicherheit** > **Sicherheitsregeln debuggen**.

Systemeigenschaft	Beschreibung	Standardeinstellung
`glide.security.access_acl_impersonation`	Ermöglicht Lesezugriff auf die folgenden Tabellen, während die Identität eines Benutzers angenommen wird: sys_security_acl, sys_security_operation, sys_security_type und sys_user_role. Dadurch kann der Benutzer, dessen Identität Sie annehmen, Daten lesen, die der Benutzer, dessen Identität Sie annehmen, nicht lesen kann.	Wahr **Hinweis:** Wenn die Eigenschaft auf „false“ festgelegt ist, wird der Benutzer, dessen Identität Sie annehmen, möglicherweise daran gehindert, ACL-bezogene Daten zu lesen. In diesem Fall ist möglicherweise eine zweite Sitzung erforderlich, die als admin oder security_admin angemeldet ist, um ACLs zu debuggen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Regelausgabenachrichten

ACL-Debugging zeigt ACL-Regelausgabenachrichten am Ende jeder Liste und jedes Formulars an. Die Ausgabenachricht zeigt Folgendes an:

Nachrichtenelement	Beschreibung
TIME	Die Gesamtzeit, die für die Verarbeitung dieser ACL-Regel benötigt wurde.
PFAD	Informationen, die jede ACL-Regel eindeutig identifizieren, im Format:<ACL rule type> /<ACL rule name> /<Operation> .
KONTEXT	Das Objekt, das von der ACL-Regel ausgewertet wird.
RC	Der Rückgabecode der ACL-Regel. Ein Wert vom Typ „true“ übergibt die ACL-Regel. Bei einem Wert vom Typ „falsch“ schlägt die ACL-Regel fehl.
REGEL	Eine kurze Zusammenfassung der Prozessoren und Skripts, gefolgt von den ACL-Ergebnissen für jede ACL-Auswertung auf Tabellen- und Feldebene. Die meisten ACL-Auswertungen zeigen ein Gesamtergebnis für „Bestanden“ oder „Fehlgeschlagen“ an, gefolgt von einer Aufgliederung der Ergebnisse für jeden Typ von ACL-Kriterien: • iAccessHandler: Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. Dies ist eine Systemsicherheitsprüfung, die Sie nicht ändern können. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet. Sie können die IAccessHandler-Prüfungen in keiner Weise ändern. Beispielsweise wird eine IAccessHandler-Implementierung für Zugriffsprüfungen auf Anwendungsressourcen verwendet, und dies kann nicht geändert werden. Dies ist ab Release Istanbul verfügbar. • Rollen: Überprüfung, ob der Benutzer die richtige Rolle hat. • Bedingung: Überprüfung, ob der Benutzer die in der ACL-Regel angegebene Bedingung erfüllt hat (falls vorhanden). • Skript: Überprüfung, ob der Benutzer das in der ACL-Regel angegebene Skript übergeben hat (falls vorhanden).

Die angezeigten Symbole zeigen an, wie die ACL ausgewertet wurde:

Symbol	Beschreibung
Ein grünes Häkchen ( )	Gibt an, dass die Tabelle oder das Feld die Kriterien erfüllt hat.
Ein rotes x-Symbol ( )	Gibt an, dass die Tabelle oder das Feld nicht bestanden hat.
Ein leeres graues Kreissymbol ( )	Gibt an, dass die ACL-Auswertung nicht durchgeführt werden musste.

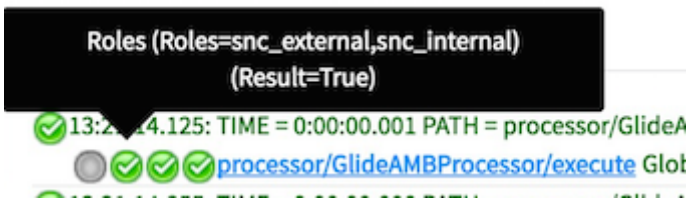
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symbol	Beschreibung
Blaues Häkchen, x oder leerer Kreis	Gibt an, dass die ACL aus einem zwischengespeicherten Ergebnis einer vorherigen ACL-Prüfung übernommen wurde. Die Symbole haben dieselbe Bedeutung wie oben.

Sie können die folgenden Aktionen für die ACL-Debug-Ausgabe ausführen:

- Aktivieren oder deaktivieren Sie diese Checkboxen oben in der Debug-Ausgabe:
  - **Sicherheitsregeln**: Ergebnisse der ACL-Prüfungen anzeigen oder ausblenden.
  - **Andere**: Zeigen Sie andere Warnungen oder Nachrichten an oder blenden Sie sie aus.
- Klicken Sie auf den Namen der ACL neben einer der Ausgabenachrichten, um diesen ACL-Datensatz zu öffnen.

- Bewegen Sie den Mauszeiger über eines der Symbole für die vier ACL-Prüfungen, um weitere Informationen anzuzeigen.



ACL-Fehlerbehebungsreferenz

Eine Liste der häufigsten ACL-Regelfehler und deren Lösungen.

Aktivieren Sie das Debugging, um die Behebung eines Problems zu unterstützen.

Problembehandlung

Fehler oder Symptom	Lösung
Sie können nicht auf Datensätze aus einer benutzerdefinierten Tabelle zugreifen.	Erstellen Sie eine Tabellen-ACL-Regel für die benutzerdefinierte Tabelle, die Benutzern Zugriff auf die Tabelle gewährt. Ohne eine explizite Tabellen-ACL-Regel müssen Benutzer die Berechtigungen in der Tabellen-Platzhalter-ACL-Regel übergeben, die standardmäßig den Zugriff nur auf Administratoren beschränkt. Aktivieren Sie das Debugging, und bestimmen Sie, welche ACL-Regeln für die benutzerdefinierte Tabelle ausgewertet werden.
Sie erstellen eine benutzerdefinierte ACL-Regel, die nicht ordnungsgemäß funktioniert.	Die wahrscheinlichsten Probleme sind, dass eine andere Regel Vorrang vor Ihrer benutzerdefinierten Regel in der Verarbeitungsreihenfolge hat oder dass der Benutzer nicht alle Berechtigungsanforderungen für den Objekttyp erfüllt. Aktivieren Sie das Debugging, und stellen Sie sicher, dass die ACL-Regel ausgewertet wird.
Ihre Feld-ACL-Regel funktioniert nicht ordnungsgemäß.	Wahrscheinlich liegt eine Tabellen-ACL-Regel vor, die der Benutzer nicht erfüllt hat. Aktivieren Sie das Debugging, und bestimmen Sie, welche ACL-Regeln für das Feld ausgewertet werden. Stellen Sie sicher, dass keine in Konflikt stehende Tabellen-ACL-Regel oder doppelte Feld-ACL-Regel vorhanden ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung (Fortsetzung)

Fehler oder Symptom	Lösung
Die ACL-Regel Ihrer Tabelle funktioniert nicht ordnungsgemäß.	Entweder befindet sich eine ACL-Regel weiter oben in der Verarbeitungsreihenfolge oder eine doppelte Tabellen-ACL-Regel, die die Tabellen-ACL-Regel beeinträchtigt. Aktivieren Sie das Debugging, und bestimmen Sie, welche ACL-Regeln für die Tabelle ausgewertet werden.
Sie können ein Feld in einer Liste sehen, aber nicht in einem Formular.	Es ist möglich, dass die ACL-Regelbedingungen oder das Skript in der Liste ausgelöst werden, aber nicht im Formular. Aktivieren Sie das Debugging, und bestimmen Sie, wann die ACL-Regeln als „wahr“ ausgewertet werden. Aktualisieren Sie die Bedingungen oder das Skript so, dass die Liste und das Formular dasselbe Verhalten aufweisen.
Sie erhalten eine Fehlermeldung, wenn Sie versuchen, eine vom Prozessor oder vom Client aufrufbare Skripteinbindung auszuführen.	Es gibt eine ACL-Regel für den Prozessor oder die vom Client aufrufbare Skripteinbindung, die der Benutzer nicht erfüllt hat. Wenn der Benutzer Zugriff auf das Objekt haben soll, aktivieren Sie das Debugging und bestimmen Sie, welche ACL-Regeln für den Prozessor oder die Skripteinbindung ausgewertet werden. Aktualisieren Sie die ACL-Regel oder die Benutzerrollen nach Bedarf, um auf das Objekt zuzugreifen.

ACL-Konfigurationsbeobachter

Der ACL-Konfigurationsbeobachter teilt Ihnen mit, welche zugehörigen ACLs in einer Tabelle vorhanden sind, wenn Sie eine ACL in derselben Tabelle einfügen, aktualisieren oder löschen.

Der ACL-Konfigurationsbeobachter ist ein Interceptor-Fenster, das jedes Mal angezeigt wird, wenn Sie wichtige Änderungen an der Zugriffssteuerungstabelle [sys_security_acl] vornehmen. Es wird ein Zusammenfassungsfenster für Sicherheitsregeln angezeigt, in dem Sie ACLs anzeigen können, die sich auf die zu ändernde ACL beziehen. Sie können keine ACLs im Fenster „Sicherheitsregeln“ ändern. Um Änderungen vorzunehmen, schließen Sie das Beobachtungsfenster, und wechseln Sie zu diesen ACLs.

Der ACL-Konfigurationsbeobachter wird in den folgenden Situationen nicht angezeigt:

- Wenn Sie einen ACL-Datensatz speichern oder aktualisieren, ohne tatsächlich Änderungen vorzunehmen.
- Wenn Sie geringfügige Aktualisierungen vornehmen (keine Einfügungen oder Löschungen), z. B. Aktualisierung von Skripts, Bedingungen und der Option admin-overrides.
- Wenn der ACL-Datensatz nicht aktiv ist.

Fenster „ACL-Sicherheitsregeln“

Der Konfigurationsbeobachter zeigt den ACL-Ausführungsplan an. Der Ausführungsplan wird im Popup-Fenster für Sicherheitsregeln angezeigt. Sie können diese Art von Informationen anzeigen:

Elemente des ACL-Konfigurationsfensters

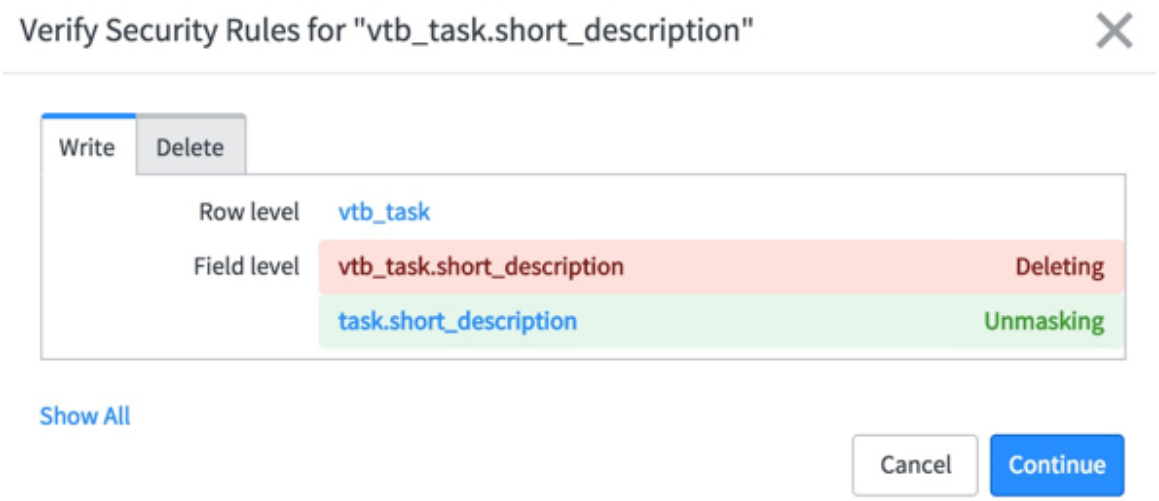
Element	Beschreibung
rote Hervorhebung	Eine ACL, die gelöscht oder deaktiviert wird.
blau hervorgehoben	Eine geänderte ACL.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elemente des ACL-Konfigurationsfensters (Fortsetzung)

Element	Beschreibung
grün hervorgehoben	Eine ACL, die hinzugefügt wird oder aktiv wird.
Passwort ändern	Eine ACL, die gültig war, bis Sie eine Änderung vorgenommen haben.
Demaskiert	Eine ACL, die erst wirksam wurde, als Sie eine Änderung vorgenommen haben.

Beispiel für Configuration Watcher



ACL-Ausführungsplan anzeigen

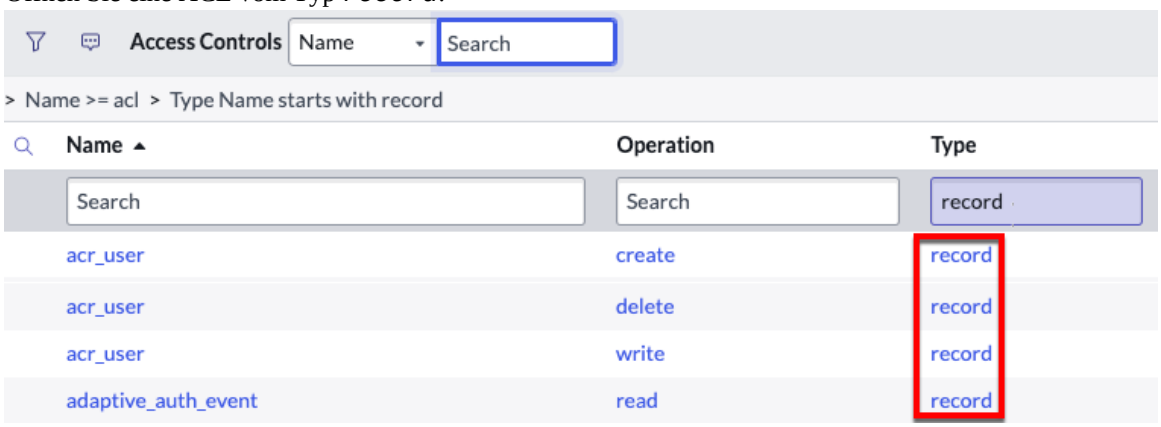
Administratoren können anzeigen, wie sich ACLs zueinander verhalten, indem sie einen Ausführungsplan für eine beliebige ACL in der Instanz anzeigen.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Führen Sie eine Erhöhung auf eine privilegierte Rolle durch.
2. Navigieren zu **Systemsicherheit** > **Zugriffssteuerung (ACL)**.
3. Öffnen Sie eine ACL vom Typ `record`.

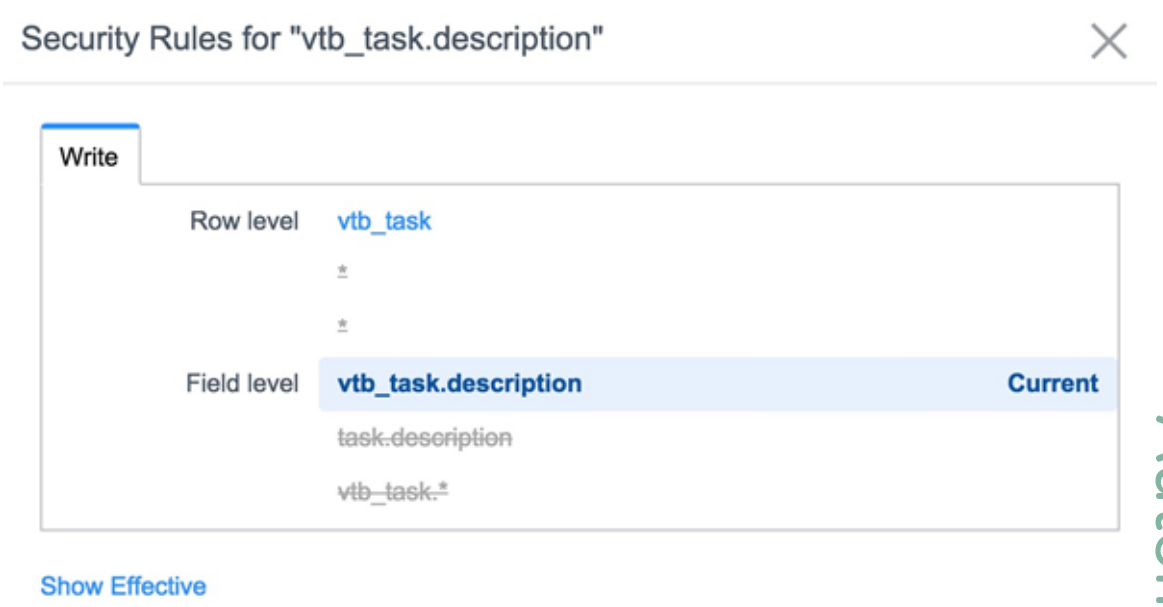


4. Klicken Sie im Abschnitt „Zugehörige Links“ auf **ACL-Ausführungsplan** anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Fenster „Sicherheitsregeln“ wird für die ACL angezeigt. In diesem Beispiel wird der Ausführungsplan für „vtb_task“ angezeigt.



Fenster des ACL-Ausführungsplans

UI-Element	Beschreibung
Titel	Der Name der ACL.
Registerkartenname	Wenn die ACL Erstellen, Lesen, Schreiben oder Löschen ist.
Zeilenebene	ACLs auf Zeilenebene, die für diese Tabelle ausgeführt werden.
Feldebene	ACLs auf Feldebene, die nur für dieses Feld (oder Spalte in der Tabelle) ausgeführt werden.

5. **Klicken** Sie auf Alle anzeigen, um alle zugehörigen ACLs anzuzeigen, einschließlich der überschriebenen ACLs und generischen ACLs, die für alle Datensätze gelten.
   Überschriebene ACLs haben eine Linie durch den Namen, und generische ACLs haben das Platzhalterzeichen Sternchen (*) für den Namen.
6. Zeigen Sie nur die unmittelbaren ACLs an, die sich auf die gerade angezeigte beziehen, und blenden Sie die ACLs in Tabellen aus, aus denen die ACL-Tabelle erweitert wird, und die generischen Platzhalter-ACLs (*), indem Sie auf **Effektive**anzeigen klicken.

Verwenden Sie den ACL-Konfigurations-Watcher

Verwenden Sie den ACL-Konfigurationsbeobachter, nachdem Sie eine Erhöhung auf die Rolle „security_admin“ durchgeführt haben.

Vorbereitungen

Erforderliche Rolle: security_admin

Führen Sie eine Erhöhung auf eine privilegierte Rolle durch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

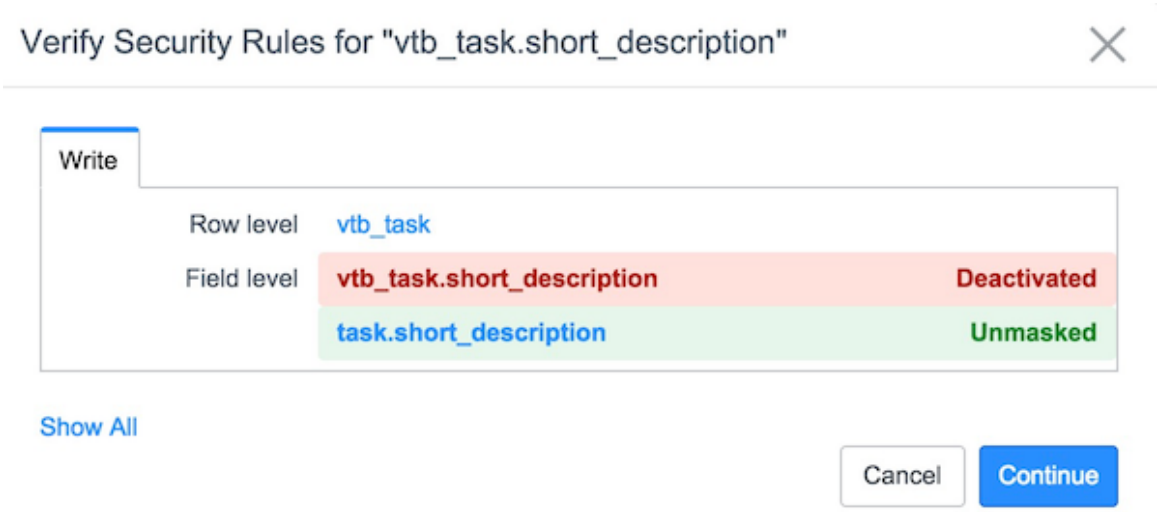
Prozedur

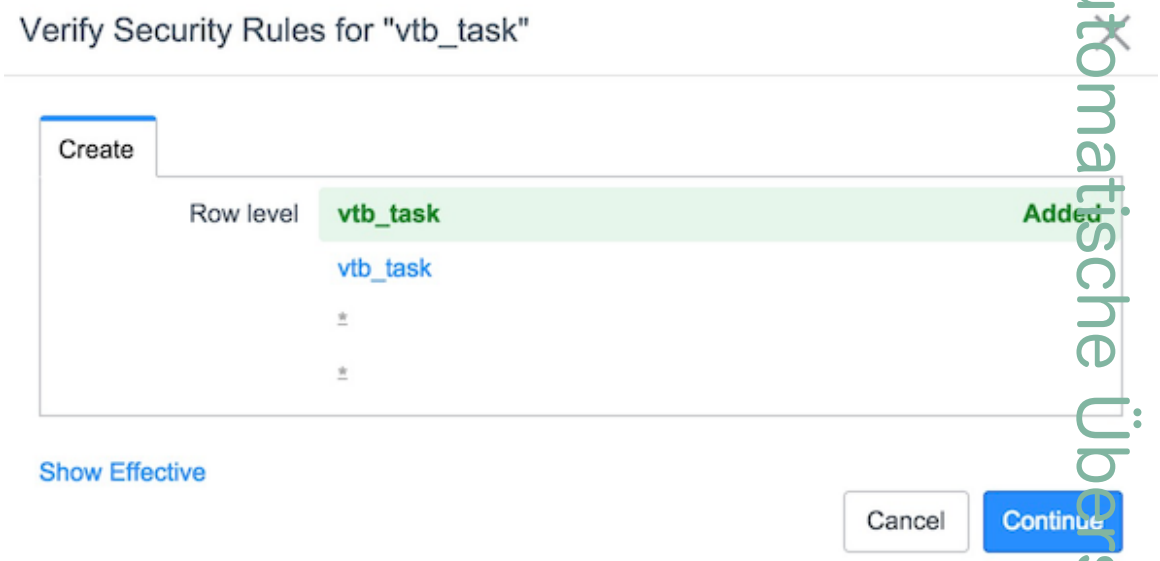
1. Öffnen Sie eine ACL, die eine Datensatztyp-ACL ist.
2. Führen Sie eine Aktion für die ACL aus, z. B. sie ändern oder eine Option aus dem Kontextmenü auswählen, z. B. **Einfügen**.
3. Wenn Sie Werte im Formular „Zugriffssteuerung“ geändert haben, klicken Sie mit der rechten Maustaste auf den Header, und wählen **Sie Speichern**, oder klicken Sie auf **Aktualisieren** oder **Löschen**.

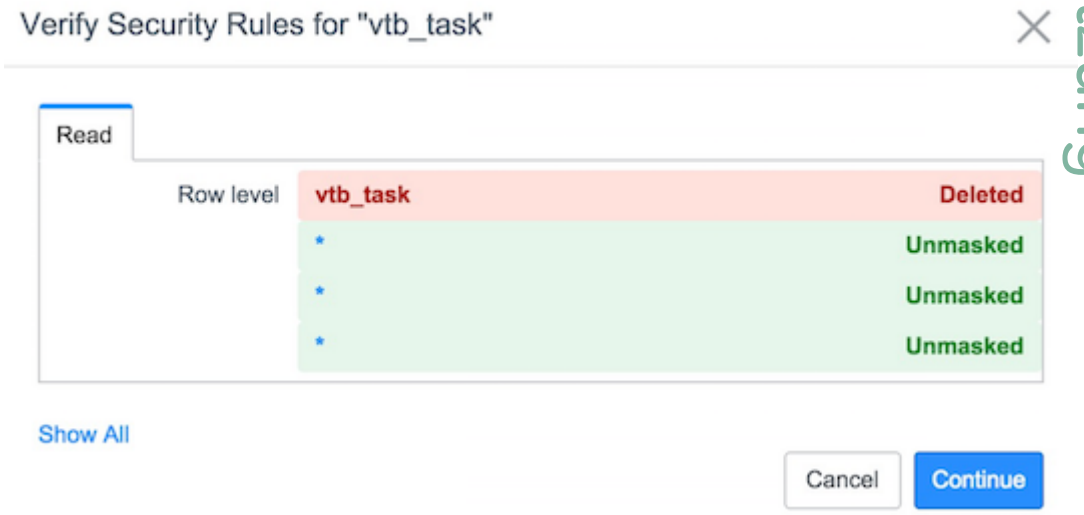
   Das Fenster Sicherheitsregeln wird angezeigt. Das System hat die Datenbankaktion für die ACL noch nicht ausgeführt, daher sind die Änderungen noch nicht gespeichert.

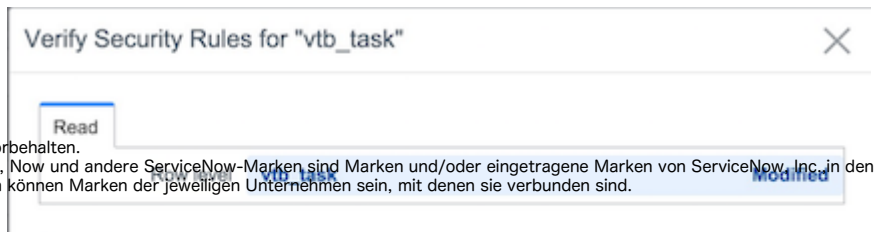
   Dies sind Beispiele für Sicherheitsregeln in der Tabelle „Private Aufgabe“ [vtb_task] der Visual Task Board-Anwendung. Unter ACL-Konfigurationsbeobachter finden Sie eine Beschreibung der Elemente in diesem Fenster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.









Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc. in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

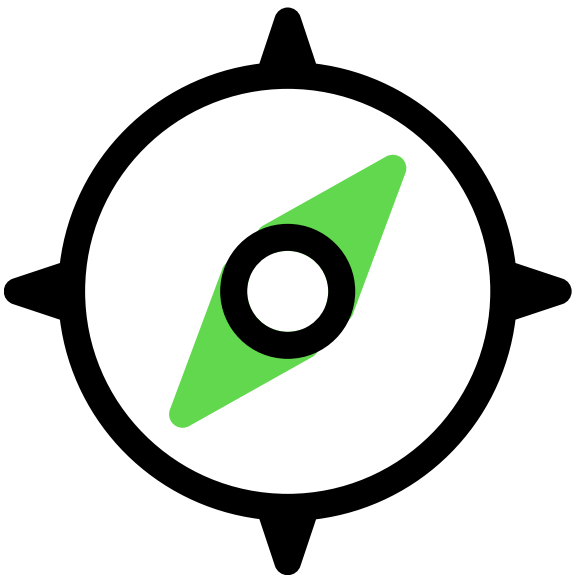
4. Genau wie beim Ausführungsplankönnen Sie auf Alle anzeigen **klicken**, um alle zugehörigen ACLs anzuzeigen, einschließlich der überschriebenen und generischen ACLs, die für alle Datensätze gelten, oder auf **Effektive** anzeigen klicken, um nur die unmittelbaren ACLs anzuzeigen, die sich auf den gerade angezeigten beziehen.
5. Zeigen Sie mit der Maus auf eine der ACLs, um eine Beschreibung anzuzeigen.

Sicherheitsattribute – Homepage

Sicherheitsattribute bieten eine flexible Alternative zum Zugriff auf Kontrolllisten.

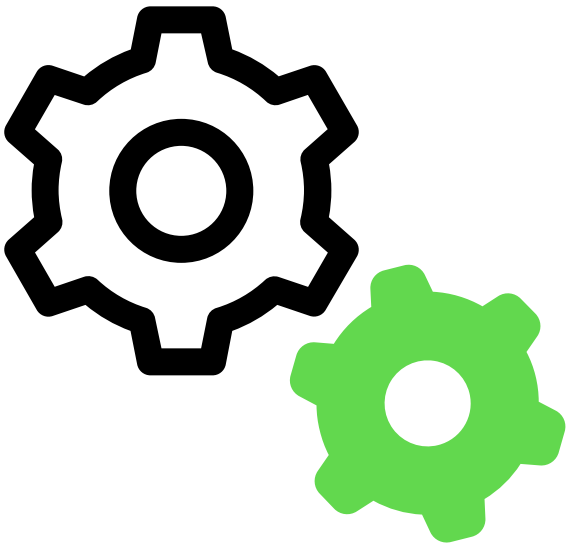
Erste Schritte

Erkunden Sie Sicherheitsattribute



Lernen Sie die Grundlagen von Sicherheitsattributen kennen

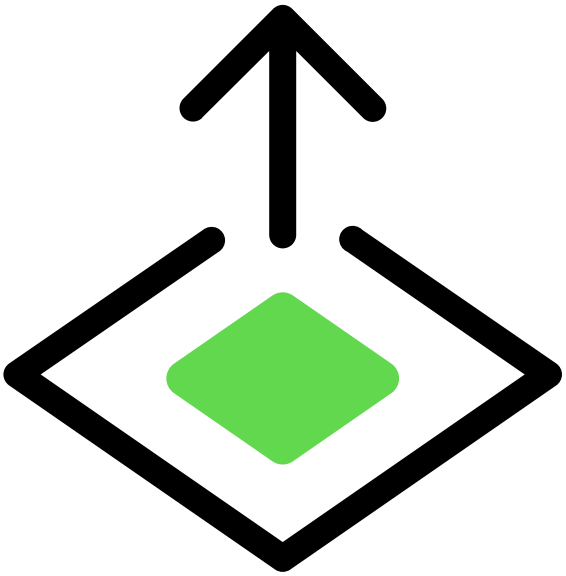
Erstellen Sie Sicherheitsattribute



Erstellen Sie neue Sicherheitsattribute

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OOB (vordefinierte) Sicherheitsattribute



Erklären Sie die OOB-Sicherheitsattribute

Protokollierung von Sicherheitsattributen

Überprüfen Sie die Protokollierung des Sicherheitsattributs

Sicherheitsattribute – Grundlagen

Ein Sicherheitsattribut ist eine hochgradig konfigurierbare Information über ein Thema oder seine Umgebung. Wenn es in Zugriffskontrollen verwendet wird, ermöglicht es eine feingranulare Sicherheitskonfiguration auf nicht komplexe Weise.

Übersicht

Sicherheitsattribute bieten eine alternative Methode für die Zugriffssteuerung über Rollendefinitionen zur derzeit gängigen ACL-Konfiguration (Access Control Lists, Zugriffssteuerungslisten). Sicherheitsattribute bieten ACL-basierte Konfigurationen mehrere Vorteile:

Bessere Sicherheit

Die verbesserte Verschleierung der Berechtigungsbewertung stellt sicher, dass Ihre Organisation sicher bleibt.

Visuell lesbar

Sicherheitsattribute sollen die Erstellung und Verwendung von Sicherheitsberechtigungen vereinfachen.

Flexible Sicherheit

Erstellen Sie Persona-Definitionen aus der Standardkonfiguration in Kombination mit benutzerdefinierten Personas.

Protokollierung und Auditing

Sicherheitsattribute bieten detaillierte Audits und Protokollierungen, um mehr Einblicke in Sicherheitsmaßnahmen und -Theorien zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Sicherheitsattribute

Erstellen Sie neue Sicherheitsattribute mit einer Schritt-für-Schritt-Anleitung.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **System Sicherheit** > **Sicherheitsattribute**.
2. Wählen Sie in der Liste „Sicherheitsattribute“ die Option **Neu**aus.
3. Füllen Sie die Felder im Formular „Sicherheitsattribute“ aus.

Sicherheitsattributfelder

Feld	Beschreibung
Bezeichnung	Bezeichnung des Sicherheitsattributs.
Name	Name des Sicherheitsattributs.
Typ	Der Typ des Sicherheitsattributs. ○ Verbindung **Hinweis:** Weitere Informationen zu zusammengesetzten Sicherheitsattributen finden Sie unter Zusammengesetzte Sicherheitsattribute ○ integer ○ Liste ○ Zeichenfolge ○ boolean(true|false)
Ist dynamisch	Gibt an, ob der Sicherheitsattributwert für jeden neu ausgewertet werden muss
Beschreibung	Anwendergenerierte Beschreibung des Sicherheitsattributs
Anwendung	Statisches Feld, Anwendungsbereich.
Suchtabelle	Verweisen Sie zur Auswertung auf eine externe Tabelle.
Tabellenspalte suchen	Verweisen Sie auf eine Tabellenspalte für die Auswertung.
Skript	Leiten Sie einen Wert von einem Skript ab.

OOB (vordefinierte) Sicherheitsattribute

Häufig verwendete, allgemeine Sicherheitsattributrollen, die zur Verwendung bereit sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht

Die sofort einsatzbereiten Sicherheitsattribute sind eine einfache Möglichkeit, die Fähigkeiten von Sicherheitsattributen mit einer Reihe vorkonfigurierter Sicherheitsattributrollen zu verwenden und zu erlernen. Die OOB-Sicherheitsattributrollen sind häufig verwendete Zugriffssteuerungsrollen.

Informationen zum Erstellen eines eigenen Sicherheitsattributs oder zum Erweitern der Fähigkeiten eines OOB-Sicherheitsattributs finden Sie unter Zusammengesetzte Sicherheitsattribute

OOB-Sicherheitsattribute

Attribut	Beschreibung
Gruppe	Anwender ist Mitglied einer angegebenen Gruppe
GroupExplicit	Benutzer ist ein explizites Mitglied einer bestimmten Gruppe
HatAdminRole	Anwender hat die Administratorpersona
Verwendung einer anderen Identität	Die Identität des Anwenders wird angenommen
Interaktive Sitzung	Aktuelle Sitzung interaktiv
Angemeldet	Benutzer ist angemeldet und authentifiziert
Netzwerkkriterien	Zusätzliche Netzwerkkriterien
Rolle	Anwender hat eine bestimmte Rolle
RoleExplicit	Anwender hat eine spezifische Rolle, die explizit definiert ist

Nicht explizites und explizites Verhalten erklärt

Sicherheitsattribute berücksichtigen differenzierte Berechtigungsanforderungen mit einer expliziten im Vergleich zu einer nicht expliziten (übernommenen) Bewertung von Rollenberechtigungen.

[qa: BEGIN review]

Example: Trennen Sie den Zugriff auf IT-Personas vom Zugriff auf HR-Rollendateien

Wir definieren ein Sicherheitsattribut, das dem Administrator das Anzeigen von HR-bezogenen Dateien ermöglicht, dem Administrator jedoch keinen Zugriff auf die Datei ermöglicht. Angenommen, die Administratorrolle ist nicht als Teil der HR-Gruppe definiert, sondern _____. Die **Rolle** sieht _____[End]

Zusammengesetzte Sicherheitsattribute

Mit zusammengesetzten Sicherheitsattributen können Sie konsistente und wiederverwendbare Sicherheitsattributprofile erstellen, die Ihren Geschäftsanforderungen entsprechen

Übersicht

Zusammengesetzte Sicherheitsattribute werden aus einem oder mehreren bereits vorhandenen Sicherheitsattributen definiert, um eine einzelne Referenzkombination von Sicherheitsattributen für die Berechtigungsauswertung zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[qa: BEGIN review]

Verhalten des zusammengesetzten Sicherheitsattributs

[End]

Erstellen Sie zusammengesetzte Sicherheitsattribute

Erstellen Sie ein zusammengesetztes Sicherheitsattribut zur einfachen Wiederverwendung.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Sicherheitsattribute**.
2. Wählen Sie in der Liste „Sicherheitsattribute“ die Option **Neu**aus.
3. Wählen Sie Verbindung im Feld **Typ** aus.
4. Füllen Sie die Felder im Formular „Sicherheitsattribute“ aus.

Sicherheitsattributfelder

Feld	Beschreibung
Bezeichnung	Bezeichnung des Sicherheitsattributs.
Name	Name des Sicherheitsattributs.
Beschreibung	Anwendergenerierte Beschreibung des Sicherheitsattributs
Bedingung	Die spezifischen Sicherheitsattributbedingungen, die zum Definieren der Sicherheitsattributauswertung verwendet werden.
Neues Kriterium	Fügen Sie einen zusätzlichen Satz von **ODER** -Bedingungen für die Auswertung hinzu.

Sicherheitsattribut Umfang

Sicherheitsattribute unterstützen die Umfangsdefinition.

Umfangsdefinition des Sicherheitsattributs

Das bereichsbezogene Verhalten von Sicherheitsattributen stimmt mit dem bereichsbezogenen Verhalten der Plattform überein. Innerhalb eines Bereichs erstellte Sicherheitsattribute sind nur in Zugriffssteuerungen im selben Bereich verfügbar.

Lokale und vorhandene Sicherheitsattribute

Vorhandene und lokale Sicherheitsattribute ermöglichen es Kunden, Sicherheitsattribut-Bedingungssätze wiederzuverwenden.

Lokale und vorhandene Attribute

Mit dem Bedingungsgenerator für ACL-Sicherheitsattribute können Kunden angeben, ob ein Sicherheitsattribut entweder vorhanden oder lokal ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Bedingungen für Sicherheitsattribute sind standardmäßig lokal.

Ein lokal definiertes Sicherheitsattribut wird nur in der einzelnen ACL gespeichert, in der es in erstellt wird.

Mit der Option „Vorhanden“ können Benutzer auf vorhandene Sicherheitsattributbedingungen für den Bedingungsgenerator verweisen.

Data Classification

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

Erkunden Sie die Datenklassifizierung

Erfahren Sie mehr über die Datenklassifizierung.

Konfigurieren Sie die Datenklassifizierung

Erstellen und konfigurieren
Sie Ihre eigenen Datenklassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz für Datenklassifizierung

Erfahren Sie, wie die Datenklassifizierung mit Demodaten funktioniert.

Analysieren von Datenklassifizierungen

Erfahren Sie, wie Sie Datenklassifizierungen analysieren.

Datenklassifizierung erkunden

Informieren Sie sich über die Datenklassifizierung.

Data Classification aktiviert die Unterstützung für:

- Einblick in die Datentypen, die auf einer Now Platform -Instanz gehostet werden.
- Compliance mit Datenschutzgesetzen und Erfüllung von gesetzlichen Anforderungen für Branchen wie Finanzdienstleistungen und Herstellung medizinischer Geräte.

Datenklassifizierungen

Die Datenklassifizierung ist ein eigenständiger Prozess, bei dem Sie Datenklassifizierungen manuell auf vorhandene Wörterbucheinträge in einer beliebigen Tabelle anwenden. Weitere Informationen finden Sie unter Data dictionary tables .

- Sie klassifizieren Daten nach Bedarf für Ihr Unternehmen und können die verfügbaren Datenklassen nach Bedarf ändern.
- Wenn Sie Daten klassifizieren, können Sie die vordefinierten Datenklassifizierungen verwenden oder eigene erstellen. Obwohl die Verwendung vordefinierter Datenklassifizierungen optional ist, wird dies als Ausgangspunkt empfohlen. Diese vordefinierten Datenklassifizierungen sind in Demodaten enthalten, die Sie in Ihrer Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

installieren können. Weitere Informationen finden Sie unter Demodaten des Plugins Data Classification werden installiert und Mit Data Classification Demodaten installierte Komponenten.

- Wenn Sie eigene Datenklassifizierungen erstellen, können Sie auch ein abgestuftes hierarchisches System mit übergeordneten und untergeordneten Datenklassifizierungen entwerfen.

Übersichts-Dashboard

Verwenden Sie das Übersichts-Dashboard, um zu verstehen, wie Ihre aktuellen Datentabellen verschiedenen Datenklassifizierungen zugeordnet werden. Sie können auch analysieren, inwieweit Ihre globalen, regionalen und internationalen Benutzer unterschiedliche Ansätze für die Datenklassifizierung in Bezug auf die Verwendung von oder den Zugriff auf Daten benötigen. Sie können auch den Inhalt und das Layout des Übersichts-Dashboards an Ihre Anforderungen anpassen.

Informationen zur Verwendung der verfügbaren Skript- und REST-APIs zum Anwenden der Klassifizierungsmetadaten in vorhandenen Prozessen, Workflows und Anwendungen finden Sie unter:

- Datenklassifizierung – REST-API
- DCManager – Global
- ScopedDCManager: Scoped

Hinweis:
Data Classification unterstützt die Domänentrennung, und die Tabelle „data_classification“ selbst ist prozessgetrennt.

Anwendungsfälle

Die Allgemeine Datenschutz-Verordnung (DSGVO) ist eine Verordnung der Europäischen Union, deren Zweck darin besteht, Einzelpersonen die Kontrolle über ihre eigenen personenbezogenen Daten zu geben. Sie können Datenklassifizierungen wie personenbezogene Daten verwenden, um zu ermitteln, wo personenbezogene Daten in Ihrer Instanz gespeichert werden. Durch die Anwendung der entsprechenden Sicherheitsmechanismen zum Schutz dieser personenbezogenen Daten vor der Weitergabe erfüllt Ihr Unternehmen die DSGVO-Anforderungen.

Wenn Sie Kundeninformationen in Now Platformspeichern, verwenden Sie den Klassifizierungscode für personenbezogene Daten (Personally Identifiable Information, PII) bei Bedarf, um Daten nachzuverfolgen, die den Vorschriften der lokalen Datenschutzgesetze unterliegen. Wenn Sie Demodaten installieren, wird dieser Klassifizierungscode automatisch auf bestimmte sicherheitsrelevante Felder in der Benutzertabelle [sys_user] angewendet. Weitere Informationen finden Sie unter:

- Mit Data Classification Demodaten installierte Komponenten
- Datenklassifizierungen zu Wörterbucheinträgen zuweisen

Sie können eine eingeschränkte Datenklassifizierung auf Spalten der Mitarbeitertabelle anwenden, in denen vertrauliche Mitarbeiterinformationen wie Sozialversicherungsnummern (SSN) gespeichert werden. Administratoren und Auditoren können dann im Übersichts-Dashboard überprüfen, ob Sie die Datenklassifizierungen den richtigen Spalten zugewiesen haben. Sie können auch die Klassifizierungsdetails für eingeschränkte Arten von Informationen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Demodaten des Plugins Data Classification werden installiert

Wenn Sie ein Upgrade auf oder eine Installation von Washington DC (und höher) durchführen, wird das Plugin Data Classification (com.glide.data_classification) automatisch aktiviert. Sie sollten jedoch die Demodaten, die mit dem Plugin geliefert werden, manuell installieren. Sie enthält mehrere wichtige vordefinierte Datenklassifizierungen und weist eine davon bestimmten Benutzertabellenspalten [sys_user] in Ihrer Instanz zu.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Unabhängig davon, ob Sie Demodaten installieren, fügt das aktivierte Plugin Data Classification die folgenden Benutzerrollen in Ihrer Instanz hinzu:

- data_classification_admin: Kann alle Aspekte der Anwendung Data Classification verwalten, einschließlich der Einrichtung und Zuweisung der Datenklassifizierung.
- data_classification_auditor: Kann Data Classification Codezuweisungen an Benutzertabellen und -spalten prüfen.

Wichtig:

Hinweis zur Verwendung durch Kunden:

Alle Entscheidungen im Zusammenhang mit der Implementierung dieser Anwendung unterliegen der alleinigen Entscheidung des Kunden. Kunden erkennen an und erklären sich damit einverstanden, dass die Verwendung der Anwendung keine Zusicherung von ServiceNow in Bezug auf die Einhaltung von Gesetzen oder Vorschriften darstellt und jede vorgeschlagene Sprache, jedes Feld oder jede vorgeschlagene Klassifizierung, die vorkonfiguriert mit der Anwendung bereitgestellt wird, keine Rechtsberatung durch ServiceNow darstellt.

Kunden sind allein verantwortlich für die Einhaltung ihrer gesetzlichen Verpflichtungen nach geltendem Recht, einschließlich (aber nicht beschränkt auf) Datenschutz, Sicherheitsanforderungen und Datenschutzgesetze, und sind für die Konfiguration und Vornahme aller erforderlichen Änderungen an dieser Anwendung verantwortlich, einschließlich (aber nicht beschränkt auf). bis) Vorlagen, um die Anforderungen der Kunden zu erfüllen.

Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin Data Classification mithilfe der Filterkriterien und der Suchleiste. Nachdem Sie das Plugin gefunden haben, wird die Meldung Installiert angezeigt.
3. Klicken Sie auf das Symbol mit den drei vertikalen Punkten, und wählen Sie dann **Reparieren** aus, um auf das Dialogfeld „Plugin aktivieren“ zuzugreifen.
4. Wählen Sie **Demodaten laden**aus, und klicken Sie dann auf **Reparieren**.

Mit Data Classification Demodaten installierte Komponenten

Wenn Sie die im Plugin Data Classification (com.glide.data_classification) enthaltenen Demodaten installieren, werden verschiedene Arten von Komponenten in Ihrer Instanz installiert. Diese Komponenten umfassen vordefinierte Datenklassifizierungen und Codezuweisungen für bestimmte Benutzerspalten [sys_user].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenklassifizierungen installiert

Datenklassifizierung	Beschreibung
Vertraulich	Vertrauliche Daten, die bei Gefährdung den Betrieb negativ beeinflussen könnten.
Intern	Interne Daten, die nicht veröffentlicht werden sollen.
Persönlich identifizierbare Informationen	Wird auch als PII bezeichnet. Daten, die potenziell zur Identifizierung einer bestimmten Person verwendet werden könnten.
Öffentlich	Daten, die der Öffentlichkeit frei zugänglich gemacht werden können.
Beschränkt	Hochsensible Unternehmensdaten, die bei Gefährdung die Organisation einem finanziellen oder rechtlichen Risiko aussetzen könnten.

Data Classification Zuweisungen

Tabelle	Zugewiesene Spalte	Zugewiesene Datenklassifizierung
sys_user	Postleitzahl	Persönlich identifizierbare Informationen
sys_user	first_name	Persönlich identifizierbare Informationen
sys_user	E-Mail	Persönlich identifizierbare Informationen
sys_user	city	Persönlich identifizierbare Informationen
sys_user	Middle_name	Persönlich identifizierbare Informationen
sys_user	Straße	Persönlich identifizierbare Informationen
sys_user	mobile_phone	Persönlich identifizierbare Informationen
sys_user	last_name	Persönlich identifizierbare Informationen
sys_user	country	Persönlich identifizierbare Informationen
sys_user	Geschlecht	Persönlich identifizierbare Informationen
sys_user	Name	Persönlich identifizierbare Informationen
sys_user	Foto	Persönlich identifizierbare Informationen
sys_user	Status	Persönlich identifizierbare Informationen
sys_user	home_phone	Persönlich identifizierbare Informationen

Erstellen von Datenklassifizierungen

Erstellen Sie Ihre eigenen benutzerdefinierten Datenklassifizierungen in der Tabelle Data Classification [data_classification], die Sie dann bestimmten Spalten in bestimmten Tabellen zuweisen können.

Vorbereitungen
Erforderliche Rolle: data_classification_admin, admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenklassifizierung** > **Datenklassen**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Klassifizierungsname	Name der Datenklassifizierung.
Beschreibung	Beschreibung der Datenklassifizierung.
Übergeordnet	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung kein übergeordnetes Element für untergeordnete Datenklassifizierungen ist.
Anwendung	Anwendungsbereich für diese Datenklassifizierung.

4. Wenn diese Datenklassifizierung ein übergeordnetes Element für untergeordnete Datenklassifizierungen sein soll, klicken Sie auf **Neu**.
   Wenn Sie keine untergeordneten Datenklassifizierungen erstellen möchten, überspringen Sie diesen Schritt.
5. Füllen Sie die Felder des Formulars aus.

   Titel

Feld	Beschreibung
Klassifizierungsname	Name der untergeordneten Datenklassifizierung.
Beschreibung	Beschreibung der untergeordneten Datenklassifizierung.
Übergeordnet	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung kein übergeordnetes Element für untergeordnete Datenklassifizierungen ist.
Anwendung	Anwendungsbereich für diese untergeordnete Datenklassifizierung.

6. Klicken Sie auf **Absenden**.

Datenklassifizierungen zu Wörterbucheinträgen zuweisen

Weisen Sie Datenklassifizierungen bestimmten Tabellenspalten in der Wörterbuchtabelle [sys_dictionary] zu. Wenn Sie Datenklassifizierungen zuweisen, werden Einträge in der Tabelle Dictionary-Data Class [m2m_dictionary_dataclass] erstellt, die Sie dann im Dashboard „Übersicht“ überprüfen können.

Vorbereitungen

Erforderliche Rolle: data_classification_admin und admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Navigatorbereich sys_dictionary.list ein.
2. Wählen Sie in Wörterbucheinträge jedes der Elemente aus, denen Sie bestimmte Datenklassifizierungen zuweisen möchten.
3. Klicken Sie nach Auswahl der Elemente auf **Aktionen für ausgewählte Zeilen**und wählen Sie **Klassifizieren**aus.

   Hinweis:
   Um zuvor zugewiesene Datenklassifizierungen für ausgewählte Wörterbuchelemente zu löschen, können Sie **Klassifizierung**löschen auswählen.

4. Wenn das Dialogfeld „Zu Datenklasse zuweisen“ angezeigt wird, wählen Sie die Datenklassifizierungen aus, die Sie den ausgewählten Wörterbuchelementen zuweisen möchten, und klicken Sie dann auf **Klassifizieren**.

   Warnung:
   Dadurch werden alle vorhandenen Klassifizierungen für die ausgewählten Wörterbuchelemente überschrieben.

   Sie können nach Bedarf mehrere Datenklassifizierungen auswählen.

   Weitere Informationen finden Sie unter Datenwörterbuchtabellen .

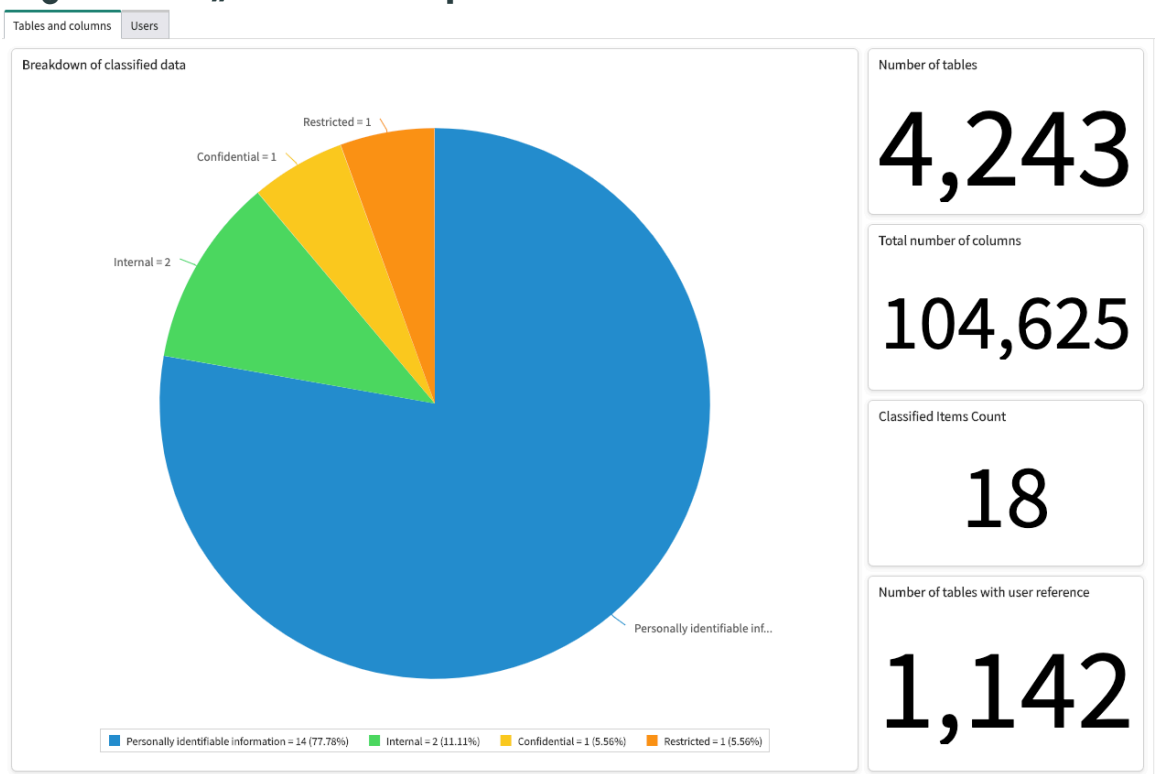
Analysieren von Datenklassifizierungen mit dem Übersichts-Dashboard

Das Übersichts-Dashboard meldet den aktuellen Status der Datenklassifizierungen in Ihrer Instanz und wie Ihre Benutzer nach Standort verteilt sind.

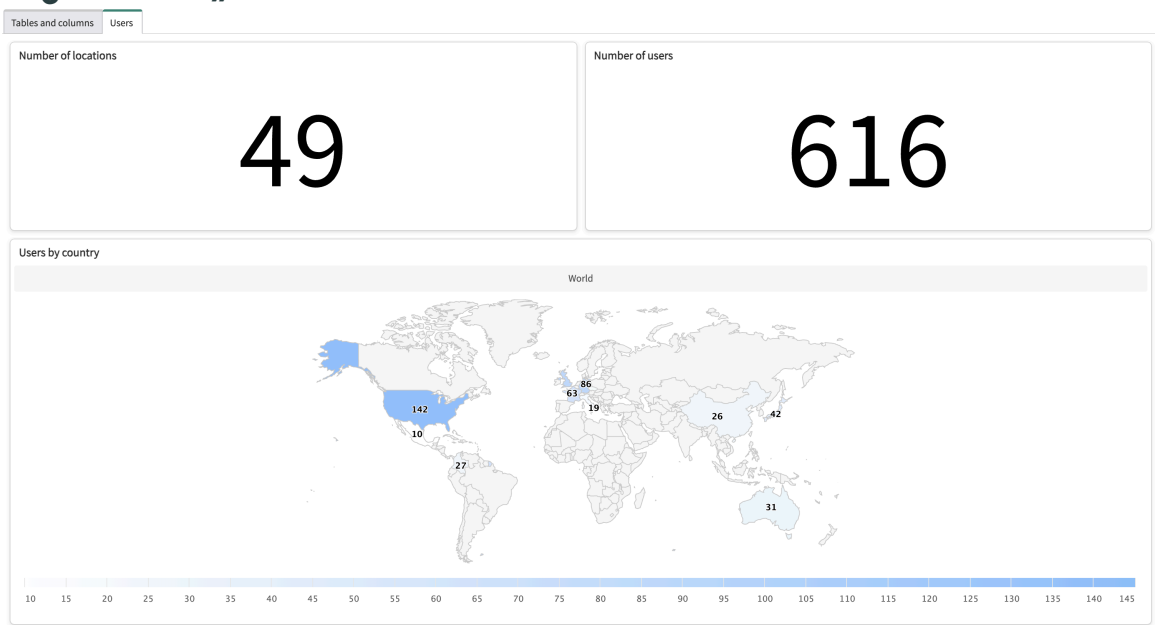
Wenn Sie die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ haben, können Sie die aktuelle Vertraulichkeit von Instanzdaten visualisieren, was die Sicherheit und Compliance mit Datenschutzgesetzen erhöht. Durch die Verwendung des Felds Standort in Benutzerdatensätzen können Administratoren Benutzer in verschiedenen Regionen mit unterschiedlichen Datenschutzbestimmungen zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Tabellen und Spalten“.



Registerkarte „Benutzer“.



Erforderliche Now Platform-Rollen

- data_classification_admin: Verwaltet alle Aspekte der Anwendung Data Classification, einschließlich Einrichtung der Datenklassifizierung und Zuweisung.
- data_classification_auditor: Prüft Data Classification Codezuweisungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

Weitere Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie unter Anwendungsfälle in Data Classification.

Benutzer	Dashboard-Verwendung
data_classification_admin	Bestätigen Sie, dass Sie Datenklassifizierungen den richtigen Feldern in Ihrer Instanz zugewiesen haben.
data_classification_auditor	Auditieren Sie die Senilität und Sicherheit der Daten in Ihrer Instanz.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Aufgliederung klassifizierter Daten	Kreisdiagramm	m2m_dictionary_dataclass	Stellt eine Aufgliederung der Instanzdatenklassifizierungen nach Datenklasse bereit.
Gesamtzahl der Tabellen	Einzelne Punktzahl	sys_dictionary	Gesamtzahl der Datentabellen in Ihrer Instanz.
Gesamtanzahl der Spalten	Einzelne Punktzahl	sys_dictionary	Gesamtzahl der klassifizierten Datenspalten in Ihrer Instanz. Diese Anzahl ist die Anzahl der Spalten, denen Sie Datenklassifizierungen zugewiesen haben.
Anzahl der klassifizierten Elemente	Einzelne Punktzahl	m2m_dictionary_dataclass	Gesamtzahl der Tabellen, denen Datenklassifizierungen zugewiesen wurden.
Anzahl der Tabellen mit Anwenderreferenz	Einzelne Punktzahl	sys_dictionary	Gesamtzahl der Tabellen, die mindestens eine Spalte enthalten, die auf die Tabelle „sys_user“ verweist.
Anzahl der Standorte	Einzelne Punktzahl	sys_dictionary	Gesamtzahl der Standorte in Ihrer Instanz.
Anzahl der Benutzer	Einzelne Punktzahl	sys_user	Gesamtzahl der Benutzer in Ihrer Instanz.
Anwender nach Land	Karte	sys_user	Standortaufgliederung der Anwender nach Land.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung und Data Classification

Domänentrennung wird für Data Classification unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Erweitert

- Umfasst die Stufen **Basis** und **Standard**.
- Ein datengesteuerter Prozess ermöglicht es Service Provider-Kunden, die Geschäftslogik basierend auf definierten Anwendungsfällen zu ändern. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass Konfigurationen von einem Kunden sich nicht auf einen anderen auswirken können.
- Mandanten der Instanz müssen die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter für sich selbst konfigurieren können. Diese Logik und diese Parameter würden für die normale Funktion der Anwendung erwartet.

Beispiel-Anwendungsfall: Mandanten-Kunden einer gemeinsam genutzten Umgebung müssen in der Lage sein, Änderungen an der Auswirkungs-, Dringlichkeits- und Prioritätsmatrix vorzunehmen, um die Priorität in ihrer Domäne festzulegen.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

So funktioniert Domain Separation in Data Classification

Für die Domänentrennung verwendet die Anwendung die Prozesstrennung für die Tabelle Data Classification [sys_data_classification]. Für die Tabelle Dictionary-Data Class [m2m_dictionary_dataclass] wird Datentrennung verwendet. Weitere Informationen zur Daten- und Prozesstrennung finden Sie unter Domänentrennung erklärt.

Zugehörige Informationen

Domänentrennung für Service Provider

Datenfilterung

Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie Datenfilterung

Erfahren Sie mehr über Datenfilterung.

Erstellen Sie Datenfilterungsregeln

Erstellen Sie Ihre eigenen Datenfilterungsregeln, die Ihren Anforderungen entsprechen.

Daten debuggen

Erfahren Sie, wie Sie die Ergebnisse der Datenfilterung debuggen.

Datenfilterung erkunden

Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Datenfilterung ist eine separate Form der Zugriffskontrolle, die auf die vorhandenen Zugriffskontrollregeln (ACLs) in Ihrer Instanz abgestimmt ist. Die Datenfilterung verweigert den Zugriff auf Tabellen und Datensätze, die nicht mit den vom Administrator definierten Betreffattributen übereinstimmen. Die Datenfilterung soll Auditing, Berichterstellung und Fehlerbehebung erleichtern.

Dies ist eine optionale Funktion, die Administratoren in ihrer Instanz aktivieren können.

Datenfilterungsfunktionen

Datenfilter

Verwenden Sie Datenfilter, um Zugriff basierend auf Informationen in einem Datensatz zu gewähren. Datenfilter verwenden Daten in einem Tabellenfeld, um zu bestimmen, ob ein Datensatz für Ihre Benutzer verfügbar ist.

Auf Betreffattributen basierender Bedingungsgenerator

Verwenden Sie Betreffattribute, um Benutzerrolle, Gruppe, Betreffkriterien oder IP-Netzwerkadresse auszuwerten.

Die Datenfilterung verwendet ein Deny-basiertes Modell

Bei der Datenfilterung wird ein Deny-basiertes Modell verwendet, um den Zugriff auf Datensätze zu steuern. Bei der Datenfilterung verweigert Ihre Instanz den Zugriff auf Datensätze, es sei denn, ein Datensatz erfüllt die durch die Datenfilterung definierten Kriterien.

Datenfilterung erzwingen

Datenfilterregeln werden nach der Datenbankabfrage für READ-Vorgänge ausgeführt und vor ACLs ausgewertet. Ein Datensatz, der von einer Datenfilterungsregel verweigert wird, wird nicht fortgesetzt und von ACL-Regeln ausgewertet.

- Die Durchsetzung der Datenfilterungsregeln stimmt mit der von READ ACLs überein.
- Datenfilterung funktioniert wie ACLs in Verbindung mit vorhandenen *`Report_view access control list`* -Verhalten. Weitere Informationen zur Konfiguration dieser Berichtssteuerungen finden Sie unter report_view-Zugriffssteuerung .

Debugging von Sitzungen

Die Datenfilterung unterstützt das Debuggen von Sitzungen. Verwenden Sie Sitzungsdebugging, um zu sehen, welche Datenfilterungsdatensätze für eine bestimmte Abfrage gelten. Administratoren können diese Informationen verwenden, um Probleme beim Benutzerzugriff auf Datensätze zu beheben.

Komponenten der Datenfilterung

Die Datenfilterung funktioniert mit den folgenden Datensatztypen:

Datenfilterungsdatensätze

Erstellen Sie einen Datenfilterungsdatensatz [sys_df_data_filterung], um Tabellenzugriff in Ihrer Instanz zu gewähren. Der Datenfilterungsdatensatz enthält die oben beschriebenen Bedingungen für **Datenfilter** und **Betreffattribut**, um den Umfang der Regel und die betroffenen Benutzer zu begrenzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

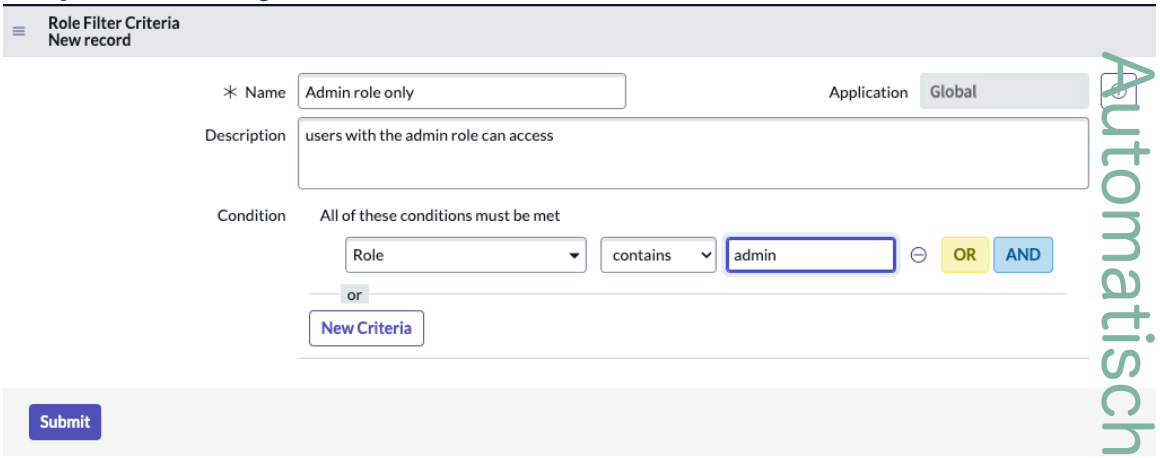
Datensätze mit Betreffkriterien

Datensätze mit Betreffkriterien [sys_df_subject_criteria] stellen bestimmte Benutzerattribute dar, mit denen Sie bestimmen können, ob der Zugriff mit einer Datenfilterregel gewährt werden soll. Diese Attribute können die Gruppen, Rollen oder IP-Adressen eines Benutzers sein. Um ein Betreffkriterium zu erstellen, müssen Sie den Betreffkriteriendatensatz sowie Kriterieneingabe- und Kriterienbedingungsdatensätze erstellen. Details zu diesem Vorgang finden Sie unter Betreffkriterien werden erstellt.

Nachdem Sie Datensätze mit Betreffkriterien erstellt haben, können Sie sie auf eine Regel anwenden. Dies geschieht auf der Registerkarte **Betreffbedingung** Ihrer Datenfilterregel.

Beispiele für Kriterieneingabedatensätze

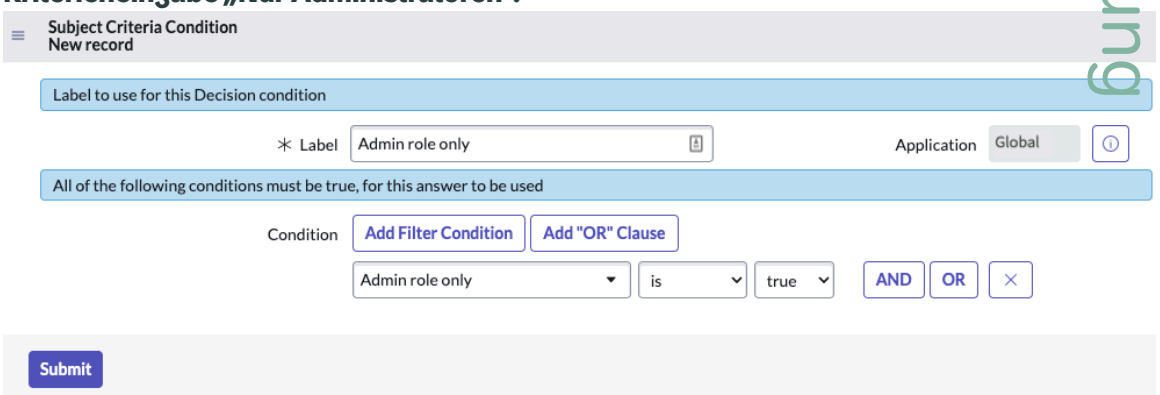
Beispielkriterieneingabe für alle Rollen, die admin enthalten



Kriterieneingaben [sys_df_subject_filter_criteria_m2m] sind Datensätze, die Kriterien enthalten, die mit dem Benutzer verglichen werden sollen. Dies kann eine Liste von Benutzergruppen oder Rollen, ein IP-Adressbereich oder ein IP-Adress-Subnetz sein. Diese Datensätze werden zusammen mit Bedingungsdatensätzen für Betreffkriterien verwendet, um anhand der Gruppen, Rollen oder IP-Adressen eines Benutzers den Zugriff auf eine Tabelle oder deren Datensätze zu bestimmen.

Bedingungsdatensätze für Betreffkriterien

Beispiel für Kriterienbedingung unter Verwendung der Kriterieneingabe „Nur Administratoren“.



Verwenden Sie Datensätze für Betreffkriterienbedingungen [sys_df_subject_criteria_condition], um zu definieren, wie Benutzerattribute mit den in Ihren Kriterieneingaben definierten Rollen, Gruppen oder IP-Adressen verglichen werden. Sie können mehrere Kriterieneingaben in einer einzelnen Betreffkriterienbedingung verwenden, um den Zugriff auf Ihre Datensätze weiter einzuschränken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenfilterung wird aktiviert

Erfahren Sie, wie Sie die Datenfilterung in Ihrer Instanz aktivieren.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**.
2. Verwenden Sie das Suchfeld, um das Plugin „Data Filterung“ (com.glide.data_filterung) zu finden.
3. Klicken Sie auf **Installieren**, und klicken Sie dann im Dialogfeld „Plugin aktivieren“ auf **Aktivieren**.

Erstellen von Datenfilterungsregeln

Erfahren Sie, wie Sie Datenfilterregeln erstellen, um Ihren Benutzern den Zugriff auf Datensätze zu gewähren, die Tabellen sind.

Vorbereitungen
Erforderliche Rolle: security_admin

Hinweis:
Um Datenfilterungsregeln zu erstellen oder zu ändern, müssen Sie eine Erhöhung auf die privilegierte Rolle durchführen. Weitere Informationen zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle erhöhen.

Prozedur

1. Navigieren zu **Alle** > **Datenfilterung** > **Datensätze der Datenfilterung**.
2. Klicken Sie in der **Datenfilterungsliste** auf **Neu**.
   Ein neues Datenfilterungsformular wird angezeigt.
3. Füllen Sie die Felder im Formular nach Bedarf aus.

Formular „Datenfilterung“.

Feld	Beschreibung
Tabelle	Tabelle, für die diese Datenfilterungsregel gilt.
Aktiv	Legt die Datenfilterungsregel als aktiv fest. **Hinweis:** Lassen Sie die Datenfilterungsregeln inaktiv, bis Sie zum Testen bereit sind, um zu vermeiden, dass Benutzer unbeabsichtigt aus Datensätzen ausgeschlossen werden.
Beschreibung	Beschreibung der Datenfilterungsregel.
Kaskadierend	Wählen Sie diese Option aus, um die Datenfilterungsregel festzulegen, die auf erweiterte Tabellen angewendet werden soll. Wählen Sie beispielsweise die Tabelle „Aufgabe“ [task] aus und aktivieren Sie die Kaskadierung. In diesem Fall gilt die Datenfilterungsregel auch für alle Tabellen, die aus der Aufgabe erweitert wurden, z. B. Incident [Incident] und Change-Anforderung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	[change_request]. Weitere Informationen zur Tabellenerweiterung finden Sie unter Tabellenerweiterung und Klassen **Hinweis:** Dieses Feld ist standardmäßig aktiviert.

4. Wählen Sie im Formularmenü **Speichern** aus.
   Nachdem Sie Ihre Datenfilterregel gespeichert haben, gilt diese Regel automatisch für alle Datensätze in der ausgewählten Tabelle. Sie können den Umfang dieser Regel auf bestimmte Datensätze in der Tabelle beschränken, indem Sie Bedingungen auf den Registerkarten **„Datenfilter“** und **„Betreffbedingung** “ verwenden.

Fügen Sie einen Datenfilter für Ihre Datenfilterregel hinzu

Sie können optional einen Datenfilter verwenden, um den Umfang Ihrer Datenfilterungsregel so einzugrenzen, dass sie nur auf bestimmte Datensätze in einer Tabelle angewendet wird.

Vorbereitungen

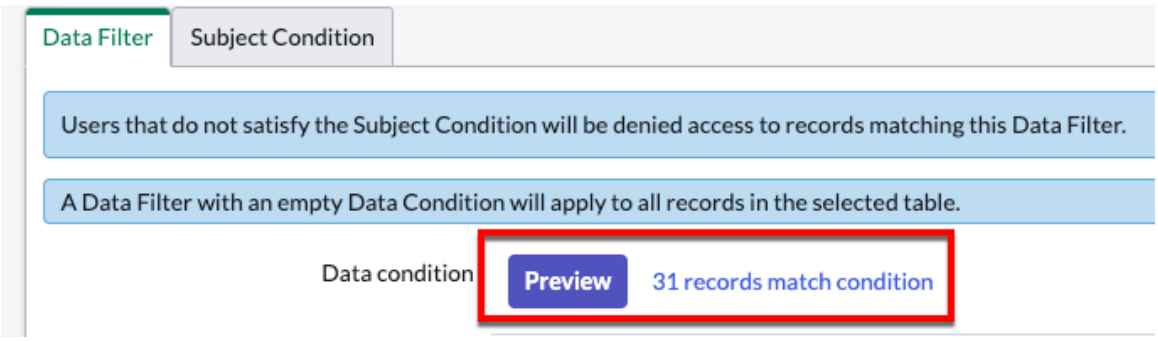
Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie in Ihrem Datenfilterungsdatensatz die Registerkarte **Datenfilter**.
2. Verwenden Sie den Bedingungsgenerator, um die Tabellendatensätze nach ihren Feldwerten zu filtern.
   Der Datenfilter verwendet denselben Bedingungsgenerator, der in anderen Teilen der Plattform verwendet wird. Weitere Informationen zur Verwendung dieser Schnittstelle finden Sie unter Bedingungsgenerator .

   Wichtig:
   Die Registerkarte **Datenfilter** wird leer angezeigt, bis Sie eine Tabelle im Feld **Tabelle** auswählen.

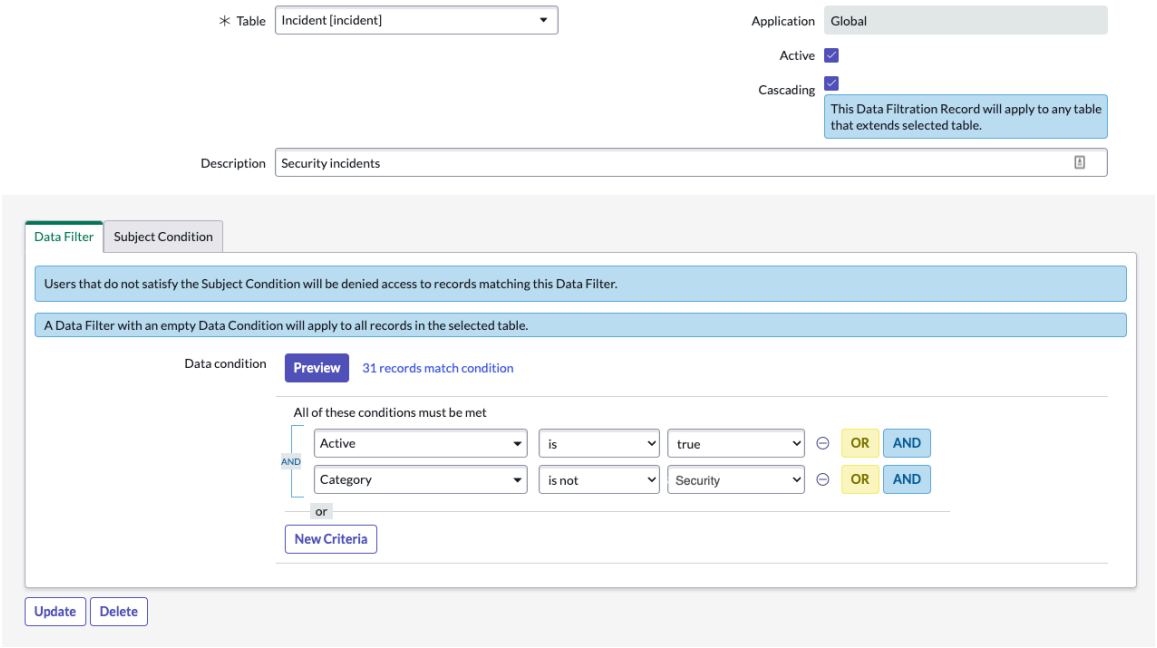
3. Verwenden Sie die Schaltfläche **Vorschau**, um anzuzeigen, wie viele Datensätze Ihrem Datenfilter entsprechen.
4. Wählen Sie die Anzahl der Datensätze aus, um eine Liste der übereinstimmenden Datensätze zu öffnen.



5. Wählen Sie **Speichern**.

Example:
Dieses Beispiel zeigt eine Datenfilterungsregel für die Incident-Tabelle [Incident]. Der Datenfilter ist so eingestellt, dass alle aktiven Datensätze ausgewählt werden, die sich nicht in der **Sicherheitskategorie** befinden. Wenn diese Regel aktiv ist, können Benutzer diese Datensätze anzeigen. Weitere Informationen zur Verwendung von Kriterien außerhalb des Datensatzinhalts finden Sie im folgenden Abschnitt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wichtig:

Der **Not** -Vorgang in Ihren Bedingungen kann abhängig vom Typ der von Ihrer Instanz verwendeten Datenbank zu unerwarteten Ergebnissen führen. Nehmen Sie zum Beispiel die folgende Bedingung:

Für diese Bedingung wäre das erwartete Ergebnis, dass die Ergebnismenge aus allen Datensätzen besteht, bei denen das Unternehmen nicht ServiceNow ist, und aus allen Datensätzen, die keinen Wert im Feld **„Unternehmen“** enthalten. Instanzen, die andere Datenbanken als MySQL und Maria verwenden, geben keine Wertedatensätze mit einem leeren **Unternehmensfeld** zurück. Wenn Sie für diese Instanzen **keine** Abfragen verwenden, schließen Sie Bedingungen ein, um sicherzustellen, dass leere Werte zurückgegeben werden.

Fügen Sie Ihrer Datenfilterungsregel Betreffattribute hinzu

Verwenden Sie optional Betreffattribute, um den Umfang Ihrer Datenfilterungsregel basierend auf Attributen wie IP-Netzwerkadresse, Benutzergruppen und Rollen oder Betreffkriterien einzugrenzen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie in Ihrem Datenfilterungsdatensatz die Registerkarte **Betreffkriterien** .
2. Verwenden Sie den Bedingungsgenerator, um die Tabellendatensätze basierend auf einem oder mehreren der folgenden Kriterien zu filtern.

Optionen für Betreffkriterien

Option	Beschreibung
Netzwerkkriterien	Ermöglicht den Zugriff auf Datensätze basierend auf dem Netzwerk-IP-Bereich oder IP-Subnetz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Betreffkriterien	Ermöglicht den Zugriff auf Datensätze basierend auf Betreffkriterien. Wählen Sie einen Betreffkriteriendatensatz aus, um seine Bedingungen auf Ihre Datenfilterungsregel anzuwenden. Weitere Informationen zum Erstellen von Betreffkriteriendatensätzen finden Sie unter Betreffkriterien werden erstellt.
Betreffgruppe	Gewähren Sie den Zugriff, wenn der Benutzer Mitglied einer bestimmten Gruppe ist. Wählen Sie eine Gruppe aus der Gruppentabelle [**sys_user_group**] aus.
Betreffrolle	Gewähren Sie den Zugriff, wenn der Benutzer Mitglied einer bestimmten Gruppe ist. Wählen Sie eine Gruppe aus der Rollentabelle [**sys_user_role**] aus.

Wichtig:
Betreffkriterienbedingungen unterstützen nur den Operator „ **ist** “.

3. Klicken Sie nach dem Hinzufügen der Betreffkriterien auf **Speichern**.

Betreffkriterien werden erstellt

Erstellen Sie Betreffkriteriendatensätze zur Verwendung in Datenfilterungsregeln.

Vorbereitungen

Erforderliche Rolle: security_admin

Wichtig:
Um Datenfilterungsregeln zu erstellen oder zu ändern, müssen Sie eine Erhöhung auf eine privilegierte Rolle durchführen. Weitere Informationen zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle erhöhen.

Prozedur

1. Navigieren zu **Alle** > **Datenfilterung** > **Betreffkriterien**.
2. **Klicken** Sie in der Liste „Antragstellerkriterien“ auf die Schaltfläche **Neu**.
   Ein neues Formular für Betreffkriterien wird angezeigt.
3. Füllen Sie die Felder im Formular nach Bedarf aus.

Felder für Betreffkriterien

Feld	Beschreibung
Name	Name für die Betreffkriterien.
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung ausgefüllt.
Beschreibung	Beschreibung für die Betreffkriterien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie mit der rechten Maustaste auf die Formularkopfzeile, und klicken Sie im Kontextmenü auf **Speichern**.
   Nach dem Speichern werden die Felder **Kriterieneingaben** und **Kriterienbedingungen angezeigt**.

Erstellen Sie eine Betreffkriterieneingabe

Erstellen Sie eine Eingabe für Betreffkriterien, um Kriterien zu definieren, nach denen Ihre Datenfilterungsregeln filtern.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Öffnen Sie in Ihrem **Betreffkriteriendatensatz die Registerkarte Kriterieneingaben**.
2. Klicken Sie in der Liste **„Kriterieneingaben“** auf **Neu**.
3. Wählen Sie die Richtlinieneingabe für die Kriterien aus, die Sie erstellen möchten.

Richtlinieneingaben

Richtlinieneingabe	Beschreibung
IP-Filterkriterien	Erstellen Sie eine Richtlinieneingabe basierend auf der IP-Adresse
Rollenfilterkriterien	Erstellen Sie eine Richtlinieneingabe basierend auf der Benutzerrolle
Gruppenfilterkriterien	Erstellen Sie eine Richtlinieneingabe basierend auf der Benutzergruppe

   Abhängig von Ihrer Auswahl in diesem Schritt wird ein Formular für **IP-Filterkriterien**, **Rollenfilterkriterien**oder **Gruppenfilterkriterien** angezeigt.

4. Füllen Sie im Formular „Filterkriterien“ die Felder nach Bedarf aus.

Filterkriterienfelder

Feld	Beschreibung
Name	Name für die Filterkriterien
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung ausgefüllt.
Beschreibung	Beschreibung der Filterkriterien

5. Unterhalb der Formularfelder befinden sich Registerkarten, auf denen die IP-Adressen, Gruppen oder Rollen für die Filterkriterieneingaben definiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterkriterienfelder für bestimmte Eingabetypen

Eingabetyp der Richtlinie	Beschreibung	Erstellung
IP-Filterkriterien	Benutzer-IP-Filterkriterien zum Erstellen eines Bereichs oder Subnetzes von IP-Adressen. Ihre Betreffkriterien können dann mit der IP-Adresse des Benutzers mit diesem Bereich oder Subnetz verglichen werden.	Verwenden Sie den **IP** -Bereich oder das **Subnetz (CIDR)**, um IP-Adressen für Ihre Eingabe zu definieren. **IP-Bereich** Doppelklicken Sie in der Liste „ **IP** -Bereiche“ auf **Neue Zeile einfügen**, und geben Sie im Feld **Start-IP**eine IP-Startadresse ein. Drücken Sie dann die Tabulatortaste, und geben Sie im Feld **End-IP** eine IP-Endadresse ein. Drücken Sie abschließend die Eingabetaste, um den Listeneintrag zu speichern. **Subnetz (CIDR)** **Doppelklicken** Sie in der Liste „Subnetze“ auf **Neue Zeile**einfügen, und geben Sie im Feld Netzwerk-IP eine Netzwerk-**IP** ein. Drücken Sie dann die Tabulatortaste, und geben Sie eine Netzmaske in das Feld **Netzmaske** ein. Drücken Sie abschließend die Eingabetaste, um den Listeneintrag zu speichern. **Hinweis:** Geplante Aufgaben, die von einem Planer ausgelöst werden, sollen Daten nicht anhand eines Netzwerkkriteriums filtern, da sie nicht den Kontext der anfordernden Client-IP haben. Eine geeignetere Art der Filterung kann die Bedingung für Rollen-/Gruppenbetreff sein.
Rollenfilterkriterien	Verwenden Sie Rollenfilterkriterien, um eine Auswahl von Rollen zu erstellen. Ihre Betreffkriterien können dann mit den zugewiesenen Rollen des Benutzers für diese Auswahl verglichen werden.	Verwenden Sie den Bedingungsgenerator im **Feld Bedingung**, um Rollen für Ihre Eingabe auszuwählen.
Gruppenfilterkriterien	Verwenden Sie Gruppenfilterkriterien, um eine Auswahl von Benutzergruppen zu erstellen. Ihre Betreffkriterien können dann mit den zugewiesenen Gruppen des	Doppelklicken Sie in der Tabelle „ **Gruppen für Kriterien** “ auf **Neue Zeile einfügen**und wählen Sie eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabetyp der Richtlinie	Beschreibung	Erstellung
	Benutzers für diese Auswahl verglichen werden.	Benutzergruppe aus. Drücken Sie die Eingabetaste, oder klicken Sie auf das grüne Häkchensymbol, um die Gruppe zu speichern. Klicken Sie unter dem ersten Eintrag auf den Text **Neue Zeile einfügen**, um weitere Einträge zu erstellen.

6. Klicken Sie nach der Definition Ihrer Eingabe auf **Absenden**.

Hinweis:
Sie können nicht nur Kriterieneingaben für Ihre Betreffkriterien erstellen, sondern auch vorhandene hinzufügen. Klicken Sie auf der Registerkarte **„Kriterieneingaben“** auf **Bearbeiten**, und wählen Sie eine vorhandene Eingabe aus.

Erstellen Sie eine Bedingung für Betreffkriterien

Erstellen Sie eine Bedingung, um Benutzerinformationen mit vorhandenen Eingaben für Betreffkriterien zu vergleichen.

Vorbereitungen

Erforderliche Rolle: security_admin

Kriterienbedingungen vergleichen Benutzerattribute mit vorhandenen Kriterieneingaben, um zu bestimmen, ob der Zugriff auf Datensätze zulässig ist. Um eine Kriterienbedingung zu erstellen, müssen Sie Betreffkriterien erstellt haben. Weitere Informationen zu diesem Prozess finden Sie unter, Erstellen Sie eine Betreffkriterieneingabe.

Prozedur

1. Öffnen Sie in Ihrem **Betreffkriteriendatensatz die Registerkarte Kriterienbedingungen**.
2. Klicken Sie in der Liste „ **Kriterienbedingungen“** auf **Neu**.
3. Füllen Sie im Formular **„Betreffkriterienbedingung“** die Felder nach Bedarf aus.

Formular „Bedingung für Betreffkriterien“

Feld	Beschreibung
Bezeichnung	Eine beschreibende Bezeichnung für Ihre Bedingung
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung ausgefüllt.

4. Erstellen Sie mithilfe des Bedingungsgenerators eine Bedingung für Ihre Betreffkriterienbedingung, indem Sie eine der folgenden Bedingungsoptionen auswählen.
   Diese Bedingungsoptionen umfassen alle von Ihnen erstellten Eingaben für Betreffkriterien.
5. **Wahlweise:** Erstellen Sie weitere Bedingungen, indem Sie auf die Schaltflächen **Filterbedingung hinzufügen** oder **„ODER“-Klausel** hinzufügen klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sofern Ihre Bedingungen nicht durch eine Klausel **oder** getrennt sind, müssen alle Bedingungen als „wahr“ ausgewertet werden, damit die Bedingung der Betreffkriterien als „wahr“ ausgewertet wird.

6. Klicken Sie auf Absenden, um die Bedingung der **Betreffkriterien** zu speichern.

Nächste Maßnahme
Verwenden Sie Betreffkriterien in Ihren Datenfilterungsregeln, um den Zugriff auf Tabellen und Datensätze zu beschränken. Weitere Informationen zur Verwendung von Betreffkriterien in Datenfilterungsregeln finden Sie unter Betreffkriterien werden erstellt.

Debugging von Datenfilterung

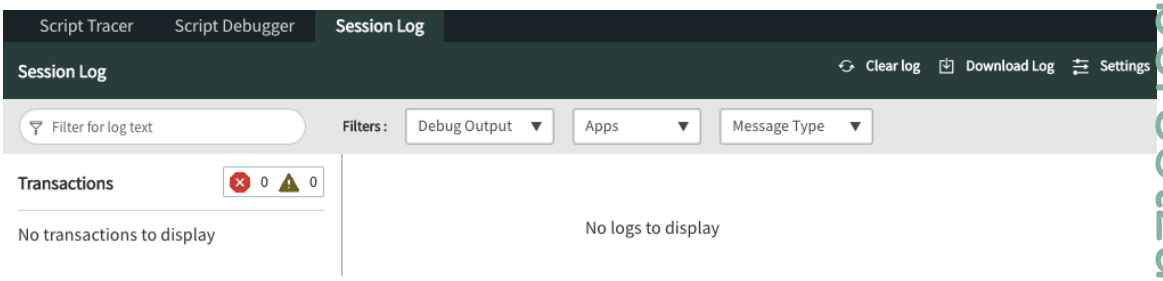
Verwenden Sie das Sitzungsprotokoll, um zu sehen, wie sich die Datenfilterung auf Ihre Datensätze auswirkt, und um Benutzerzugriffsprobleme zu debuggen.

Vorbereitungen
Erforderliche Rolle: admin

Ausgabeinformationen werden in den Sitzungsprotokollen angezeigt, wenn Benutzer auf Datensätze zugreifen. Sie können diese Protokollierungsinformationen zusammen mit Identitätswechsel verwenden, um zu erfahren, warum Benutzer Datensätze sehen oder nicht. Sie können diese Informationen dann verwenden, um Ihre Datenfilterungsregeln anzupassen und sicherzustellen, dass Benutzer nur das sehen, was Sie beabsichtigen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Debugging** > **Alle Sicherheitseinstellungen debuggen**.
   Der **Skript-Debugger** wird in einer neuen Browserregisterkarte oder in einem neuen Fenster geöffnet.



2. Wählen Sie im Fenster **„Skript-Debugger** “ die Registerkarte **Sitzungsprotokoll** aus.
3. Nehmen Sie auf einer anderen Browserregisterkarte oder in einem anderen Fenster die Identität eines Benutzers an, um Probleme mit dem Zugriff dieses Benutzers zu beheben.

Hinweis:
Identitätswechsel ermöglicht es einem Administrator, eine Instanz mit den Einstellungen eines anderen Benutzers anzuzeigen und darauf zuzugreifen. Weitere Informationen zum Identitätswechsel finden Sie unter Identität eines Benutzers annehmen .

4. Greifen Sie beim Annehmen der Identität eines Benutzers auf eine Liste oder einen Datensatz zu, in der/dem Sie unerwartetes Verhalten feststellen.
   Dieses Verhalten kann ein Datensatz sein, den der Benutzer sieht, aber nicht sehen sollte, oder eine Liste von Datensätzen, die für einen Benutzer nicht wie erwartet angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach dem Zugriff auf Datensätze mit dem Benutzer, dessen Identität Sie annehmen, sollten Sie die Ausgabe im Sitzungsdebugger sehen.

5. Suchen Sie im Sitzungs-Debugger nach Informationen zur Datenfilterung.

Dieses Beispiel zeigt zwei Protokollnachrichten, bei denen ein Datenfilter den Zugriff auf Datensätze verweigert. Die Protokolleinträge werden als roter Text angezeigt und enthalten den Grund für die Verweigerung des Zugriffs durch den Datenfilter sowie die sys_id des Datenfilters. Sie können auf diese sys_id klicken, um den Datenfilterungsdatensatz zu öffnen.

Dieses Beispiel zeigt eine Protokollnachricht, bei der ein Datenfilter den Zugriff auf einen Datensatz erlaubt hat. Diese Protokolleinträge werden als grüner Text angezeigt. Wie bei der ersten Nachricht können Sie auf diese sys_id klicken, um den Datenfilterungsdatensatz zu öffnen.

6. Verwenden Sie diese Informationen, um Anpassungen an Ihren Datenfilterregeln vorzunehmen. Wiederholen Sie diese Schritte, um Ihre Regeln zu verfeinern und Benutzern den erforderlichen Zugriff zu gewähren.

Datenschutz

Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren. Nachdem sie anonymisiert wurden, gelten sie nicht mehr als persönliche Daten, die Vorschriften unterliegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie Data Privacy

Erfahren Sie mehr über Datenschutz.

Konfigurieren Sie Data Privacy

Erfahren Sie, wie Sie Data Privacy konfigurieren.

Rollen in Data Privacy

Rufen Sie Details zu Rollen in Data Privacy ab.

Erweiterte Datenschutzfunktionen

Erfahren Sie mehr über die erweiterten Funktionen von Data Privacy.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz erkunden

Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren. Nachdem sie anonymisiert wurden, gelten sie nicht mehr als persönliche Daten, die Vorschriften unterliegen.

Erklärt die Bedeutung des Datenschutzes und die Schritte, die Unternehmen unternehmen können, um vertrauliche Informationen durch Klassifizierung und Anonymisierung zu schützen. Mit der Store-Anwendung Data Privacy geben wir einen Überblick über das Haupt-Dashboard und die Funktionen.

Entwickler müssen mit Daten in Nicht-Produktionsinstanzen arbeiten, um sicherzustellen, dass ihre Implementierungen wie erwartet funktionieren. Der Import von Daten aus Ihrer Produktionsinstanz ist zwar eine nützliche Methode zur Simulation der Produktion, stellt jedoch ein Sicherheitsrisiko dar. Administratoren können Datenschutz verwenden, um Entwicklern Daten bereitzustellen, die keine privaten Informationen enthalten, damit sie in einer Nicht-Produktionsumgebung sicher arbeiten können.

Datenklassifizierung

Identifizieren und klassifizieren Sie Ihre vertraulichen Daten anhand vordefinierter Kriterien, die vom Vertraulichkeitsgrad der Datentypen in Ihrer Instanz bestimmt werden. Datenvertraulichkeitsstufen bestimmen, wie jeder Typ klassifizierter Daten behandelt werden soll. Es gibt mehrere vordefinierte Klassen, die mit Datenschutz auf Basisebene bereitgestellt werden. Verwenden Sie den Klassifizierungsabschnitt von Data Privacy, um Daten in Ihrer Instanz zu kennzeichnen und zu gruppieren. Fügen Sie Klassen hinzu, zeigen Sie die Datenklassenstruktur an, und klassifizieren Sie Daten. Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ.

Erklärt, wie Daten mit der Store-Anwendung Data Privacy klassifiziert werden.

Anonymisierung von Benutzerdaten

Als Administrator legen Sie fest, ob alle Informationen für alle Benutzer oder für eine Teilmenge von Benutzern anonymisiert werden sollen. Nach der Anonymisierung werden die Daten für die ausgewählten Benutzerdatensätze durch zufällige oder von Ihnen definierte Werte ersetzt. Beim Ersetzen von Werten kann die Datenstruktur mit verschiedenen Techniken beibehalten werden.

Erklärt, wie Daten mit der Store-Anwendung Data Privacy anonymisiert werden.

Datenschutzoptionen

- Datenschutz (klassisch): Verwenden Sie zuerst die Datenklassifizierungs-App, um Ihre Daten nach Typ zu gruppieren, indem Sie vordefinierte oder benutzerdefinierte Datenklassifizierungen verwenden. Erstellen Sie dann Datenschutztechniken und -aufgaben, um personenbezogene Daten zu anonymisieren.
- Datenschutz (Store-App): Klassifizieren und anonymisieren Sie Ihre Daten in der Datenschutz-App.

Überlegungen

- Nur klassifizierte Daten können anonymisiert werden. Weitere Informationen zu Datenklassen und Klassifizierungen finden Sie unter Datenklassifizierung (klassisch) oder in der Store-App Datenklassifizierung.
- PII in Protokollen und andere Audit-Daten werden nicht anonymisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nur strukturierte Daten können anonymisiert werden. Unstrukturierte Daten wie Journalfelder, Kommentare, Anhänge und andere Felder, in denen Teiltext personenbezogene Daten darstellen kann, werden nicht anonymisiert. Weitere Informationen finden Sie unter Unterstützte Feldtypen für die Anonymisierung.
- Bei Integrationen mit SSO-Systemen (Single Sign-on) werden Benutzerinformationen möglicherweise aus ihren Source-of-Truth-Systemen neu synchronisiert. Es gibt keinen Mechanismus, um die dauerhafte Deidentifizierung von sys_user-Daten sicherzustellen. Weitere Informationen zur Benutzeradministration und zu sys_users finden Sie unter Benutzeradministration .

Domänentrennung und Datenschutz

Domänentrennung wird aus Datenschutzgründennicht unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

Zugehörige Informationen

Domänentrennung für Service Provider

Unterstützte Feldtypen für die Anonymisierung

Überprüfen Sie, welche Feldtypen beim Anonymisieren von Daten unterstützt werden.

Hinweis:
Nicht alle klassifizierten Feldtypen sind für die Anonymisierung verfügbar.

Einige Feldtypen mit hohem Risiko sind standardmäßig deaktiviert (siehe Tabelle). Weitere Informationen zu Feldern finden Sie unter Feldtypen .

Unterstützte Feldtypen für die Anonymisierung

Feldtyp	Standardmäßig verfügbar
Audio	Nein
Bedingung	Nein
Bedingungszeichenfolge	Nein
currency	Ja
Dezimalzahl	Ja
due_date	Ja
schweben	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldtyp	Standardmäßig verfügbar
glide_date	Ja
glide_date_time	Ja
glide_duration	Nein
glide_time	Ja
html	Nein
icon	Nein
integer	Ja
ip_addr	Nein
ip_address	Nein
Journal	Nein
journal_input	Nein
journal_list	Nein
longint	Ja
name_values	Nein
percent_complete	Nein
phone_number_e164	Ja
price	Ja
Zeichenfolge	Ja
string_full_utf8	Ja
übersetzen_html	Nein
translate_text	Nein
URL	Nein
user_image	Nein
Video	Nein
wiki_text	Nein

Datenschutzrollen

Data Privacy fügt diese Rollen hinzu.

Rollenbeschreibung

Rollentitel [Name]

Name der Rolle. Text in Klammern entspricht dem Feld **Name** in der Rollentabelle [sys_user_role].

Beschreibung

Beschreibung der Rolle und ihres Verwendungszwecks.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Abonnement

Gibt an, ob die Rolle eine kostenpflichtige Benutzerrolle ist, die die Zuteilung von Benutzern mit dieser Rolle zu Abonnements erfordert.

Erweitert

Gibt an, ob die Rolle eine erhöhte Rolle ist. Erweiterte Rollen werden keinen Benutzern oder Gruppen zugewiesen und müssen durch Erhöhung verwendet werden. Weitere Informationen finden Sie unter Auf eine privilegierte Rolle hochstufen.

Überlegungen

Warnungen oder andere Überlegungen für Administratoren.

Hinweis:

Vereinfachen Sie die Benutzerverwaltung, indem Sie Rollen eher Gruppen als einzelnen Benutzern zuweisen. Erstellen Sie Gruppen, die alle für bestimmte Personas erforderlichen Rollen enthalten, und weisen Sie diesen Gruppen Benutzer zu. Wenn Benutzer zu neuen Rollen wechseln, können Sie Gruppen neu zuweisen und Szenarien vermeiden, in denen Benutzer unerwartete Rollen beibehalten.

Weitere Informationen zur Verwaltung von Benutzern, Gruppen und Rollen finden Sie unter Benutzeradministration.

Datenschutzadministrator

Die Datenschutzadministratorrolle ist eine Administratorrolle, die zum Erstellen von Datenschutztechniken und -richtlinien verwendet wird.

Datenschutzadministrator [data_privacy_admin]

Enthält Rollen

Keine

Zu Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Nein

Überlegungen

Vermeiden Sie es, Benutzern diese Rolle zuzuweisen, wenn gezieltere Rollen verfügbar sind.

Datenschutz-Auditor

Der Datenschutzprüfer ist eine schreibgeschützte Rolle, die zum Anzeigen von Datenschutzdatensätzen verwendet wird.

Datenschutzprüfer [data_privacy_auditor]

Enthält Rollen

Keine

Zu Gruppen zugewiesen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Keine

Abonnement

Nein

Erweitert

Nein

Überlegungen

Keine

Datenschutz-Klonprozessor

Benutzer mit der Rolle „Datenschutz-Klonprozessor“ können Datenklassen-Datenschutzaufträge erstellen und ausführen.

Datenschutz-Klonprozessor [data_privacy_clone_processor]

Enthält Rollen

Keine

Zu Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Keine

Datenschutzbeauftragter

Benutzer mit der Rolle „Datenschutzbearbeiter“ erstellen Datenschutzaufträge in der Benutzertabelle [sys_user] und führen sie aus.

Datenschutzbearbeiter [data_privacy_processor]

Enthält Rollen

Keine

Zu Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Keine

Datenschutz (klassisch)

Data Privacy (Classic) ist als Familien-Release verfügbar. Die letzten Familien-Updates wurden beim Tokyo-Release veröffentlicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz aktivieren (klassisch)

Sie können das Datenschutz-Plugin (com.glide.data_privacy) für Platform Security aktivieren, wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und installiert zugehörige ServiceNow® Store Anwendungen und Plugins, sofern sie nicht bereits installiert sind.

Vorbereitungen

Datenschutz erfordert ein vom Rest der Now Platformgetrenntes Abonnement.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste „Alle Anwendungen“ in Ihrer Instanz aktivieren.

Hinweis:

Bevor Sie ein Abonnement kaufen, können Sie die Funktion in einer Instanz außerhalb der Produktion kostenlos testen, indem Sie sie über den Now Support Servicekatalog anfordern.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Data Privacy installiert:

- Plugins
- Rollen
- Tabellen

Weitere Informationen finden Sie unter Mit Data Privacy (klassisch) installiert.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Data Privacy“ (com.glide.data_privacy).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:

Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Mit Data Privacy (klassisch) installiert

Erfahren Sie mehr über die mit dem Plugin „Data Privacy“ (com.glide.data_privacy) installierten Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Tabellen

Tabelle	Beschreibung
Datenschutz-Verbundauftrag [dp_federated_job]	Verbundaufgaben für Datenschutz
Datenschutzauftrag [dp_job]	Datenschutzaufträge
Datenschutzauftrag [dp_job_summary]	Zusammenfassungen der Datenschutzaufgabe
Datenschutztechnik [dp_technik]	Datenschutztechniken
Primärer Referenzlink [dp_primary_reference]	Primäre Referenzlinks
Technik für klassifiziertes Datenschutzfeld [dp_field_technique]	Klassifizierte Feldtechniken für Datenschutz
Datenschutzkonfiguration [dp_configuration]	Datenschutzkonfigurationen
Konfiguration der Datenschutztechnik [dp_technique_with_params]	Datenschutztechniken
Parameter für Datenschutztechnik [dp_technique_with_parameter]	Datenschutztechniken mit Parametern
Parameterwert für Datenschutztechnik [dp_technique_with_parameter_value]	Parameterwerte, die in Datenschutztechniken mit Parametern verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration des Datenschutzes (klassisch).

Erfahren Sie, wie Sie Datenschutztechniken und -richtlinien erstellen und wie Sie Datenschutzaufträge erstellen und ausführen.

Datenschutztechniken

Datenschutztechniken sind Optionen, die Sie auswählen, um festzulegen, wie Ihre Daten anonymisiert werden. Sie müssen eine Datenschutztechnik erstellen, auf die in der Datenschutzaufgabe verwiesen werden soll. Informationen zum Zuordnen einer Datenschutztechnik zu einer zugehörigen **Konfiguration der Datenschutztechnik finden**Sie unter Erstellen Sie eine Konfiguration für Datenschutztechnik.

Datenschutzrichtlinien

Konfigurieren Sie eine Datenschutzrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden. Details siehe Erstellen Sie eine Datenschutzrichtlinie.

Datenschutzaufträge

Datenschutzaufgaben verwenden alle diese Komponenten, um Ihre Daten zu anonymisieren. Weitere Informationen zu diesen Aufgaben finden Sie unter Konfigurieren Sie einen Datenschutzauftrag.

Erstellen Sie eine Konfiguration für Datenschutztechnik

Erstellen Sie eine Datenschutztechnikkonfiguration, um anzupassen, wie der Datenschutz Ihre Daten anonymisiert.

Vorbereitungen
Erforderliche Rolle: data_privacy_admin und admin

Prozedur

1. Erhöhen Sie auf die Rolle **data_privacy_admin**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Konfiguration der Datenschutztechnik**.
3. Klicken Sie auf **Neu**.
4. Geben Sie im Feld **Name** einen Namen für die Konfiguration der Datenschutztechnik ein.
5. **Wählen** Sie im Feld Datenschutztechnik eine Datenschutztechnik aus.

Datenschutztechniken

Technik	Beschreibung
Keine Aktion	Diese Technik ist ein Platzhalter. Bei Auswahl werden keine Felder geändert.
Zufälliges Ersetzen	Diese Technik tauscht Werte mit zufällig generierten Werten aus. Zeichenfolgen- und Zahlendaten können diese Technik verwenden.
Wählen Sie Ersetzen aus	Diese Technik führt eine selektive Ersetzung von Zeichenfolgendaten durch. Alle Zeichen zwischen den Start- und Endindizes der Eingabe werden durch das ausgewählte Zeichen ersetzt. Sie können Zeichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Technik	Beschreibung
	angeben, die von der Maskierung ausgeschlossen werden sollen: ○ start_index: Technik maskiert Daten ab dem angegebenen Zeichen. Wenn das Feld leer gelassen wird, beginnt die Maskierung mit dem ersten Zeichen. ○ end_index: Die Technik maskiert Daten vom Anfang der Zeichenfolge bis zum angegebenen Zeichen. Wenn das Feld leer gelassen wird, endet die Maskierung mit dem letzten Zeichen. ○ exclude_char: Definieren Sie ein Zeichen, das von der Maskierung ausgeschlossen werden soll. ○ ersatz_char: Definieren Sie ein Zeichen, das für die Maskierung verwendet wird. Wenn keines angegeben ist, werden standardmäßig Sternchen (*) verwendet.
Statisches Ersetzen	Diese Technik tauscht Werte mit statischen Werten aus. Zeichenfolgen-, Zahlen- und Datumsdaten können diese Technik verwenden: ○ date_time_value: Datumswerte durch dieses Datum ersetzen. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss. ○ date_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt. ○ number_value: Ersetzen Sie Zahlenwerte durch diese Zahl. ○ string_value: Ersetzen Sie Zeichenfolgenwerte durch diesen Text.
Entfernen	Diese Technik entfernt Werte und ersetzt sie durch leere Werte (Null).

Hinweis:
Der zuvor unterstützte Wert „ **Ersetzen** “ ist veraltet und wurde in „ **Ersetzen – Veraltet** “ umbenannt. Er sollte nicht verwendet werden.

6. Klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie im Kontextmenü auf **Speichern**. Nachdem der Datensatz gespeichert wurde, wird die Liste **Parametrisierte Datenschutzwerte** angezeigt.
7. Verwenden Sie die Datensätze in der Liste **„Parameterisierte** Datenschutzwerte“, um die Konfiguration der Datenschutztechnik anzupassen.
   Die verfügbaren parametrisierten Werte hängen von der von Ihnen ausgewählten Datenschutztechnik ab. Es gibt keine parametrisierten Werte für die Techniken **„Keine Aktion“** und „ **Entfernen** “.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametrisierte Datenschutzwerte für selektives Ersetzen

Wert des Parameters für Datenschutztechnik	Beschreibung	Standardwert
char_to_replace	Zeichen, das beim Ersetzen von Werten durch selektives Ersetzen verwendet werden soll.	*
end_index	Die Technik maskiert Daten vom Anfang der Zeichenfolge bis zum angegebenen Zeichen. Wenn leer gelassen, endet die Maskierung mit dem letzten Zeichen.	(leer)
exclude_char	Zeichen zum Überspringen der Maskierung. In diesem Wert kann nur ein einzelnes Zeichen verwendet werden. Wenn mehrere eingegeben werden, wird das erste Zeichen verwendet.	(leer)
start_index	Die Technik maskiert Daten ab dem angegebenen Zeichen.	1

Parametrisierte Datenschutzwerte für Ersetzen

Wert des Parameters für Datenschutztechnik	Beschreibung	Standardwert
date_time_value	Ersetzen Sie Datums- und Uhrzeitwerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss.	1988-11-11 10:10:10
date_value	Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt.	1988-11-11
number_value	Ersetzen Sie Zahlenwerte durch diese Zahl.	1234567
erhalten_daten_länge	Setzen Sie diese Option auf „ **true** “, um die Datenlänge beizubehalten. Deidentifizierte Daten haben dieselbe Länge wie die ursprünglichen Daten.	Wahr
string_value	Ersetzen Sie Zeichenfolgenwerte durch diesen Text.	TEXT123
use_random_generated_value	Auf „ **true“** setzen, um Daten durch zufällig generierte Werte zu ersetzen. Nur Zeichenfolgen- und Zahlendaten können durch zufällige Werte ersetzt werden.	false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert des Parameters für Datenschutztechnik	Beschreibung	Standardwert
	Diese Option überschreibt statische Werte.	

8. Klicken Sie auf **Speichern**.

Erstellen Sie eine Datenschutzrichtlinie

Konfigurieren Sie eine Datenschutzrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden.

Vorbereitungen

Die Datenschutzkonfiguration definiert Tabellen, sys_user und andere sowie Spalten für die De-Identifizierung, abhängig vom Anwendungsfall, und gibt parametrisierte Typen der Techniken an, die bei der De-Identifizierung von Daten verwendet werden sollen.

Hinweis:
Um eine Datenschutzkonfiguration abzuschließen, müssen Sie zuerst eine Konfiguration für die Datenschutztechnik konfigurieren. Weitere Informationen finden Sie unter Erstellen Sie eine Konfiguration für Datenschutztechnik.

Erforderliche Rolle: data_privacy_admin und admin

Prozedur

1. Erhöhen Sie auf die Rolle **data_privacy_admin**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Systemsicherheit** > **Datenschutz (klassisch)** > **Konfiguration der Datenschutzrichtlinie**.
3. Wählen Sie **Neu**.
4. Geben Sie im Feld **Name** einen Namen für die Konfiguration der Datenschutzrichtlinie ein.
5. **Wählen** Sie im Feld Datenklasse die Datenklasse aus, die mit dieser Richtlinie verwendet werden soll.
   Datenschutzrichtlinien können nur für klassifizierte Daten gelten. Weitere Informationen zur Datenklassifizierung finden Sie unter Datenklassifizierung.
   Nach der Auswahl einer Datenklasse werden die Listen „ **Datenschutz – klassifizierte Feldtechniken“** und **„Links zu primären Datenschutzreferenzen“** im Formular angezeigt.
6. **Wahlweise:** Wählen **Sie Auf alle Daten in Klasse** anwenden aus, um die Anonymisierung auf alle Daten in der ausgewählten Datenklasse anzuwenden.
   Wenn Sie dieses Feld nicht auswählen, können die Benutzer Ihres Datenschutzverarbeiters auswählen, welche Benutzer beim Erstellen von Datenschutzaufträgen anonymisiert werden sollen. Wenn Sie dieses Feld auswählen, ist diese Option nicht verfügbar.
   - **Beim Klonen anwenden**: Diese Option wird verfügbar. Wenn diese Option ausgewählt ist, wird die Datenschutzkonfiguration während des Datenschutzklons ausgeführt.
   - **Anwendungsreihenfolge**: Eine Datenschutzaufgabe für die Postclone-Konfiguration mit einer höheren Anwendungsreihenfolge wird möglicherweise vor einer anderen Aufgabe mit einer niedrigeren Reihenfolge gestartet.

   Wichtig:
   Vermeiden Sie es, mehrere Datenschutzrichtlinien mit derselben Anwendungsreihenfolge zu erstellen, da die resultierende Verarbeitungsreihenfolge für diejenigen mit derselben Reihenfolge inkonsistent ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. **Wahlweise:** Wählen Sie **Supports Rollback** aus, um die Deanonymisierung der Daten aus einer Datenschutzaufgabe zu aktivieren.
   Weitere Informationen finden Sie unter Setzen Sie eine Datenschutzaufgabe zurück.
   Nachdem Sie beim Erstellen einer Datenschutzaufgabe die Option **Unterstützt Rollback** ausgewählt haben, wird die Option zum Zurücksetzen der Aufgabe verfügbar.
8. Wechseln Sie zur Registerkarte **„Techniken** des klassifizierten Datenschutzfelds“, um die Liste **„Techniken des klassifizierten Datenschutzfelds** “ anzuzeigen.
9. Wählen Sie einen Eintrag im Feld **Tabelle** aus, um das Feld **Konfiguration der Datenschutztechnik** für jeden Listeneintrag zu öffnen.
   In der Liste „ **Techniken für klassifiziertes Datenschutzfeld** “ werden alle Daten angezeigt, die in der ausgewählten Datenklasse anonymisiert werden sollen. Für jeden dieser Einträge müssen Sie eine anzuwendende Datenschutztechnik auswählen.
10. Wählen Sie eine anzuwendende **Datenschutztechnikkonfiguration** aus.

> **Wichtig:**
> Wenn Sie einen Eintrag nicht anonymisieren, wählen Sie die **DoNoting-** Technik aus, anstatt den Eintrag leer zu lassen. Richtlinien mit leeren Werten im Feld **„Konfiguration der Datenschutztechnik“** können nicht ausgeführt werden, wenn sie in Datenschutzaufgaben verwendet werden.

11. Wählen Sie **Absenden** oder **Speichern**, um den Datensatz zu speichern.

Nächste Maßnahme

Konfigurieren Sie einen Datenschutzauftrag.

Konfigurieren Sie einen Datenschutzauftrag

Konfigurieren Sie einen Datenschutzauftrag in Ihrer Produktionsinstanz, um anonymisierte Daten in Ihrer Nicht-Produktionsinstanz für Benutzer- und Datenklassenaufträge zu verwenden.

Vorbereitungen

Die Datenschutzaufgabe unterstützt zwei Anwendungsfälle der Deidentifizierung:

- Vertrauliche Daten bestimmter sys_users
- Vertrauliche Daten einer bestimmten Datenklasse.

Erforderliche Rolle: data_privacy_processor und admin

Prozedur

1. Erhöhen Sie auf die Rolle **data_privacy_processor**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Datenschutzauftrag**.
3. Klicken Sie in der Liste „Datenschutzaufträge“ auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Felder für Datenschutzaufträge

Feld	Beschreibung
Name	Name des Jobs
Beschreibung	Beschreibung der Aufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Datenschutzkonfiguration	Die Konfiguration der Datenschutzrichtlinie, die für diesen Auftrag verwendet werden soll. Weitere Informationen zu Konfigurationen von Datenschutzrichtlinien finden Sie unter Erstellen Sie eine Datenschutzrichtlinie.
Benutzer	Wählen Sie die Anwender oder Anwendergruppen aus, die in diesem Auftrag anonymisiert werden sollen. Bis zu 1000 Benutzer einer Gruppe können verarbeitet werden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn die ausgewählte Datenschutzrichtlinienbedingung eine Auswahl von Benutzerdatensätzen erfordert.
Probelauf	Führen Sie die Aufgabe als Test aus. Bei Ausführung dieses Auftrags sind keine Datensätze betroffen. Die Ergebnisse werden im Feld **Zusammenfassung** so angezeigt, als ob die Aufgabe ausgeführt worden wäre. **Hinweis:** **Probelauf** muss deaktiviert sein, wenn ein Datenschutzauftrag mit Rollback konfiguriert wird. Details siehe Setzen Sie eine Datenschutzaufgabe zurück.
Status	Status der Datenschutzaufgabe: ○ **Bereit für Zeitplan**: Standardstatus für neue Aufträge. ○ **Rollback**wird ausgeführt: Der Auftrag wurde so festgelegt, dass ein Rollback der Anonymisierung durchgeführt wird. ○ **Rollback abgeschlossen**: Das Rollback des Anonymisierungsauftrags wurde erfolgreich abgeschlossen. Ein schreibgeschütztes Feld.
Geschätzte Anzahl der Datensätze	Die geschätzte Anzahl von Datensätzen, die sich dieser Job auswirkt. Ein schreibgeschütztes Feld.
Zusammenfassung	Ein schreibgeschütztes Feld, in dem die Ergebnisse der Aufgabe angezeigt werden, wenn Sie sie ausführen.
Zeitfensterstart	Der Beginn des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird nach der in diesem Feld eingegebenen Zeit ausgeführt. Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeitfensterende	Das Ende des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird vor der in diesem Feld eingegebenen Zeit ausgeführt. Wenn die Aufgabe noch nicht abgeschlossen ist, wird die Aufgabe angehalten und beim nächsten Start des Zeitfensters fortgesetzt. Die Endzeit muss nach der Startzeit liegen. Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.

5. Klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie im Kontextmenü die Option **Speichern** aus.
   Nach dem Speichern des Datensatzes werden die Schaltflächen **Aufgabe planen** und **Aufgabe löschen** angezeigt.
6. **Klicken** Sie auf Aufgabe planen, um die Aufgabe auszuführen.
   Die Aufgabe wird zwischen den in den Feldern **Start des Zeitfensters** und **Ende** des Zeitfensters ausgewählten Zeiten ausgeführt. Wenn die Aufgabe während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird die Aufgabe beim nächsten Start des Zeitfensters fortgesetzt.

   Hinweis:
   Ein Auftrag kann nur einmal ausgeführt werden, auch wenn **Probelauf** ausgewählt ist. Um dieselbe Aufgabe erneut auszuführen, erstellen Sie eine Datenschutzaufgabe mit denselben Feldwerten.

7. **Wahlweise:** Wählen Sie eine der folgenden Funktionen aus:
   - Auftrag**abbrechen**: Bricht den Datenschutzauftrag ab.
   - **Pause**: Hält den Auftrag an und setzt die Aufzeichnung zurück, wenn „Rollback“ ausgewählt wurde. Nach Ablauf von drei Tagen für Rollback-Kontexte wird eine Warnmeldung angezeigt. Details siehe Setzen Sie eine Datenschutzaufgabe zurück.
   - **Fortsetzen**: Startet einen angehaltenen Auftrag neu. Rollback wird für fortgesetzte Aufgaben nicht unterstützt, wenn sie angehalten sind. Brechen Sie die Aufgabe ab, und erstellen Sie eine Datenschutzaufgabe. Die Aufzeichnung verwendet einen nicht abgelaufenen Rollback-Kontext.

Rollback für Datenschutzauftrag

Datenbankänderungen werden für Aktionen wie Aufträge und Skripts erfasst, sodass die Änderungen zurückgesetzt werden können. Setzen Sie eine Datenschutzaufgabe zurück, wenn menschliches Versagen versehentlich falsche Benutzerinformationen anonymisiert. Durch das Rollback werden die Daten aus der Datenschutzaufgabe deanonymisiert.

Übersicht

- Das Rollback ist auf einige Tage pro konfigurierter Ablaufdauer des RollbackContext des neuen RollbackType *REDACT*beschränkt. Nach Ablauf des einer Datenschutzaufgabe zugeordneten RollbackContext ist die Rollback-Funktion für diese Aufgabe nicht mehr verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Rollback-Kontext aus der Deanonymisierung wird standardmäßig drei Tage lang gespeichert.
- Die Standardablaufzeit kann vom Datenschutzadministrator im **RollbackContext** des neuen **RollbackType** *REDACT.* auf einen Wert größer als eins festgelegt werden. Legen Sie den Wert in der Glide-Systemeigenschaft *glide.rollback.expiration_days_redact*fest. Siehe Rollback-Kontexte.

  Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

  für zusätzliche Informationen.

- Rollback ist für Datenschutzaufgaben verfügbar, die sich im Status „Abgeschlossen“, „Abgebrochen“ oder „Fehler“ befinden.
- Für jeden erfolgreichen sys_user-Deanonymisierungsauftrag, der mit einer Datenschutzrichtlinie mit aktivierter Rollback-Unterstützung konfiguriert ist, wird ein Rollback-Kontext erstellt. Pro Datenschutzaufgabe kann es höchstens einen Rollback-Kontext geben.

Setzen Sie eine Datenschutzaufgabe zurück

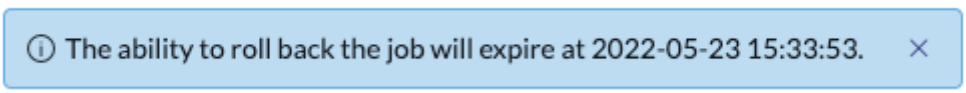
Setzen Sie einen Datenschutzauftrag in Ihrer Nicht-Produktionsinstanz, der anonymisierte Daten aus Ihrer Produktionsinstanz verwendet, auf einen Status vor der Deidentifizierung einer Datenklasse oder eines Benutzerauftrags zurück.

Vorbereitungen
Erforderliche Rolle: data_privacy_admin oder data_privacy_processor und admin

Prozedur

1. Erhöhen Sie auf die Rolle „ **data_privacy_processor“** oder **„data_privacy_admin“**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz** > **Datenschutzauftrag**.

   Hinweis:
   Im Voraus muss eine Konfiguration der Datenschutzrichtlinie erstellt werden, die das Rollback unterstützt. Erstellen Sie eine Datenschutzrichtlinie
3. Erstellen Sie eine Datenschutzaufgabe, und wählen Sie eine Datenschutzkonfiguration aus, die Rollback unterstützt.
   Weitere Informationen finden Sie unter Konfigurieren Sie einen Datenschutzauftrag.
4. Planen Sie die Aufgabe für die Datenanonymisierung.
   - Nach der Ausführung des Auftrags werden die Daten für die ausgewählte Konfiguration anonymisiert.
   - Im Job wird eine Nachricht angezeigt, die über die Ablaufzeit informiert. Innerhalb des Ablaufzeitraums haben Sie die Möglichkeit, den Auftrag zurückzusetzen.

5. Erhöhen Sie auf die Rolle **data_privacy_processor**.
6. Öffnen Sie die Datenschutzaufgabe, für die ein Rollback ausgeführt werden soll.
7. Wählen Sie **Rollback** aus, um die Daten zu deanonymisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutzklon

Beim Klonen von Kundendaten aus einer Quell- in eine Zielinstanz, in der Regel aus der Produktion in eine Instanz außerhalb der Produktion, werden vertrauliche Daten in der Zielinstanz deidentifiziert.

Ein Datenschutzadministrator konfiguriert Post-Clone-Richtlinien. Nachdem das Post-Klon-Skript in der Zielinstanz abgeschlossen ist, sehen die Benutzer deidentifizierte Daten und haben keinen Zugriff auf die ursprünglichen Daten. Datenschutzadministratoren können Deidentifizierungsrichtlinien konfigurieren, die beim Klonen auf die Zielinstanz angewendet werden, um sicherzustellen, dass die Zielinstanz keine ursprünglichen vertraulichen Daten enthält. Für die Richtlinie wird eine Reihenfolge im Verhältnis zu anderen auszuführenden Richtlinien angegeben.

Hinweis:
Das Klonen von Datenschutzdaten ist für selbst gehostete Instanzen verfügbar.

Der Datenschutzklon weist die folgenden zusätzlichen Attribute auf:

- Das Datenschutz-Plugin erstellt das Post-Klon-Skript, das auf der Zielinstanz ausgeführt werden soll.
- Für die PostClone-Konfiguration erstellte Datenschutzaufgaben können parallel ausgeführt werden, wenn sie nicht dieselben Tabellen betreffen
- Eine Datenschutzaufgabe für die Postclone-Konfiguration mit einer höheren Anwendungsreihenfolge wird möglicherweise vor einer anderen Aufgabe mit niedrigerer Reihenfolge gestartet, wenn die Aufgabe mit der höheren Reihenfolge keine Tabelle umfasst, die sich auf eine andere Aufgabe mit niedrigerer Reihenfolge bezieht.
- Mit dem Datenschutz-Plugin befinden sich Datenschutztabellen standardmäßig im Tabellensatz Clone Data Preservers
- Beim Versuch, eine Datenschutztabelle (dp_[table]) zu Klon-Ausschlusstabellen hinzuzufügen, wird eine Warnung angezeigt, die Tabelle darf nicht ausgeschlossen werden.

Konfigurieren Sie die Datenschutz-Klonanforderung

Die Integration des Datenschutzklons wird mithilfe eines PostClone-Skripts konfiguriert, um Datenschutzaufträge für konfigurierte Richtlinien für das Ziel zu erstellen und auszuführen. Nach der Ausführung des Skripts sehen Benutzer deidentifizierte Daten und haben keinen Zugriff auf die ursprünglichen Daten.

Vorbereitungen

Erforderliche Rolle: data_privacy_clone_processor, data_privacy_admin und admin

Prozedur

1. Aktivieren Sie das Datenschutz-Plugin (com.glide.data_privacy) in der Quellinstanz.
   Das Plugin kann nur von Kundenservice und Supportinstalliert werden.
   Das PostClone-Skript für Datenschutz ist installiert.
2. Erhöhen Sie auf die Rolle **data_privacy_admin**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
3. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Konfiguration der Datenschutzrichtlinie**.
4. Erstellen Sie eine Konfiguration für die Datenschutzrichtlinie.
   Wählen **Sie Auf alle in Datenklasseanwenden und Beim Klonen anwenden**aus. Weitere Informationen finden Sie unter Erstellen Sie eine Datenschutzrichtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Sichern Sie die Datenschutzkonfigurationen.
6. Senden Sie als Datenschutzadministrator eine Klonanforderung.

Ergebnisse
Das PostClone-Skript für Datenschutz wird auf der Zielinstanz ausgeführt, und das PostClone-Skript erstellt einen Verbundauftragsdatensatz für Datenschutz in der Zielinstanz. Die Verbundaufgabe erstellt und führt eine Datenschutzaufgabe für jede Nachklonrichtlinie in Anwendungsreihenfolge auf der Zielinstanz aus. Die Sicherungsquelle wird auf der Zielinstanz geklont. Das PostClone-Skript für Datenschutz erstellt Datenschutzaufträge für konfigurierte Richtlinien in der Zielinstanz und führt sie aus.

Der Klonprozessor für erhöhten Datenschutz kann sich bei der Zielinstanz anmelden und den Status des Verbundauftrags nach dem Klonen in dp_federated_job.list und dp_job.list überwachen.

Datenschutz

Die Data Privacy Store-App ist eine Next Experience-Aktualisierung für Datenklassifizierung und Datenschutz mit modernem Erscheinungsbild und Benutzerfreundlichkeit. Die Store-App „Data Privacy“ wird in Utah und höher unterstützt.

Datenschutz besteht aus mehreren Komponenten: Übersicht, Klassifizierung und Anonymisierung.

Übersicht

Verwenden Sie den Abschnitt „Übersicht“ als Ausgangspunkt, um Ihre Daten und die Datenschutz-Compliance zu verwalten. Details siehe Übersicht über Datenschutz.

Klassifizierung

Datenklassifizierung ist der Prozess der Organisation von Daten in Kategorien, die das Abrufen, Sortieren und Speichern für die zukünftige Verwendung erleichtern. Die Verwendung eines Klassifizierungssystems hilft, sich auf die Anforderungen der Vertraulichkeits- und Sicherheitsrichtlinie zu konzentrieren. Klassifizieren Sie Daten, die für die Anonymisierung verwendet werden sollen. Weitere Informationen zu Datenklassen und Klassifizierungen finden Sie unter Datenklassifizierung.

Anonymisierung

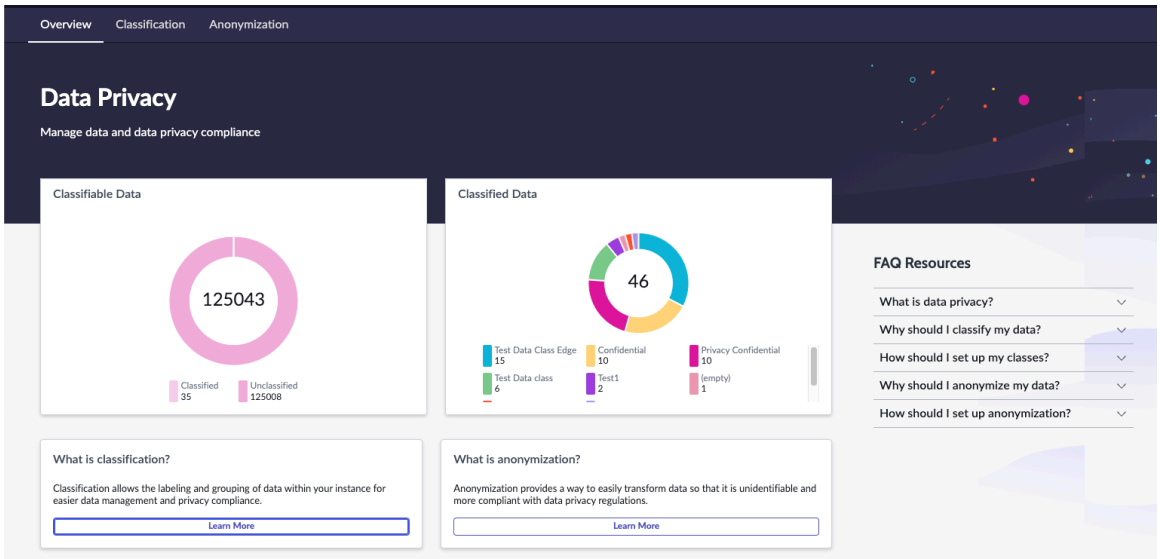
Anonymisieren Sie Informationen für alle Benutzer oder für eine Teilmenge von Benutzern, und definieren Sie die Techniken. Weitere Informationen finden Sie unter Datenanonymisierung.

Übersicht über Datenschutz

Die Übersichts-Homepage ist ein Ausgangspunkt für die Verwaltung Ihrer Daten und der Datenschutz-Compliance.

Das Übersichts-Dashboard meldet den aktuellen Status von Datenklassifizierungs- und Anonymisierungsaufgaben in Ihrer Instanz. Sie können Ihre Daten mit dem Dashboard „Übersicht“ anzeigen, um zu sehen, wie viele Daten klassifiziert werden können, welche Datenklassen verfügbar sind, wie viele Daten in jeder Klasse vorhanden sind und einen Gesamtstatus der Anonymisierungsaufgaben zu erhalten. Die klassifizierten Daten sind in verschiedene Kategorien unterteilt. Wenn Sie eine Unterkategorie in einem der beiden Diagramme auswählen, wird die Kategorie zum Gesamtdiagramm hinzugefügt oder daraus entfernt, und die Anzahl wird angepasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klassifizierbare Daten

Zeigt die Gesamtzahl der Datensätze in der Instanz an, die klassifiziert werden können. Die Anzahl wird in die Gesamtzahl der klassifizierten Daten und die Summe der nicht klassifizierten Daten unterteilt. Dies gibt Administratoren einen schnellen Überblick über potenzielle Klassifizierungsmöglichkeiten.

Klassifizierte Daten

Zeigt die Gesamtzahl der Datensätze in der Instanz an, die klassifiziert wurden. Die Anzahl wird in die Gesamtzahl der klassifizierten Daten für jede zugewiesene Datenklasse aufgeschlüsselt. Dies ermöglicht einen schnellen Überblick darüber, wie viele Daten in jedem Bereich klassifiziert wurden.

Anonymisierungsaufgaben

Zeigt Datenschutzaufträge an, die derzeit von Aufträgen verarbeitet werden, die in Ihrer Nicht-Produktionsinstanz für Benutzer- und Datenklassenaufträge abgeschlossen wurden.

Weitere Informationen

Die Abschnitte „ **Weitere** Informationen“ bieten einen schnellen Überblick über das Verständnis der Klassifizierung und Anonymisierung sowie eine einfache Möglichkeit, mit dem Prozess zu beginnen.

FAQ-Ressourcen

Greifen Sie in den Lernressourcen des Produkts auf Klassifizierung oder Anonymisierung zu, um zusätzliche Informationen darüber zu erhalten, wie Sie mit der Absicherung Ihrer Instanz durch Datenschutz beginnen können.

Aktivieren Sie Data Privacy

Data Privacy umfasst Datenklassifizierung und Anonymisierung und wird aus dem ServiceNow Storeinstalliert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Um die Datenanonymisierung zu verwenden, muss Data Privacy (Classic) zuerst mit der Berechtigung ServiceNow Vault aktiviert werden. Weitere Informationen finden Sie unter Datenschutz aktivieren (klassisch).

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** > **Datenschutz**.
2. Suchen Sie die Anwendung über die Filterkriterien und die Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie eine Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.

   (Optional) Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für häufige Anwendungsfälle veranschaulichen. Das Laden von Demodaten wird empfohlen, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

   Wichtig:
   Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.
6. Wählen Sie **Installieren** aus.

Datenklassifizierung

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

Data Classification aktiviert die Unterstützung für:

- Einblick in die Datentypen, die auf einer Now Platform -Instanz gehostet werden.
- Compliance mit Datenschutzgesetzen und Erfüllung von gesetzlichen Anforderungen für Branchen wie Finanzdienstleistungen und Herstellung medizinischer Geräte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenklassifizierungen

Die Datenklassifizierung ist ein eigenständiger Prozess, bei dem Sie Datenklassifizierungen manuell auf vorhandene Wörterbucheinträge in einer beliebigen Tabelle anwenden. Weitere Informationen finden Sie unter Data dictionary tables .

- Sie klassifizieren Daten nach Bedarf für Ihr Unternehmen und können die verfügbaren Datenklassen nach Bedarf ändern.
- Wenn Sie Daten klassifizieren, können Sie die vordefinierten Datenklassifizierungen verwenden oder eigene erstellen. Obwohl die Verwendung vordefinierter Datenklassifizierungen optional ist, wird dies als Ausgangspunkt empfohlen. Diese vordefinierten Datenklassifizierungen sind in Demodaten enthalten, die Sie in Ihrer Instanz installieren können.
- Wenn Sie eigene Datenklassifizierungen erstellen, können Sie auch ein abgestuftes hierarchisches System mit übergeordneten und untergeordneten Datenklassifizierungen entwerfen.

Hinweis:
Data Classification unterstützt die Domänentrennung, und die Tabelle „data_classification“ selbst ist prozessgetrennt. Weitere Informationen finden Sie unter Domänentrennung und Data Classification.

Anwendungsfälle

Die Allgemeine Datenschutz-Verordnung (DSGVO) ist eine Verordnung der Europäischen Union, deren Zweck darin besteht, Einzelpersonen die Kontrolle über ihre eigenen personenbezogenen Daten zu geben. Sie können Datenklassifizierungen wie personenbezogene Daten verwenden, um zu ermitteln, wo personenbezogene Daten in Ihrer Instanz gespeichert werden. Durch die Anwendung der entsprechenden Sicherheitsmechanismen zum Schutz dieser personenbezogenen Daten vor der Weitergabe erfüllt Ihr Unternehmen die DSGVO-Anforderungen.

Wenn Sie Kundeninformationen in Now Platformspeichern, verwenden Sie den Klassifizierungscode für personenbezogene Daten (Personally Identifiable Information, PII) bei Bedarf, um Daten nachzuverfolgen, die den Vorschriften der lokalen Datenschutzgesetze unterliegen.

Sie können eine eingeschränkte Datenklassifizierung auf Spalten der Mitarbeitertabelle anwenden, in denen vertrauliche Mitarbeiterinformationen wie Sozialversicherungsnummern (SSN) gespeichert werden. Administratoren und Auditoren können dann im Übersichts-Dashboard überprüfen, ob Sie die Datenklassifizierungen den richtigen Spalten zugewiesen haben. Sie können auch die Klassifizierungsdetails für eingeschränkte Arten von Informationen anzeigen.

Erstellen Sie Datenklassifizierungen

Erstellen Sie Ihre eigenen benutzerdefinierten Datenklassifizierungen in der Tabelle [data_classification], die Sie dann bestimmten Spalten in bestimmten Tabellen zuweisen können. Erstellen Sie neue Datenklassen, um den Klassifizierungsprozess zu starten.

Vorbereitungen
Erforderliche Rolle: data_classification_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz** > **Klassifizierung**.
2. Wählen Sie **+Datenklasse hinzufügen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Im Basissystem sind mehrere Datenklassen enthalten.

3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Klassenname	Name der Datenklassifizierung.
Übergeordnete Klasse	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung kein untergeordnetes Element einer übergeordneten Datenklassifizierung ist.
Beschreibung	Beschreibung der Datenklassifizierung.

4. Klicken Sie auf **Absenden**.
Die neue Datenklasse wird hinzugefügt. Wenn die Datenklasse eine untergeordnete Klasse ist, wird sie in der linken Navigationsleiste unter der übergeordneten Klasse aufgelistet.

Daten klassifizieren

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Weisen Sie Datenklassifizierungen bestimmten Tabellenspalten in der Wörterbuchtabelle [sys_dictionary] zu. Wenn Sie Datenklassifizierungen zuweisen, werden Einträge in der Tabelle Dictionary-Data Class [m2m_dictionary_dataclass] erstellt, die Sie dann im Dashboard „Übersicht“ überprüfen können.

Vorbereitungen
Erforderliche Rolle: data_classification_admin, admin

Prozedur

1. Wählen Sie **Neu** aus, um Daten aus einer zu klassifizierenden Tabelle zuzuweisen.
2. Wählen Sie die Datenklasse aus der Dropdown-Liste aus.
3. Wählen Sie die Datensätze aus, die die zu klassifizierenden Tabellen und Spalten widerspiegeln.
Wählen Sie zusätzliche Zeilen aus, die pro Seite in der Tabelle angezeigt werden sollen, um die Suche nach einer bestimmten Tabelle zu erleichtern.
4. Wählen Sie **Daten klassifizieren aus**.
Die Daten werden unter dem Klassifizierungsnamen in der Tabelle „Klassifizierte Daten“ klassifiziert.
5. Zeigen Sie die Daten an, oder exportieren Sie sie in Excel, CSV, JSON oder PDF.
Wählen Sie aus, ob Sie die Daten im ausgewählten Format herunterladen oder per E-Mail erhalten möchten.

Datenanonymisierung

Die Anonymisierung bietet eine Möglichkeit, Daten einfach umzuwandeln, sodass sie nicht identifizierbar sind und den Datenschutzbestimmungen besser entsprechen.

Administratoren können den Anonymisierungsprozess sowohl in Produktions- als auch in Nicht-Produktionsinstanzen durchführen. Datenschutz kann in Produktionsinstanzen verwendet werden, um Benutzer zu deidentifizieren. Die Anonymisierung von Datenklassen sollte nur für Nicht-Produktionsinstanzen verwendet werden. Dadurch wird sichergestellt,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dass Daten wie E-Mail-Adressen oder physische Adressen durch ähnlich formatierte, aber anonymisierte Versionen ersetzt werden.

Administratoren können die Anonymisierung auch als Teil ihrer Prozesse für das Recht auf Vergessenwerden (RTBF) der Datenschutz-Grundverordnung (DSGVO) verwenden, um Benutzerinformationen zu anonymisieren. Weitere Informationen finden Sie unter https://gdpr-info.eu/art-17-gdpr/ .

Verwenden Sie den Anonymisierungsabschnitt von Data Privacy, um Datenschutzrichtlinien und -techniken zu erstellen und anzuzeigen und Massenzuweisungen für den Datenschutz durchzuführen. Zeigen Sie alle Aufträge mit Beschreibung, verwendeter privater Richtlinie und Status an. Um auf den Anonymisierungsabschnitt zugreifen zu können, muss ein Administrator zuerst eine Erhöhung auf die Rollen „data_privacy_admin“ und „data_privacy_processor“ durchführen.

Anonymisierungstechniken

Anonymisierungstechniken sind Optionen, die Sie auswählen, um festzulegen, wie Ihre Daten anonymisiert werden. Sie müssen eine Anonymisierungstechnik erstellen, auf die im Anonymisierungsauftrag verwiesen werden soll. Informationen zum Zuordnen einer Datenschutztechnik zu einer zugehörigen **Anonymisierungstechnikkonfiguration finden**Sie unter .

Anonymisierungsrichtlinien

Konfigurieren Sie eine Anonymisierungsrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden. Weitere Informationen zu Erstellen Sie Anonymisierungsrichtlinien finden Sie unter.

Anonymisierungsaufträge

Anonymisierungsaufgaben verwenden alle diese Komponenten, um Ihre Daten zu anonymisieren. Weitere Informationen zu diesen Aufgaben finden Sie unter Erstellen Sie einen Anonymisierungsauftrag.

Erstellen Sie Anonymisierungstechniken

Erstellen Sie eine Datenschutztechnikkonfiguration, um anzupassen, wie der Datenschutz Ihre Daten anonymisiert.

Vorbereitungen
Erforderliche Rolle: data_privacy_admin und admin

Prozedur

1. Erhöhen Sie auf die Rolle **data_privacy_admin**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**.
3. Wählen Sie **Techniken anzeigen aus**.
   Es stehen mehrere vordefinierte Techniken zur Auswahl.

Technik	Beschreibung
Wählen Sie Ersetzen aus	Diese Technik führt eine selektive Ersetzung von Zeichenfolgendaten durch. Alle Zeichen zwischen den Start- und Endindizes der Eingabe werden durch das ausgewählte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Technik	Beschreibung
	Zeichen ersetzt. Sie können Zeichen angeben, die von der Maskierung ausgeschlossen werden sollen: ◦ start_index: Technik maskiert Daten ab dem angegebenen Zeichen. Wenn das Feld leer gelassen wird, beginnt die Maskierung mit dem ersten Zeichen. ◦ end_index: Die Technik maskiert Daten vom Beginn der Zeichenfolge bis zum angegebenen Zeichen. Wenn das Feld leer gelassen wird, endet die Maskierung mit dem letzten Zeichen. ◦ exclude_char: Definieren Sie ein Zeichen, das von der Maskierung ausgeschlossen werden soll. ◦ ersatz_char: Definieren Sie ein Zeichen, das für die Maskierung verwendet wird. Wenn keines angegeben ist, werden standardmäßig Sternchen (*) verwendet.
Statisches Ersetzen	Diese Technik tauscht Werte mit statischen Werten aus. Zeichenfolgen-, Zahlen- und Datumsdaten können diese Technik verwenden: ◦ date_time_value: Datumswerte durch dieses Datum ersetzen. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss. ◦ date_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt. ◦ number_value: Ersetzen Sie Zahlenwerte durch diese Zahl. ◦ string_value: Ersetzen Sie Zeichenfolgenwerte durch diesen Text.
Zufälliges Ersetzen	Diese Technik tauscht Werte mit zufällig generierten Werten aus. Zeichenfolgen- und Zahlendaten können diese Technik verwenden.
Entfernen	Diese Technik entfernt Werte und ersetzt sie durch leere Werte (Null).
Keine Aktion	Diese Technik ist ein Platzhalter. Bei Auswahl werden keine Felder geändert.
Wählen Sie Ersetzen durch X aus	Wandelt Zeichenfolgendaten um und ersetzt vertrauliche Zeichen selektiv durch den Buchstaben X. **Hinweis:** Standardtechnik für Datenmuster in Datenerkennung erkunden.
Anonymisierung von Datenmustern	Anonymisiert erkannte Datenmuster nur in unstrukturierten Datenfeldern, während der zugrunde liegende Kontext intakt bleibt. **Hinweis:** Die Einstellungen für diese Technik beziehen sich auf die Einstellungen der Anonymisierungstechnik für Datenmuster in Datenerkennung erkunden.

4. Wählen **Sie Benutzerdefinierte Technik hinzufügen**aus, wenn Sie keine vordefinierte Technik verwenden.
5. Füllen Sie die Felder im Formular **„Technik anpassen“** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld1	Beschreibung
Basistechnik	Wählen Sie eine vordefinierte Technik aus, da benutzerdefinierte Techniken auf den vordefinierten Techniken basieren.
Technikname	Geben Sie einen Namen für die Technik ein.
Technikbeschreibung	Geben Sie eine Beschreibung für die Technik ein.

6. Wählen Sie **Weiter**.
7. Geben Sie die Technikparameter ein.
   Die verfügbaren parametrisierten Werte hängen von der von Ihnen ausgewählten Datenschutztechnik ab. Es gibt keine parametrisierten Werte für die Techniken **„Keine Aktion“** und „ **Entfernen** “.

Parametrisierte Datenschutzwerte für die Basistechniken

Basistechnik	Wert des Parameters für Datenschutztechnik	Beschreibung	Standardwert
Wählen Sie Ersetzen aus	end_index	Die Technik maskiert Daten vom Anfang der Zeichenfolge bis zum angegebenen Zeichen. Wenn leer gelassen, endet die Maskierung mit dem letzten Zeichen.	(leer)
Wählen Sie Ersetzen aus	exclude_char	Zeichen zum Überspringen der Maskierung. In diesem Wert kann nur ein einzelnes Zeichen verwendet werden. Wenn mehrere eingegeben werden, wird das erste Zeichen verwendet.	(leer)
Wählen Sie Ersetzen aus	ersatz_zeichen	Zeichen, das beim Ersetzen von Werten durch selektives Ersetzen verwendet werden soll.	Ein Sternchen (*) wird verwendet, wenn kein anderer Wert eingegeben wird.
Wählen Sie Ersetzen aus	start_index	Die Technik maskiert Daten ab dem angegebenen Zeichen.	Wenn das Feld leer gelassen wird, beginnt die Maskierung beim ersten Zeichen.
Statisches Ersetzen	date_time_value	Ersetzen Sie Datums- und Uhrzeitwerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss.	1988-11-11 10:10:10
Statisches Ersetzen	date_value	Ersetzen Sie Datumswerte durch dieses Datum.	1988-11-11

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basistechnik	Wert des Parameters für Datenschutztechnik	Beschreibung	Standardwert
		Verwenden Sie das Format jjjj-MM-tt.	
Statisches Ersetzen	number_value	Ersetzen Sie Zahlenwerte durch diese Zahl.	1234567
Statisches Ersetzen	string_value	Ersetzen Sie Zeichenfolgenwerte durch diesen Text.	TEXT123
Zufälliges Ersetzen	erhalten_daten_länge	Setzen Sie diese Option auf „ **true** “, um die Datenlänge beizubehalten. Deidentifizierte Daten haben dieselbe Länge wie die ursprünglichen Daten.	Wahr

8. Wählen **Sie Benutzerdefinierte Technik erstellen aus**.
   Ihre benutzerdefinierte Technik wird den Anonymisierungstechniken hinzugefügt.

Nächste Maßnahme

Unter Erstellen Sie Anonymisierungsrichtlinien erfahren Sie, wie Sie eine Anonymisierungsrichtlinie konfigurieren, um anzugeben, welche Techniken bei der Anonymisierung Ihrer Daten verwendet werden.

Erstellen Sie Anonymisierungsrichtlinien

Konfigurieren Sie eine Anonymisierungsrichtlinie, um anzugeben, welche Techniken bei der Anonymisierung Ihrer Daten verwendet werden.

Vorbereitungen

Die Datenschutzkonfiguration definiert Tabellen, sys_user und andere sowie Spalten für die De-Identifizierung, abhängig vom Anwendungsfall, und gibt parametrisierte Typen der Techniken an, die bei der De-Identifizierung von Daten verwendet werden sollen.

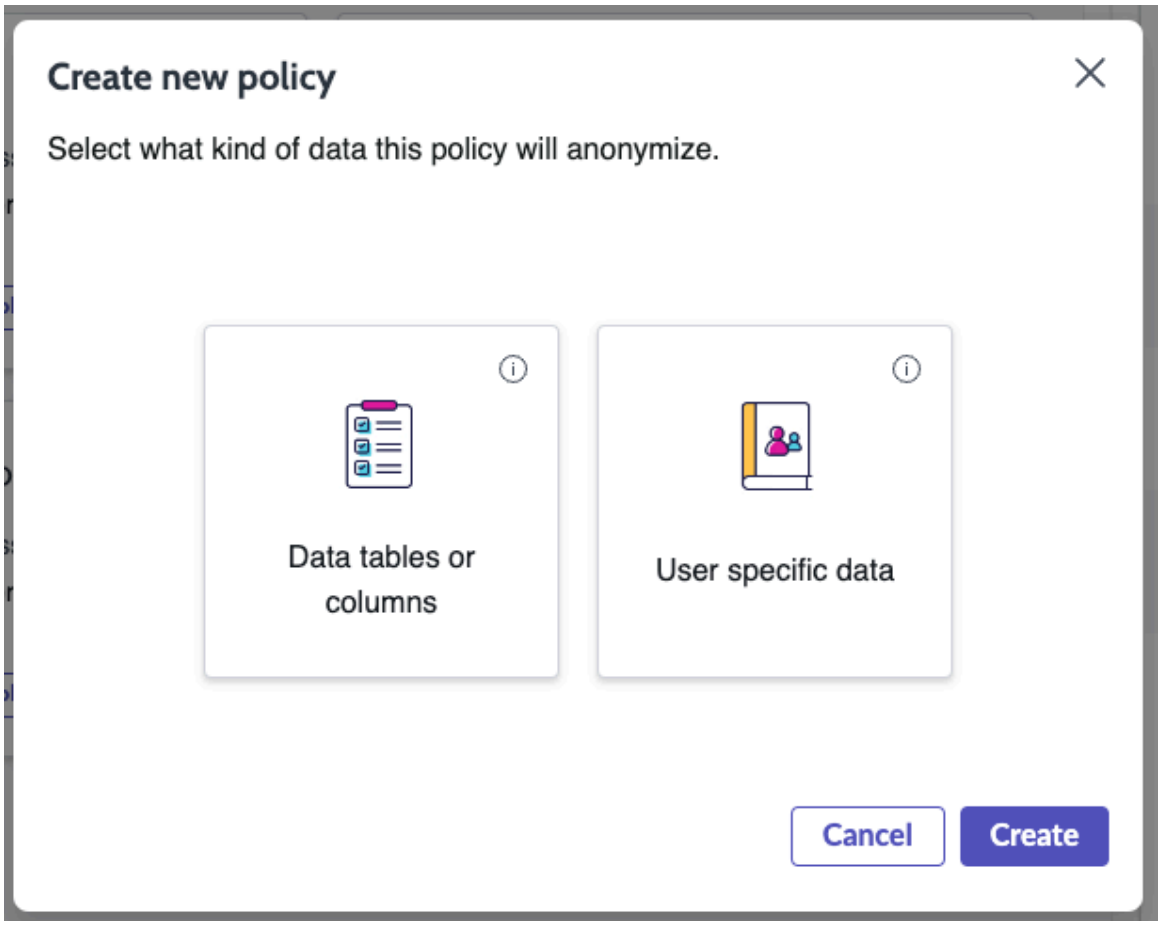
Hinweis:
Um eine Datenschutzkonfiguration abzuschließen, müssen Sie zuerst eine Konfiguration für die Datenschutztechnik konfigurieren. Weitere Informationen finden Sie unter .

Erforderliche Rolle: data_privacy_admin und admin

Prozedur

1. Erhöhen Sie auf die Rolle **data_privacy_admin**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**.
   Alle Anonymisierungsrichtlinien werden angezeigt. Veröffentlichte Richtlinien sind verfügbar, um die Anonymisierungsaufgabe zu planen.
3. Wählen **Sie Neue Richtlinie erstellen aus**.
4. Wählen Sie diese Option aus, um entweder **Datentabellen oder -spalten** oder **benutzerdefinierte Daten**zu anonymisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Datenschutzrichtlinien können nur für klassifizierte Daten gelten. Weitere Informationen zur Datenklassifizierung finden Sie unter Datenklassifizierung.

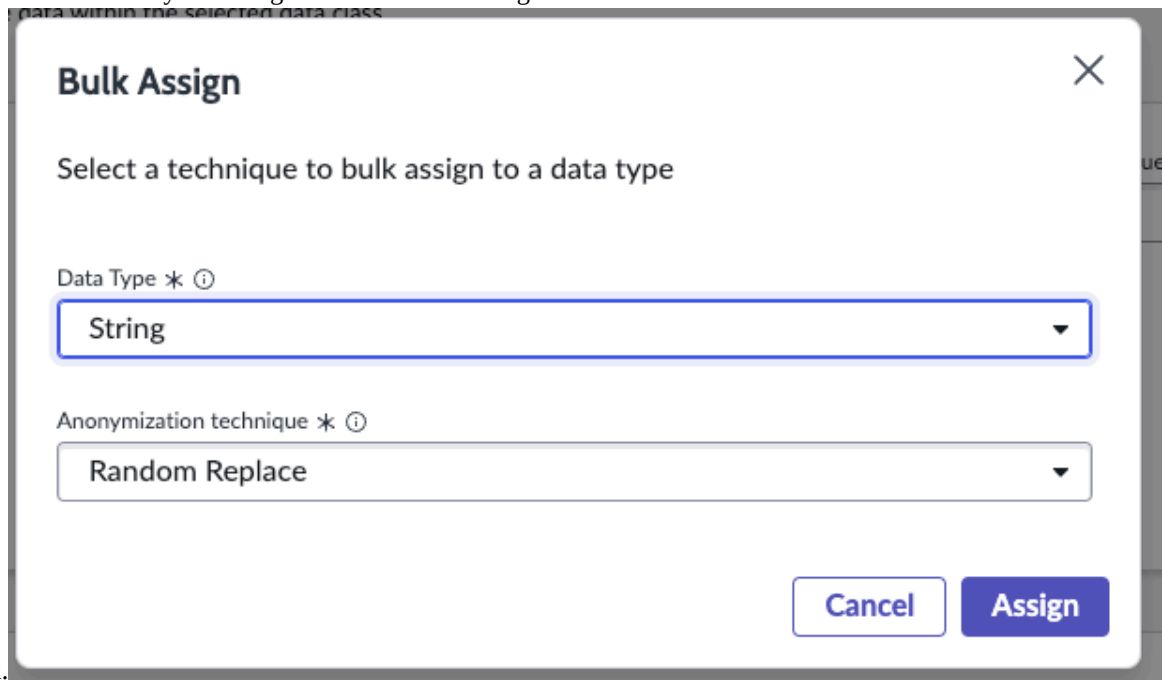
5. Wählen Sie **Erstellen** aus.
   Zum Abschließen der Richtlinie sind sequenzielle Schritte erforderlich: **Details definieren**und **Techniken zuweisen**. Die**Benutzerreferenz auswählen** ist auch erforderlich, wenn die Richtlinie für anwenderspezifische Daten definiert wird.
6. Definieren Sie die Details für die neue Anonymisierungsrichtlinie.
   - Geben Sie den Richtliniennamen in das Feld **Name** und die Richtlinienbeschreibung in das Feld **Beschreibung** ein.
   - **Wählen** Sie im Feld Datenklasse die Datenklasse aus, die mit dieser Richtlinie verwendet werden soll.

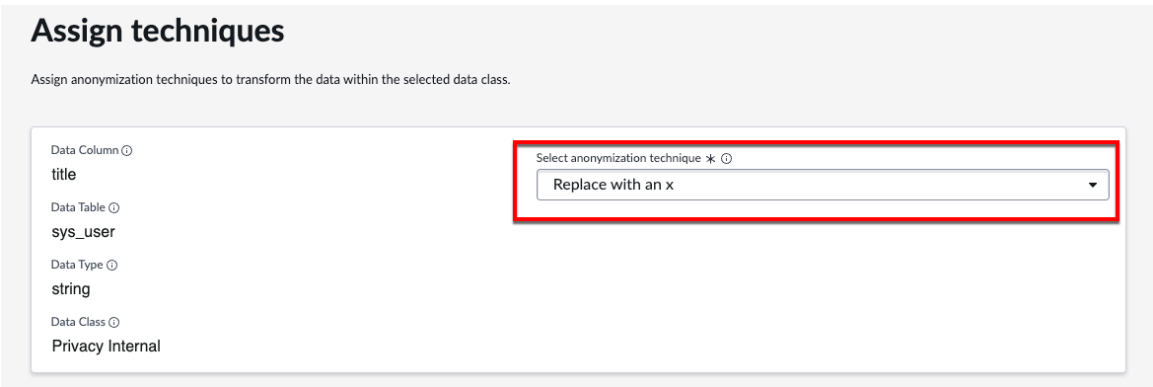
   Hinweis:
   Wenn Sie einen Eintrag nicht anonymisieren, wählen Sie die **DoNothing-** Technik aus, anstatt den Eintrag leer zu lassen. Richtlinien mit leeren Werten im Feld „Konfiguration der Datenschutztechnik“ können nicht ausgeführt werden, wenn sie in Datenschutzaufgaben verwendet werden.

Nach Auswahl einer Datenklasse wird das Formular „Techniken zuweisen“ für jeden Datensatz angezeigt, der für die definierte Datenklasse zurückgegeben wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Weisen Sie Anonymisierungstechniken für die ausgewählte Datenklasse zu.





8. **Wahlweise:** Wenn Datenmusteranonymisierung ausgewählt ist, wählen Sie die zu verwendende Anonymisierungstechnik aus.
9. **Wahlweise:** Legen Sie die Reihenfolge für Datenmuster fest.
10. **Wahlweise:** Klicken Sie auf die Schaltfläche **Test**, um die Richtlinie zu testen.
11. Wählen Sie **Speichern**.
12. Wählen Sie **Veröffentlichen** aus, um die Anonymisierungsrichtlinie für die Zeitplanung zu aktualisieren und zu den Anonymisierungsrichtlinien zurückzukehren.

> **Hinweis:**
> Nur veröffentlichte Richtlinien können für die Planung von Anonymisierungsaufgaben verwendet werden.

Nächste Maßnahme

Erstellen Sie einen Anonymisierungsauftrag.

Konfigurieren Sie die Klonanforderung für die Datenanonymisierung

Die Integration des Datenschutzklons wird mithilfe eines PostClone-Skripts konfiguriert, um Datenschutzaufträge für konfigurierte Richtlinien für das Ziel zu erstellen und auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Ausführung des Skripts sehen Benutzer deidentifizierte Daten und haben keinen Zugriff auf die ursprünglichen Daten.

Vorbereitungen

Das PostClone-Skript für Datenschutz wird mit der Aktivierung des Datenschutz-Plugins (com.glide.data_privacy) installiert. Details siehe Aktivieren Sie Data Privacy.

Erforderliche Rolle: data_privacy_clone_processor, data_privacy_admin und admin

Prozedur

1. Aktivieren Sie das Datenschutz-Plugin (com.glide.data_privacy) in der Quellinstanz.
   Das PostClone-Skript für Datenschutz ist installiert.
2. Erhöhen Sie auf die Rolle **data_privacy_admin**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
3. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**.
4. Wählen **Sie Neue Richtlinie erstellen aus**.
   Details siehe Erstellen Sie Anonymisierungsrichtlinien.
5. Wählen Sie **Datentabellen oder -spalten aus**.
6. Wählen Sie **Erstellen** aus.
7. Geben Sie einen Namen ein, und wählen Sie eine Datenklasse aus.
8. **Aktivieren Sie die Richtlinie während des Klonens**.
9. Wählen Sie die auszuführende Richtlinienreihenfolge aus, wenn mehrere Klonrichtlinien vorhanden sind. Eine Datenschutzaufgabe für die Postclone-Konfiguration mit einer höheren Anwendungsreihenfolge wird möglicherweise vor einer anderen Aufgabe mit niedrigerer Reihenfolge gestartet, wenn die Aufgabe mit der höheren Reihenfolge keine Tabelle umfasst, die sich auf eine andere Aufgabe mit niedrigerer Reihenfolge bezieht.
10. Wählen Sie **Fortsetzen** aus.
11. Schließen Sie die Richtlinienkonfiguration ab, und veröffentlichen Sie die Richtlinie.
12. Sichern Sie die Datenschutzkonfigurationen.
13. Planen Sie die Anonymisierungsaufgabe.
    Details siehe Erstellen Sie einen Anonymisierungsauftrag.
14. Senden Sie als Datenschutzadministrator eine Klonanforderung.

Ergebnisse

Das PostClone-Skript für Datenschutz wird auf der Zielinstanz ausgeführt, und das PostClone-Skript erstellt einen Verbundauftragsdatensatz für Datenschutz in der Zielinstanz. Die Verbundaufgabe erstellt und führt eine Datenschutzaufgabe für jede Nachklonrichtlinie in Anwendungsreihenfolge auf der Zielinstanz aus. Die Sicherungsquelle wird auf der Zielinstanz geklont. Das PostClone-Skript für Datenschutz erstellt Datenschutzaufträge für konfigurierte Richtlinien in der Zielinstanz und führt sie aus.

Der Klonprozessor für erhöhten Datenschutz kann sich bei der Zielinstanz anmelden und den Status des Verbundauftrags nach dem Klonen in dp_federated_job.list und dp_job.list überwachen.

Erstellen Sie einen Anonymisierungsauftrag

Konfigurieren Sie einen Datenschutzauftrag in Ihrer Produktionsinstanz, um anonymisierte Daten in Ihrer Nicht-Produktionsinstanz für Benutzer- und Datenklassenaufträge zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Datenschutzaufgabe unterstützt zwei Anwendungsfälle der Deidentifizierung:

- Vertrauliche Daten bestimmter sys_users
- Vertrauliche Daten einer bestimmten Datenklasse.

Erforderliche Rolle: data_privacy_processor und admin

Prozedur

1. Erhöhen Sie auf die Rolle **data_privacy_processor**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**.
3. Wählen Sie in einer Anonymisierungsrichtlinie **Aufgabe** planen für die Richtlinie aus, die in der Aufgabe verwendet werden soll.
   Eine Richtlinie muss sich im Status „Veröffentlicht“ befinden, um eine Anonymisierungsaufgabe zu planen.

> ⚠ **Warnung:**
> Anonymisierungsaufgaben sind äußerst destruktiv und können nur bei einem Rollback rückgängig gemacht werden. Überprüfen Sie alle Informationen, z. B. Datensätze und Tabellen, die verarbeitet wurden, bevor Sie eine Aufgabe planen.

4. Füllen Sie die Felder des Formulars aus.

Felder für Datenschutzaufträge

Feld	Beschreibung
Verwendete Richtlinie	Schreibgeschützter Name der ausgewählten Datenschutzrichtlinienkonfiguration, die für diesen Auftrag verwendet werden soll. Bearbeiten Sie die Richtlinie, um zusätzliche Informationen zur Richtlinie anzuzeigen. Weitere Informationen zu Konfigurationen von Datenschutzrichtlinien finden Sie unter Erstellen Sie Anonymisierungsrichtlinien.
Stellenbeschreibung	Beschreibung der Aufgabe.
Startzeit	Der Beginn der Zeit für die Ausführung dieses Auftrags in **HH:MM:SS**.
Endzeit	Das Ende des Zeitfensters für die Ausführung dieses Auftrags in **HH:MM:SS**. Die Endzeit muss nach der Startzeit liegen. Die Aufgabe wird vor der in diesem Feld eingegebenen Zeit ausgeführt. Wenn die Aufgabe noch nicht abgeschlossen ist, wird die Aufgabe angehalten und beim nächsten Start des Zeitfensters fortgesetzt.
Probelauf	Führen Sie die Aufgabe als Test aus. Bei Ausführung dieses Auftrags sind keine Datensätze betroffen. Die Ergebnisse werden in der

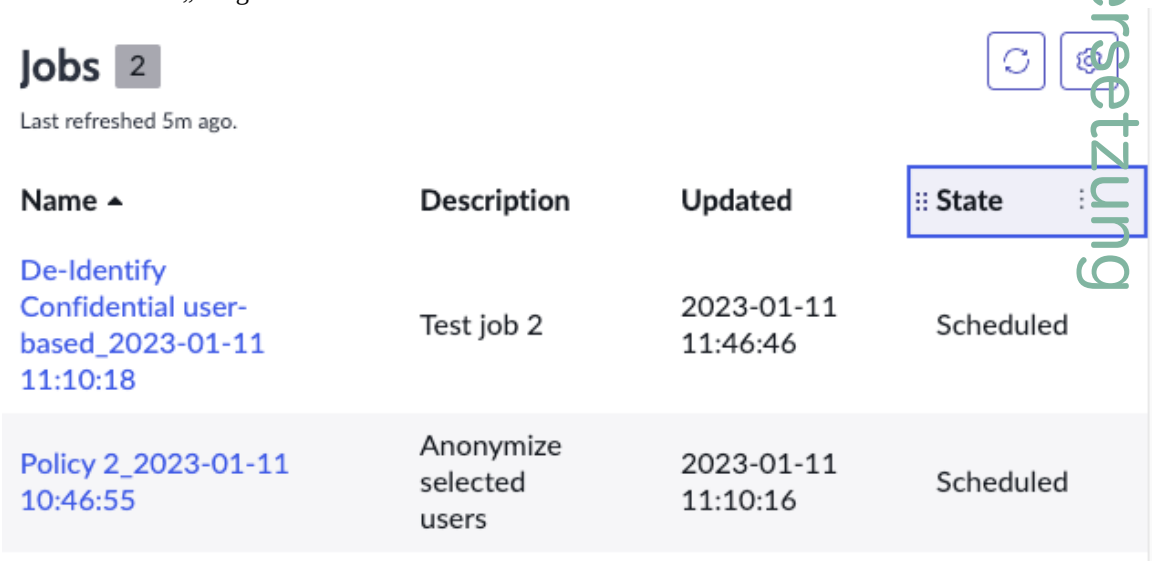
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Auftragsliste **angezeigt**, als ob der Auftrag ausgeführt worden wäre. **Hinweis:** **Probelauf** muss deaktiviert sein, wenn ein Datenschutzauftrag mit Rollback konfiguriert wird. Details siehe Setzen Sie eine Datenschutzaufgabe zurück.
Benutzer auswählen	Wählen Sie maximal zehn Anwender aus, die in diesem Auftrag anonymisiert werden sollen. **Hinweis:** Dieses Pflichtfeld wird nur angezeigt, wenn die ausgewählte Datenschutzrichtlinienbedingung eine Auswahl von Benutzerdatensätzen erfordert.

5. Wählen Sie im Formular **Auftrag** planen aus, um die Anonymisierung in die Auftragswarteschlange zu platzieren.
Die Aufgabe wird zwischen den in den Feldern **Startzeit** und **Endzeit** ausgewählten Zeiten ausgeführt. Wenn die Aufgabe während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird die Aufgabe beim nächsten Start des Zeitfensters fortgesetzt.

Hinweis:
Ein Auftrag kann nur einmal ausgeführt werden, auch wenn **Probelauf** ausgewählt ist. Um eine Aufgabe basierend auf derselben Richtlinie erneut auszuführen, wählen Sie **Aufgabe planen** aus, und füllen Sie das Formular mit denselben Feldwerten aus.

Die Aufgabe wird im Bereich „Aufgaben“



aufgelistet.

Feld	Beschreibung
Name	Name des Anonymisierungsauftrags.
Beschreibung	Beschreibung des Anonymisierungsauftrags.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung des Auftrags.
Status	Status der Datenschutzaufgabe: ○ **Geplant**: Standardstatus für neue Aufgaben. ○ **Abgeschlossen**: Der Auftrag hat die ausgewählten Daten erfolgreich anonymisiert. ○ **Abgebrochen**: Der Auftrag wurde manuell abgebrochen. ○ **Fehler**: Beim Speichern des Auftrags ist ein Problem aufgetreten. Planen Sie die Aufgabe neu, oder erstellen Sie eine neue Aufgabe. Wenn der Fehler weiterhin auftritt, können Probleme mit der Konfiguration auftreten. ○ **Rollback**wird ausgeführt: Der Auftrag wurde so festgelegt, dass ein Rollback der Anonymisierung durchgeführt wird. ○ **Rollback abgeschlossen**: Das Rollback des Anonymisierungsauftrags wurde erfolgreich abgeschlossen. Ein schreibgeschütztes Feld.

6. Wählen Sie im Bereich „ **Aufträge** “ einen Auftrag aus, um die Auftragsübersicht zu öffnen.
Nachdem eine Aufgabe geplant wurde, werden die Schaltflächen Aufgabe **abbrechen** und **Anhalten** in der Aufgabenübersicht angezeigt.

Zusätzliche Felder für regelmäßige Aufgaben

Feld	Beschreibung
Geschätzte Anzahl der Datensätze	Die geschätzte Anzahl von Datensätzen, die von diesem Probelauf betroffen sind, bevor er ausgeführt wird. Ein schreibgeschütztes Feld
Gesamtzahl der verarbeiteten Datensätze	Die Gesamtzahl der einzelnen Datensätze, die von diesem Auftrag betroffen sind. Ein schreibgeschütztes Feld.
Gesamtzahl der verarbeiteten Datentabellen	Die Gesamtzahl der von diesem Auftrag verarbeiteten Datentabellen. Ein schreibgeschütztes Feld.
Verbleibende Zeit bis zum Rollback	Die verbleibende Zeit, in der ein abgeschlossener Datenanonymisierungsauftrag zurückgesetzt und die Daten deanonymisiert werden können. Ein schreibgeschütztes Feld.
Gesamtanzahl der verarbeiteten Anwender	Die Gesamtzahl der einzelnen Benutzerdatensätze, auf die sich dieser Auftrag auswirkt. Ein schreibgeschütztes Feld.
Auftrag abbrechen	Wählen Sie diese Option aus, um den Anonymisierungsauftrag abzubrechen. Dies muss vor der Startzeit des Auftrags ausgewählt werden. Wenn diese Option ausgewählt ist, wird der Auftragsstatus auf „ *Abgebrochen*“ aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Pausierung	Wählen Sie diese Option aus, um den Auftrag anzuhalten und die Aufzeichnung zurückzusetzen, wenn „Rollback“ ausgewählt wurde. Nach Ablauf von drei Tagen für Rollback-Kontexte wird eine Warnmeldung angezeigt. Diese muss nach der Startzeit des Auftrags und vor der Endzeit des Auftrags ausgewählt werden. Wenn diese Option ausgewählt ist, wird der Auftragsstatus auf *Angehalten*aktualisiert.
Fortfahren	Startet einen angehaltenen Auftrag neu. Rollback wird für fortgesetzte Aufgaben nicht unterstützt, wenn sie angehalten sind. Brechen Sie die Aufgabe ab, und erstellen Sie eine Datenschutzaufgabe. Die Aufzeichnung verwendet einen nicht abgelaufenen Rollback-Kontext. Wenn diese Option ausgewählt ist, wird der Aufgabenstatus auf „ *Geplant*“ aktualisiert.
Exportieren	Lädt eine PDF-Datei mit den Details der Datenschutzaufgabe herunter.

Rollback für Datenschutzauftrag

Datenbankänderungen werden für Aktionen wie Aufträge und Skripts erfasst, sodass die Änderungen zurückgesetzt werden können. Setzen Sie eine Datenschutzaufgabe zurück, wenn menschliches Versagen versehentlich falsche Benutzerinformationen anonymisiert. Durch das Rollback werden die Daten aus der Datenschutzaufgabe deanonymisiert.

Übersicht

- Das Rollback ist auf einige Tage pro konfigurierter Ablaufdauer des RollbackContext des neuen RollbackType *REDACT*beschränkt. Nach Ablauf des einer Datenschutzaufgabe zugeordneten RollbackContext ist die Rollback-Funktion für diese Aufgabe nicht mehr verfügbar.
  - Ein Rollback-Kontext aus der Deanonymisierung wird standardmäßig drei Tage lang gespeichert.
  - Die Standardablaufzeit kann vom Datenschutzadministrator im **RollbackContext** des neuen **RollbackType** *REDACT.* auf einen Wert größer als eins festgelegt werden. Legen Sie den Wert in der Glide-Systemeigenschaft *glide.rollback.expiration_days_redact*fest. Siehe Rollback-Kontexte.

    Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Add a system property .

    für zusätzliche Informationen.
- Rollback ist für Datenschutzaufgaben verfügbar, die sich im Status „Abgeschlossen“, „Abgebrochen“ oder „Fehler“ befinden.
- Für jeden erfolgreichen sys_user-Deanonymisierungsauftrag, der mit einer Datenschutzrichtlinie mit aktivierter Rollback-Unterstützung konfiguriert ist, wird ein Rollback-Kontext erstellt. Pro Datenschutzaufgabe kann es höchstens einen Rollback-Kontext geben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setzen Sie eine Datenschutzaufgabe zurück

Setzen Sie einen Datenschutzauftrag in Ihrer Nicht-Produktionsinstanz, der anonymisierte Daten aus Ihrer Produktionsinstanz verwendet, auf einen Status vor der Deidentifizierung einer Datenklasse oder eines Benutzerauftrags zurück.

Vorbereitungen

Erforderliche Rolle: data_privacy_admin oder data_privacy_processor und admin

Prozedur

1. Erhöhen Sie auf die Rolle „ **data_privacy_processor“** oder **„data_privacy_admin“**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle erweitern.
2. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz** > **Anonymisierung**.

   Hinweis:
   Im Voraus muss eine Konfiguration der Datenschutzrichtlinie erstellt werden, die das Rollback unterstützt. Weitere Informationen finden Sie unter Erstellen Sie Anonymisierungsrichtlinien.

3. Wählen Sie eine Anonymisierungsaufgabe aus, die sich im Status **Abgeschlossen** befindet.
   - Nach der Ausführung des Auftrags werden die Daten für die ausgewählte Konfiguration anonymisiert.
   - In der Auftragszusammenfassung informiert das Feld **Verbleibende Zeit für Rollback** über die Ablaufzeit. Innerhalb dieses Zeitrahmens haben Sie die Möglichkeit, den Auftrag zurückzusetzen.
4. Wählen Sie **Rollback** aus, um die Daten zu deanonymisieren.
   Der Auftragsstatus wird bei Erfolg auf „Rollback_Complete“ aktualisiert.

Datenschutz-API

Referenz für Datenschutz-API

DataPrivacyAPI – anonymize(String input)

Anonymisiert die Eingabezeichenfolge durch Anwendung der Datenmuster-Anonymisierungstechnik mit aktiven Datenmustern, die im Plugin Datenerkennung konfiguriert sind.

Parameter

Name	Typ	Beschreibung
Eingabe	Zeichenfolge	Eingabezeichenfolge, die anonymisiert werden soll.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Serialisierte JSON-Zeichenfolge. Erfolg Gibt „true“ zurück, wenn die Anonymisierung erfolgreich war

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse (Fortsetzung)

Typ	Beschreibung
	inputChanged Gibt „true“ zurück, wenn sich der anonymisierte Wert von der Eingabe unterscheidet. Fehler Gibt den Fehlercode zurück, wenn ein Fehler aufgetreten ist Ausgabe Wenn „ Erfolg “ auf „wahr“ gesetzt ist, enthält es eine anonymisierte Zeichenfolge.

Example: Code-Beispiel

```
var privacyApi = new SNC.DataPrivacyApi();
var input = 'SSN: 123-45-6789';
var jsonString = privacyApi.anonymize(input);  // activate necessary data patterns first in
 discovery plugin
var output = JSON.parse(jsonString);

if (output.success) {
   gs.info('anonymized string: ' + output.output);
} else {
  gs.info('anonymization failed: ' + output.error);
}
```

Konfiguration

Name	Konfigurationsmodus	Beschreibung
DataPrivacyApi.anonymize-Eingabegröße	sys_property: data_privacy.api.input.size	Systemeigenschaft zum Definieren der maximalen Eingabegröße, die von DataPrivacyApi.anonymize-Aufrufen unterstützt wird. , . • Der Standardwert ist 4000 • Bereich ist ein ganzzahliger Wert zwischen 0 und 10.000
Cache-Nutzung nach Datenschutz-API	sys_property: data_privacy.api.use.cache	Systemeigenschaft zum Definieren, ob DataPrivacyApi die Konfigurationen zwischenspeichern soll. • Der Standardwert ist „true“. • Bereich ist boolesch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration (Fortsetzung)

Name	Konfigurationsmodus	Beschreibung
Zeitüberschreitung für Anonymisierungs-API	DataPrivacyApi.setAnonymizeTimeout (lange Zeitüberschreitung Millis)	API-Aufruf, um die maximale Zeit in Millisekunden für den Abschluss der DataPrivacyAPI.anonymize-Aufrufe zu definieren. • Der Standardwert ist 20.000 (ms). • Bereich ist ein ganzzahliger Wert zwischen 0 und 50000 (ms).

Datenerkennung

Verwenden Sie Datenerkennung, um vertrauliche Daten innerhalb einer Instanz zu identifizieren, z. B. Kreditkarteninformationen, E-Mails oder Sozialversicherungsnummern.

Erkunden Sie die Datenerkennung

Erfahren Sie mehr über Data Discovery.

Konfigurieren Sie die Datenerkennung

Erhalten Sie Hilfe bei der Konfiguration der Daten-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen in der Datenerkennung

Erfahren Sie mehr über Rollen in Data Discovery.

Daten-Discovery-Ergebnisse

Überprüfen Sie die Daten-Discovery-Ergebnisse.

Datenerkennung erkunden

Verwenden Sie Datenerkennung, um vertrauliche Daten innerhalb einer Instanz zu identifizieren, z. B. Kreditkarteninformationen, E-Mails oder Sozialversicherungsnummern.

Datenerkennung führt einen benutzerdefinierten Satz von Aufträgen für einen Satz von Tabellen aus. Die -Jobs suchen nach vertraulichen Informationen und melden sie zur Überprüfung im Dashboard Datenerkennung. Eine regelmäßige Aufgabe verwendet automatisch alle aktiven Datenmuster und Zieltabellen, wenn sie ausgeführt wird.

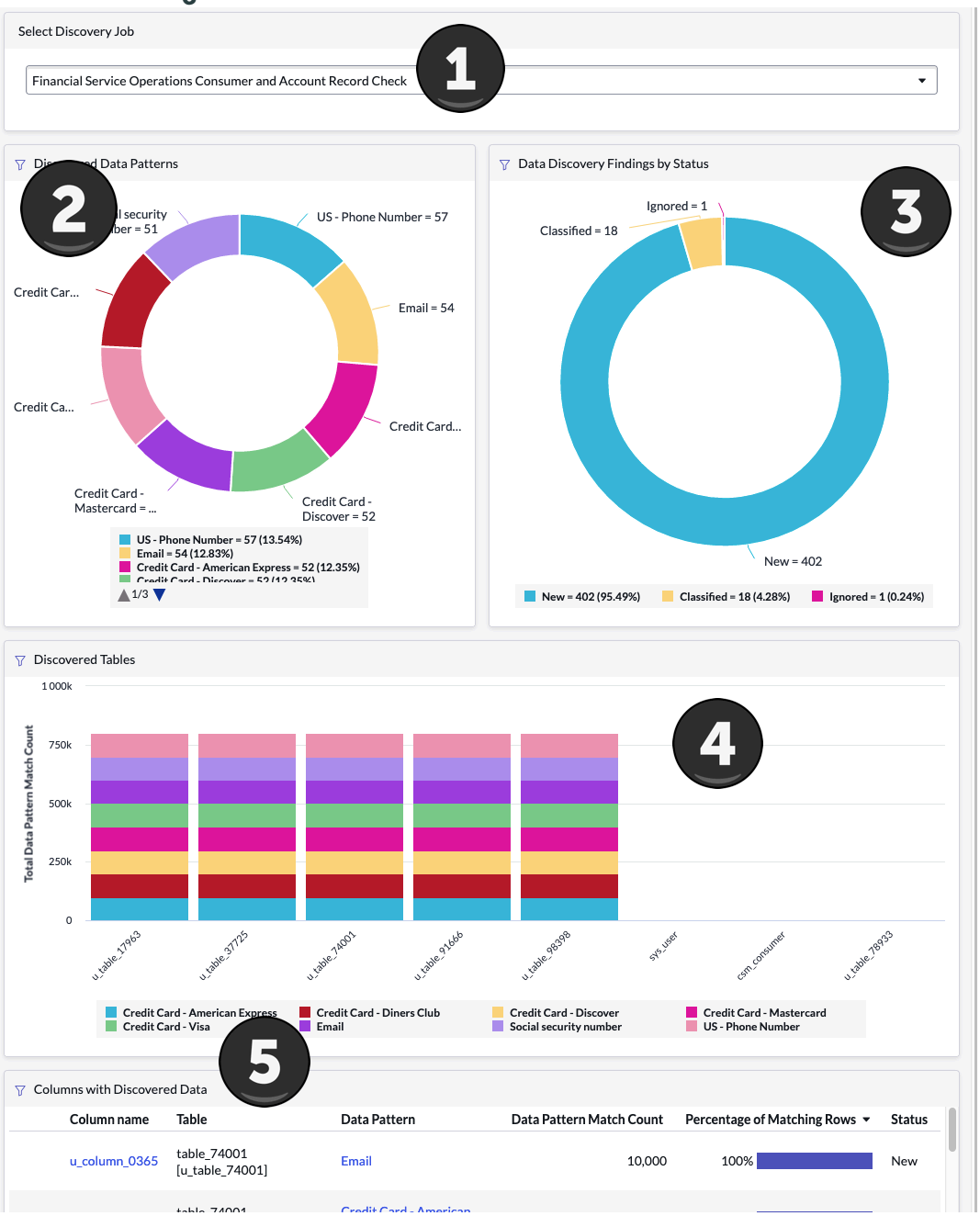
Datenerkennung enthält auch vorab zugewiesene Rollen mit unterschiedlichen Zugriffsebenen für Daten.

Zugriff auf das Dashboard von Datenerkennung

Navigieren zu **Alle** > **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Dashboard** , um das Dashboard Datenerkennung anzuzeigen und Ihre aktuellen Auftragsergebnisse zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerkennung-Dashboard



Datenerkennung Dashboard-Leitfaden

Nummer	Abschnittstitel	Abschnittsdetails
1	**Discovery-Auftrag auswählen**	
2	**Erkannte Datenmuster**	Zeigt die Anzahl und den Prozentsatz der erkannten Datenmuster nach Typ an
3	**Daten-Discovery-Ergebnisse nach Status**	Zeigt die Anzahl und den Prozentsatz der erkannten Datenmuster nach Status an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerkennung Dashboard-Leitfaden (Fortsetzung)

Nummer	Abschnittstitel	Abschnittsdetails
4	**Erkannte Tabellen**	Zeigt erkannte Muster nach Diagramm an
5	**Spalten mit erkannten Daten**	Zeigt Details zu den Spalten mit erkannten Datenmustern an

Datenerkennung aktivieren

Die Anwendung installiert Datenerkennung und zugehörige ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

Die Daten-Discovery erfordert ein vom Rest der Now Platformgetrenntes Abonnement.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste „Alle Anwendungen“ in Ihrer Instanz aktivieren.

Hinweis:

Bevor Sie ein Abonnement kaufen, können Sie die Funktion in einer Instanz außerhalb der Produktion kostenlos testen, indem Sie sie über den Now Support Servicekatalog anfordern.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit der Datenerkennung installiert:

- Rollen
- Tabellen

Weitere Informationen zu den installierten Rollen und Tabellen finden Sie unter Datenerkennung Rollen und Standarddatenmuster.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Data Discovery“ (sn_data_discovery).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Klassifizieren Sie Daten auf der Seite Datenerkennung „ Ergebnisse“.

Klassifizieren Sie vertrauliche Daten, die von allen erfolgreichen Aufgaben über Datenerkennung Ergebnisse gefunden wurden.

Vorbereitungen

Erforderliche Rolle: data_discovery_admin

Eine Aufgabe muss eine erfolgreiche Ausführung abschließen, bevor Ergebnisdaten als klassifiziert angezeigt werden können.

Warum und wann dieser Vorgang ausgeführt wird

Auf der Seite Datenerkennung „ Ergebnisse“ werden alle Dateneinträge angezeigt, die von einem Job gefunden wurden. Auf der Seite „Ergebnisse“ können Sie die Einträge überprüfen und einer Klassifizierung zuordnen.

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Daten-Discovery-Ergebnisse**.
2. Wählen Sie den Eintrag aus, den Sie klassifizieren möchten.
3. Wählen Sie in der Liste Datenerkennung Ergebnisse die **Option Klassifizieren**aus.
4. Wählen Sie die Datenklassen aus, die Sie den Tabelleneinträgen zuordnen möchten.
5. Wählen Sie **Klassifizieren aus**.

Datenerkennung Aufträge

Datenerkennung überprüft Ihre Zielinformationen anhand benutzerdefinierter Datenmuster und Zieltabellen.

Datenerkennung funktioniert, indem zuerst eine Aufgabe im Abschnitt „ **Daten-Discovery-Auftrag**“ geplant wird. Wenn eine regelmäßige Aufgabe ausgeführt wird, werden alle aktiven Datenmuster in den aktuellen Zieltabellen durchsucht. Weitere Informationen zum Erstellen und Konfigurieren einer Datenerkennung -Aufgabe finden Sie unter Konfigurieren Sie einen Datenerkennung -Job.

Hinweis:
Pro Tabelle und Muster werden bis zu 10.000 Datensätze gescannt.

Datenerkennung Datenmuster

Im Abschnitt „ **Datenmuster** “ werden alle aktuellen Datenmuster angezeigt, sowohl aktive als auch inaktive. Ein Datenmuster ist ein regulärer Ausdruck, der zum Abgleichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vertraulicher Daten verwendet wird. Weitere Informationen zum Zugriff auf und zum Konfigurieren von Datenmustern finden Sie unter Konfigurieren Sie Muster Datenerkennung ..

Hinweis:
Im Abschnitt „ **Aktive** Datenmuster“ werden nur aktive Muster angezeigt. Inaktive Muster werden nicht angezeigt.

Zieltabellen

Im Abschnitt „ **Zieltabellen** “ werden alle Tabellen aufgelistet, die für einen Auftrag verarbeitet werden können. Um auf die Zieltabellen zuzugreifen, wählen Sie **Zieltabellen**aus.

Die folgenden Tabellen werden nicht unterstützt:

- sr
- sysx
- v
- sh$
- syslog
- UA
- Nutzungsanalysen
- ECC
- Klon
- jrobin
- pa
- sla_repair_log
- -Scan
- gcf
- fm_log
- Protokoll
- np$
- sn_data_discovery
- dp_configuration
- dp_federated_job
- dp_field_technique
- dp_job
- dp_job_summary
- dp_primär_referenz
- dp_technik
- data_classification
- m2m_dictionary_dataclass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen Datenerkennung -Job

Konfigurieren Sie eine Datenerkennung -Aufgabe, und überprüfen Sie den Status der laufenden Aufgaben. Ein Datenerkennung -Job definiert, wann ein Muster für eine Zieltabelle ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: data_discovery_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Daten-Discovery-Auftrag**.
2. Wählen Sie in der Liste Datenerkennung Jobs die Option **Neu**aus.
3. Füllen Sie die Felder im Formular Datenerkennung „ Auftragsfelder“ aus.

Datenerkennung Auftragsfelder

Feld	Beschreibung
Name	Name des Jobs
Beschreibung	Beschreibung der Aufgabe.
Scantyp	Anzahl der zu scannenden Einträge. Mögliche Status: ○ **Beispiel**: Scannt 10.000 Einträge. ○ **Vollständig**: Scannt alle Einträge.
Kontext	Auftragsdetails zu gescannten Mustern, Treffern in Zieltabelleneinträgen und verstrichene Zeit.
Status	Status des Auftrags Datenerkennung. Mögliche Status: ○ **Bereit für Zeitplan**: Standardstatus für neue Aufträge. ○ **Geplant**: Die Ausführung der Aufgabe ist geplant. ○ **In Bearbeitung**: Auftrag wird aktiv ausgeführt. ○ **Abgeschlossen**: Auftrag wurde erfolgreich ausgeführt. ○ **Fehler**: Die Ausführung des Auftrags wurde aufgrund eines Fehlers beendet. ○ **Abgebrochen**: Der Auftrag wurde abgebrochen. ○ **Angehalten**: Die Aufgabe wurde angehalten.
Zusammenfassung	Zeigt die Ergebnisse des Jobs an, nachdem Sie ihn ausgeführt haben.
Startdatum	Legt das Startdatum für den Auftrag fest.
Zeitfensterstart	Der Beginn des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird nach der in diesem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Feld eingegebenen Zeit ausgeführt. Die im Feld **Zeitfensterstart** eingegebene Zeit muss vor der im Feld **Zeitfensterende** eingegebenen Zeit liegen. **Hinweis:** Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.
Zeitfensterende	Das Ende des Zeitfensters zum Ausführen dieser Aufgabe. Die Aufgabe wird bis zu dem in diesem Feld eingegebenen Zeitpunkt ausgeführt. Wenn die Aufgabe dieses Mal nicht abgeschlossen wurde, wird die Aufgabe angehalten und beim nächsten Start des Zeitfensters fortgesetzt. Die im Feld **Zeitfensterende** eingegebene Zeit muss nach der im Feld **Zeitfensterstart** eingegebenen Zeit liegen. **Hinweis:** Ein gültiger Zeitwert ist die koordinierte Weltzeit, basierend auf der 24-Stunden-Schreibweise.

4. Wählen Sie **Absenden**.
   Die Schaltflächen **Auftrag planen** und **Aktualisieren** werden angezeigt.
5. **Wählen** Sie Auftrag planen aus, um den Auftrag auszuführen.
   Die Aufgabe wird zwischen den in den Feldern **Start des Zeitfensters** und **Ende** des Zeitfensters ausgewählten Zeiten ausgeführt. Wenn die Aufgabe während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird die Aufgabe beim nächsten Start des Zeitfensters fortgesetzt.
6. **Wahlweise:** Wählen Sie eine der folgenden Funktionen aus:
   - Auftrag**abbrechen**: Bricht den Auftrag ab.
   - **Pause**: Hält den Auftrag an.
   - **Fortsetzen**: Startet einen angehaltenen Auftrag neu.

Konfigurieren Sie Muster Datenerkennung .

Konfigurieren Sie ein Datenerkennung -Muster, und überprüfen Sie die aktuellen Muster. Ein Datenerkennung -Muster definiert den regulären Ausdruck, der zum Abgleichen von Daten mit einer Zieltabelle verwendet wird.

Vorbereitungen

Erforderliche Rolle: data_discovery_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery** > **Alle Datenmuster**.
2. Wählen Sie in der Liste Datenerkennung Muster die Option **Neu**aus.
3. Füllen Sie die Felder im Formular Datenerkennung „ Auftragsfelder“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerkennung Auftragsfelder

Feld	Beschreibung
Interner Umfang	Umfang des Musters.
Beschreibung	Beschreibung der Aufgabe.
Name	Name des Datenmusters.
Anwendung	Anwendungsbereich des Musters.
Ausdruck	Regulärer Ausdruck, der zum Erkennen des Datenmusters verwendet wird.
Stichwort (optional)	Ein bestimmtes Wort (oder durch Komma getrennte Wörter), nach dem um einen Ausdruck gesucht werden soll. Muss mit **Stichwortnähe**verwendet werden **Hinweis:** Ein Stichwort kann verwendet werden, um nach zusätzlichem Kontext für ein Muster zu suchen. Beispielsweise kann die Verwendung von Stichwörtern helfen, zwischen einem Geburtsdatum und einem Einstellungsdatum zu unterscheiden, da sie dieselbe Formatierung MM/TT/JJ aufweisen.
Stichwortnähe (optional)	Wie weit vom Ausdruck entfernt, um nach Stichwörtern zu suchen. Muss mit **Stichwort**verwendet werden **Hinweis:** Der Standardwert ist 30, die Obergrenze ist 64

4. Wählen Sie **Absenden**.
   - Mit der Schaltfläche **Test** können Sie Ihren regulären Ausdruck testen, bevor Sie die Datenmusterliste absenden.

Das Datenmuster muss als aktiv festgelegt werden, damit es mit geplanten Aufgaben verwendet werden kann.

5. Navigieren zu **Systemsicherheit** > **Daten-Discovery** > **Aktive Datenmuster**.
6. Wählen Sie in der Liste Datenerkennung Aktives Muster die Option **Bearbeiten**aus.
7. Wählen Sie die Musterliste unter **Verfügbare Listen** aus, und verschieben Sie sie nach **Ausgewählte Listen**.

Standarddatenmuster

Überprüfen Sie die regulären Ausdrücke für Standarddatenmuster, die in Datenerkennungenthalten sind. Diese Standarddatenmuster können verwendet werden, um Tabelleneinträge für eine weitere Klassifizierung zu filtern.

Die folgenden Standardmuster sind für die Datenerkennung verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Regulärer Ausdruck
Kreditkarte: Visa	\b4[0-9]{12}(?:[0-9]{3})?\b
Kreditkarte: American Express	\b3[47][0-9]{13}\b
Kreditkarte: Mastercard	\b(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}\b
Kreditkarte: „Diners Club“.	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b
Kreditkarte: Erkennen	\b6(?:011|5[0-9]{2})[0-9]{12}\b
Sozialversicherungsnummer	\b(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4}\b
E-Mail	\b[\w!#$%&'*+/=?`{\|}~^-]+(?:\.[\w!#$%&'*+/=?`{|}~^ -]+)*@(?:[a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}\b
USA: Telefonnummer	\b\(?([0-9]{3})\)?[-.]?([0-9]{3})[-.]?([0-9]{4})\b

Konfigurieren Sie die Zieltabelle Datenerkennung .

Fügen Sie Zieltabellen hinzu, die in Datenerkennung -Jobs verwendet werden sollen. Nur Zieltabellen werden nach Datenmustern durchsucht.

Vorbereitungen
Erforderliche Rolle: data_discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Job Datenerkennung ausgeführt wird, wird er für alle Zieltabellen mit allen aktiven Mustern ausgeführt.

Prozedur

1. Auswahlvorgang **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Zieltabellen**.
2. Wählen Sie **Neu**.
3. Wählen Sie Ihre Zieltabelle im Feld **Tabellenname** aus.
4. Wählen Sie **Absenden**.

Datenerkennung Rollen

Sie können Datenerkennung Rollen zuweisen, um den Benutzerzugriff auf bestimmte Datentypen zu beschränken.

Daten-Discovery-Administrator [sn_data_discovery.data_discovery_admin]

Datenmuster und zugehörige Aufgaben anzeigen, erstellen und ändern.

- Datenmuster:
  - Erstellen
  - Lesen
  - Aktualisieren
  - Löschen
- Aktive Datenmuster:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Löschen
- Lesen

- Aufträge:
  - Erstellen
  - Lesen
  - Aktualisieren
  - Löschen
  - Zeitplan
  - Pausierung
  - Fortfahren
  - Abbrechen
- Zieltabellen:
  - Erstellen
  - Lesen
  - Schreiben

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

- data_classification_auditor
- data_classification_admin
- sn_data_discovery.data_discovery_api_processor

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Administratoren wird diese Rolle bei der Produktinstallation automatisch zugewiesen.

Hinweis:
Vermeiden Sie es, eine Administratorrolle zu gewähren, wenn spezialisiertere Rollen verfügbar sind.

Daten-Discovery-Auditor [sn_data_discovery.data_discovery_auditor]

Lesen Sie Datenmuster und Zieltabellen.

- Datenmuster lesen
- Lesen Sie aktive Datenmuster
- Lesen Sie Datenerkennung Aufträge
- Zieltabellen lesen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enthält die Rollen

Liste der in der Rolle enthaltenen Rollen.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Datenklassifizierungsadministrator [data_classification_admin]

Lesen Sie Datenmuster, Erkennungsaufgaben und die Tabelle „data_classification“, wenn eine aktivierte spezifische Mustersuche klassifiziert wird.

Enthält die Rollen

Die Datenklassifizierungsrolle enthält die Liste der Rollen, die in der Rolle „data_classification_auditor“ enthalten sind.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Hinweis:
Weitere Informationen zur Administratorrolle für die Datenklassifizierung finden Sie unter Demodaten des Plugins Data Classification werden installiert.

Datenerkennung Auftragsergebnisse

Die Seite Datenerkennung „ Ergebnisse“ zeigt Details zu den von einem Job gefundenen Daten. Sie können die Seite „Ergebnisse“ verwenden, um die Ergebnisse einer Aufgabe zu überprüfen und mit der Klassifizierung von Daten zu beginnen.

Auf der Seite Datenerkennung „ Ergebnisse“ werden nach Abschluss der Aufgabe die folgenden Details angezeigt.

Spalte	Beschreibung
Wörterbucheintrag	Spalte der Zieltabelle, in der sich die Daten befanden
Tabelle	Zieltabelle, in der die Daten gefunden wurden
Datenmuster	Datenmuster, das zum Suchen der Daten verwendet wird
Anzahl der Übereinstimmungen von Datenmustern	Anzahl der Dateneinträge, die dem Datenmuster entsprechen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Gesamtanzahl der Zeilenscans	Anzahl der während der Aufgabe gescannten Zeilen
Prozentsatz der übereinstimmenden Zeilen	Prozentsatz der Zeilen in der Zieltabelle, die dem Datenmuster entsprechen
Datenerkennung Auftrag	Auftrag, der in der Zieltabelle verwendet wird
Status	Status des Eintrags

Nachdem Sie einen Datenerkennung -Job ausgeführt haben, haben die Ergebnisse den Status Neu. Wenn keine Aktion erforderlich ist, können Sie die Daten unverändert lassen, wodurch der Status automatisch auf Ignoriert gesetzt wird. Andernfalls können Sie die Daten klassifizieren, indem Sie z. B. benutzerdefinierte Datenklassifizierungen erstellen, um die Datenanonymisierung mit dem Tool Data Classification vorzubereiten.

Konsolidieren Sie die Ergebnisse

Auftragsergebnisse können mit der Schaltfläche Ergebnisse konsolidieren **konsolidiert** werden. Auftragsergebnisse, die von zwei separaten Aufträgen gemeinsam verwendet werden, werden dann unter dem zuletzt ausgeführten Auftrag konsolidiert.

Hinweis:
Nur abgeschlossene vollständige Scan-Aufträge können konsolidiert werden

Klassifizieren Sie Daten auf der Ergebnisseite des Auftrags Datenerkennung .

Klassifizieren Sie Daten in Datenerkennung direkt von der Ergebnisseite eines Auftrags aus.

Vorbereitungen
Erforderliche Rolle: data_discovery_admin und admin

Eine Aufgabe muss eine erfolgreiche Ausführung abschließen, bevor Ergebnisdaten als klassifiziert angezeigt werden können.

Prozedur

1. Gehe zu **Systemsicherheit** > **Daten-Discovery** > **Daten-Discovery-Auftrag**.
2. Wählen Sie den Eintrag aus, den Sie klassifizieren möchten.
3. Wählen Sie in der Liste Datenerkennung Ergebnisse die **Option Klassifizieren**aus.
4. Wählen Sie die Datenklassifizierungen aus, die Sie den Tabelleneinträgen zuordnen möchten.
5. Wählen Sie **Klassifizieren aus**.

Daten-Discovery-API

Referenz für Daten-Discovery-API

DataPatternValidator – match(String pattern, String input)

Validiert, ob die Eingabe mit dem Muster des regulären Ausdrucks (regulärer Ausdruck) übereinstimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
pattern	Zeichenfolge	Das Muster des regulären Ausdrucks
Eingabe	Zeichenfolge	Die abzugleichenden Eingabedaten

Ergebnisse

Typ	Beschreibung
Boolean	Gibt „true“ zurück, wenn die Eingabe mit dem Muster übereinstimmt, andernfalls „false“.

Example: Code-Beispiel

```
var datapatternValidatorApi = new sn_data_discovery_api.DataPatternValidator();
var pattern = '\\b[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\\b';
var input = '09/09/2023';
var output = datapatternValidatorApi.matches(pattern, input);
if (output) {
  gs.info('pattern found!');
} else {
  gs.info('pattern not found');
}
```

DataPatternValidator – isValid(String pattern)

Überprüft, ob das angegebene Muster ein gültiger regulärer Ausdruck ist.

Parameter

Name	Typ	Beschreibung
pattern	Zeichenfolge	Das Muster des regulären Ausdrucks

Ergebnisse

Typ	Beschreibung
Boolean	Gibt „true“ zurück, wenn der Ausdruck ein gültiger regulärer Ausdruck ist, andernfalls „false“.

Example: Code-Beispiel

```
var datapatternValidatorApi = new sn_data_discovery_api.DataPatternValidator();
var pattern = '\\b[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\\b';
var output = datapatternValidatorApi.isValid(pattern);
if (output) {
 gs.info('pattern is valid!');
} else {
  gs.info('pattern is not valid');
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DataPatternValidator – passwordMatches(String pattern, String input, String stichwörter, int stichwortProximity)

Validiert, ob die angegebenen Eingabedaten mit dem Muster des regulären Ausdrucks (regulärer Ausdruck) zusammen mit den Stichwörtern übereinstimmen. Weitere Informationen zu Stichwörtern und Stichwortnähe finden Sie unter Konfigurieren Sie Muster Datenerkennung ..

Parameter

Name	Typ	Beschreibung
pattern	Zeichenfolge	Das Muster des regulären Ausdrucks
Eingabe	Zeichenfolge	Die abzugleichenden Eingabedaten
Stichwörter	Zeichenfolge	Kommagetrennte Stichwortwerte, die abgeglichen werden sollen
StichwortProximity	int	Die Nähe des Stichworts aus dem übereinstimmenden Muster

Ergebnisse

Typ	Beschreibung
Boolean	Gibt „true“ zurück, wenn der Ausdruck ein gültiger regulärer Ausdruck ist, andernfalls „false“.

Example: Code-Beispiel

```
var datapatternValidatorApi = new sn_data_discovery_api.DataPatternValidator();
var pattern = '\\b[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\\b';
var keywords = 'dob,date of birth';
var keywordProximity = 20;
var matchInput = 'dob: 09/09/2023';
var noMatchInput = '09/09/2023';
var output = datapatternValidatorApi.keywordMatches(pattern, matchInput, keywords,
 keywordProximity);
gs.info('match found for input: ' + matchInput + ' = ' + output);
output = datapatternValidatorApi.keywordMatches(pattern, noMatchInput, keywords,
 keywordProximity);
gs.info('match found for noMatchInput: ' + noMatchInput + ' = ' + output);
```

DataPatternScanner – scan(String input)

Hinweis:
Dem DataPatternScanner-Konstruktor muss ein Array von Datenmuster-System-IDs übergeben werden.

Parameter

Name	Typ	Beschreibung
Eingabe	Zeichenfolge	Die zu scannenden Eingabedaten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Serialisierte JSON-Zeichenfolge hasMatches Gibt „true“ zurück, wenn mindestens 1 Musterübereinstimmung vorhanden ist. "finding" : [{ # für jedes Muster mit Übereinstimmung, enthält Liste der Start- und Endpositionen von Übereinstimmungen. Fehler Enthält einen Fehlercode und eine Meldung, wenn die API fehlgeschlagen ist, andernfalls leer. unprocessedPatterns Gibt ein Array von Datenmuster-Sys-IDs zurück, die nicht verarbeitet wurden Suche Gibt die ID jedes Musters und eine Liste der Start- und Endpositionen der Übereinstimmungen zurück.

Example: Code-Beispiel

```
var emailSysId = '8e5605bceb0561107977d256385228e6';
var ssnSysId = '4964417ceb0561107977d256385228b8';
var dataPatternSysIds = [emailSysId, ssnSysId] // Email and SSN
var dataDiscoveryApi = new sn_data_discovery_api.DataDiscoveryScanner(dataPatternSysIds);

var input = 'my ssn is 123-45-6789 and email is abcd@company.com'
var jsonString = dataDiscoveryApi.scan(input);
var output = JSON.parse(jsonString);

if (output.hasMatches) {
  gs.info('found matches for patterns in input');
  for (var i=0; i<output.finding.length; i++) {
      curFinding = output.finding[i];
      gs.info('first match for ' + curFinding.pattern + ' is (' + curFinding.matches[0]['start'] + ','
 + + curFinding.matches[0]['end'] + ')');
  }
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration

Name	Konfigurationsmodus	Beschreibung
Maximale Länge der Stichwortzeichenfolge (CSV).	Kann nicht konfiguriert werden	Definiert die maximale Länge der Zeichenfolge, die im Feld „DataPattern.keyword“ konfiguriert werden kann • Der Standardwert ist 128 • Der Höchstwert beträgt 128
Mindest- und Höchstwert für Stichwortnähe	Kann nicht konfiguriert werden	Definiert den minimalen und maximalen Wert, der in das Feld DataPattern.keyword_proximity eingegeben werden kann. • Mindestens 0 • Maximal 64
Maximale Eingabegröße für Übereinstimmungen und „keywordMatches“-API	Kann nicht konfiguriert werden	Definiert die maximale Eingabegröße, die von den APIs „DataPatternValidator.matches“ und „DataPatternValidator.keywordMatches“ unterstützt wird • Der Standardwert ist 2048 • Der Höchstwert beträgt 2048
Zeitüberschreitung für Scan-API	DataDiscoveryScanner.setScanTimeout (lange Zeitüberschreitung Millis)	API-Aufruf, um die maximale Zeit in Millisekunden für den Abschluss der DataDiscoveryScanner.scan-Aufrufe zu definieren. • Der Standardwert ist 20.000 (ms). • Bereich ist ein ganzzahliger Wert zwischen 0 und 50000 (ms).

Domänentrennung für Service Provider

Mit der ServiceNow Platform können Service Provider (SPs) ihren Kunden ein schnelleres Onboarding bieten, die Compliance erfüllen und ihre Daten durch Domänentrennung schützen. Sie können Client-Daten, Prozesse und Berichte in logische Gruppierungen unterteilen, die als Domänen bezeichnet werden. SPs steuern, wer welche Inhalte sieht und darauf zugreifen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Erfahren Sie mehr über die Domänentrennung.

Konfigurieren

Konfigurieren Sie die Domänentrennung.

Referenz

Ruft Details zur Domänentrennung ab.

Analysieren

Erfahren Sie mehr über die Analyse der Domänentrennung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung erkunden

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logisch definierte Domänen unterteilen.

Die Domänentrennung ist am besten geeignet für Kunden, die:

- absolute Datentrennung zwischen Business-Entitäten (Datentrennung) benötigen.
- Geschäftsprozessdefinitionen und Benutzerschnittstellen für jede Domäne anpassen möchten (delegierte Verwaltung).
- einige globale Prozesse und globale Berichte in einer einzigen Instanz verwalten.
- Trennen Sie Daten zwischen Service Providern, Kunden, Partnern oder Unterorganisationen.
- Geringfügige oder moderate Prozessunterschiede zwischen Kunden aufweisen.

Domänentrennung im Vergleich zu separaten Instanzen

Die Domänentrennung bietet zwar Unterstützung für mehrere Mandanten, die Mehrmandantenfähigkeit ist jedoch auch weiterhin in einer einzelnen Instanz enthalten. Einige globale Eigenschaften, Daten und Prozesse werden über alle Domänen hinweg gemeinsam genutzt. Zum Beispiel ist die Angabe des Benutzernamens auf der *Anmeldeseite* des Systems global und kann nicht pro Domäne angegeben werden.

Wenn Sie eine vollständige Trennung aller Systemeigenschaften benötigen und keine globalen Berichte oder globalen Prozesse benötigen, sind separate Instanzen die beste Option.

Datentrennung

Mitglieder einer Domäne sehen nur die Daten, die in ihrer Domäne oder den untergeordneten Domänen enthalten sind, die sich in der Domänenhierarchie niedriger befinden. Standardmäßig sind alle Benutzer und alle Datensätze Mitglieder der globalen Domäne, es sei denn, ein Administrator weist sie einer bestimmten Domäne zu. Sobald Sie einer Domäne einen Benutzer oder einen Datensatz zugewiesen haben, vergleicht die Instanz die Domäne des Benutzers mit der Domäne des Datensatzes, um zu bestimmen, ob der Benutzer den Datensatz aufrufen kann.

ServiceNow-Anwendungen werden mit den folgenden inkrementellen Supportstufen definiert. Diese Ebenen basieren auf der Perspektive der tatsächlichen Anwendungsfälle und Personas.

Datentrennung: Mandanten sehen nur Daten, für die sie über Berechtigungen verfügen. Mandanten können Zugriff auf andere Mandantendaten erhalten, können jedoch keine Mandantendaten abfragen, wenn sie keinen Zugriff haben.

UI-Trennung: Unterstützt eine mandantenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.

Geschäftslogiktrennung: Sie können mandantenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Business Rules, Client-Skripts, UI-Richtlinien und UI-Aktionen erstellen.

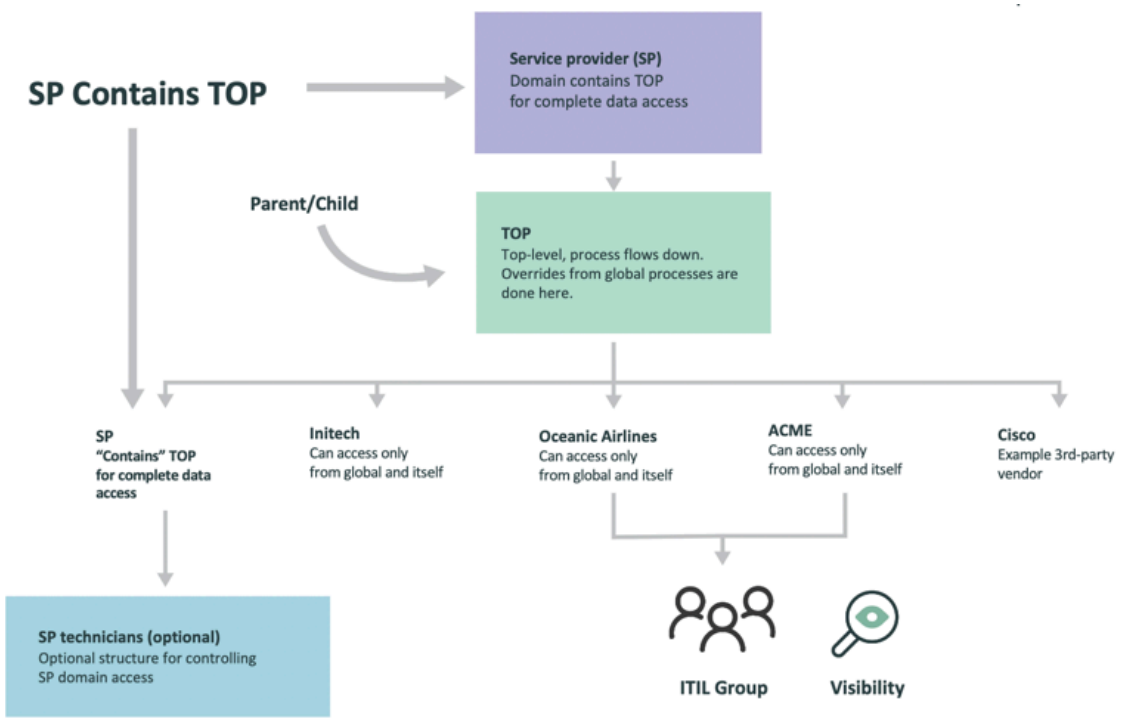
Hierarchische Modellierung: Geschachtelte Mehrmandantenfähigkeit, sodass übergeordnete Mandanten auf untergeordnete Mandantenressourcen zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Geschäftslogik für übergeordnete Mandanten wird automatisch für untergeordnete Mandanten ausgeführt und kann auf jeder Ebene überschrieben werden.

Cross-Mandanten-Intelligenz (Domänenbereich): Verarbeitet automatisch die Daten, Metadaten, Geschäftslogik und den Verarbeitungskontext für Mandanten, die Zugriff auf zusätzliche Mandantendaten haben.

Im Allgemeinen sind Daten, die auf einer höheren Ebene in der Domänenhierarchie definiert sind, auf niedrigeren Ebenen der Hierarchie nicht sichtbar.



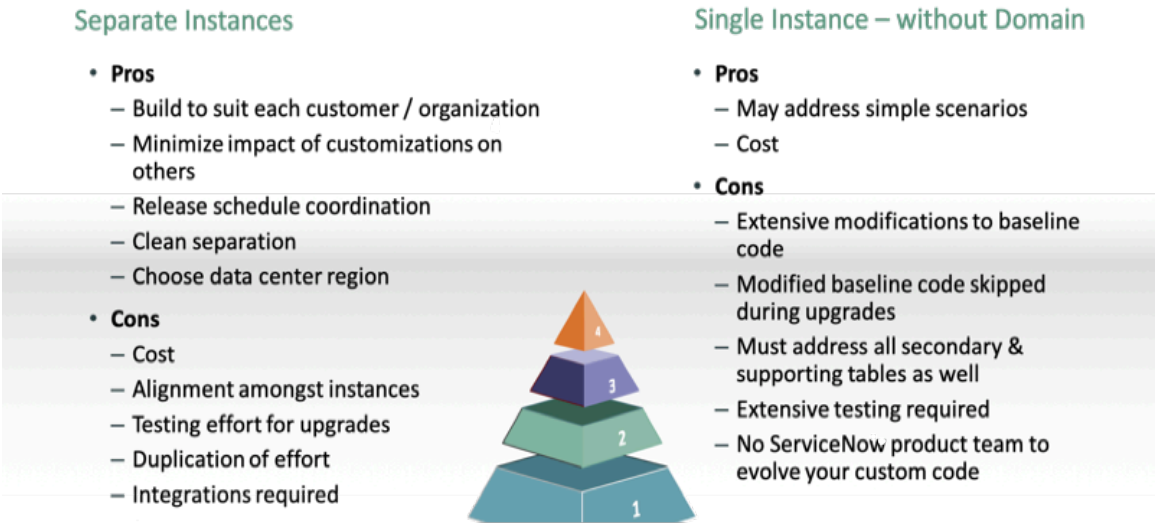
Domänenpfadmigration

Domänenpfade werden für alle Kunden verwendet. Domänennummerierung wird nicht verwendet. Kundenservice und Support kann beim Upgrade helfen.

Alternativen zur Domänentrennung

Separate Instanzen sind eine gängige Alternative zur Domänentrennung. Dies bietet ein hohes Maß an Flexibilität bei der Erfüllung der Anforderungen für Kunden und Stakeholder mit geringen oder gar keinen Auswirkungen auf andere.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



⚠ Warnung:
Wenden Sie sich vor der Aktivierung der Domänentrennung an Ihren -Mitarbeiter, um sicherzustellen, dass sie für Ihre Umgebung geeignet ist. Die Domänentrennung erhöht den Verwaltungsaufwand. Sie kann zwar deaktiviert, aber nicht aus einer Instanz entfernt werden.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Plugin für Domänentrennung

Konfiguration, die an interne oder externe Kunden delegiert werden kann

DieDomänentrennung soll ServiceNow® Service Providern (SPs) die Möglichkeit geben, die Services zu konfigurieren, die sie ihren Kunden anbieten. Es ist nicht so konzipiert, dass Kunden von diese Services selbst verwalten können, mit Ausnahme einiger Bereiche, auf die in diesem Thema näher eingegangen wird.

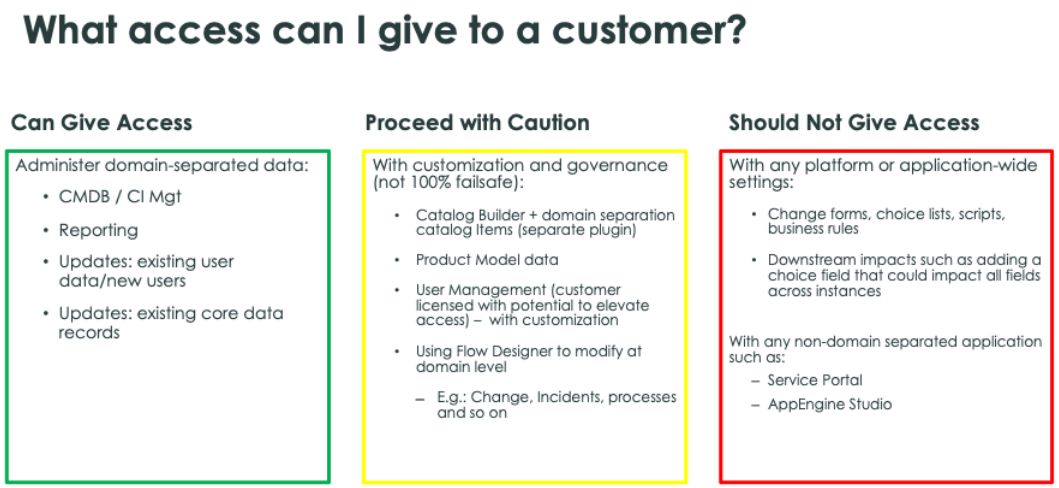
Übersicht

Für SP-Kunden ist es sicher, Daten in ihrer Domäne selbst zu verwalten, die sich nicht auf die Lizenzierung oder andere Kunden auswirken. Beispielsweise ist es für einen Kunden sicher, neue Berichte zu erstellen oder Konfigurationselemente zu verwalten, aber es ist nicht sicher, Felder, Auswahlmöglichkeiten, Geschäftsregeln und andere Prozesse anzupassen, bei denen dies Auswirkungen auf andere Kunden in derselben Instanz haben kann.

Die administrativen Rollen des [ServiceNow -Basissystems und ihre Zugriffskontrollen auf der ServiceNow -Plattform sind für ein einzelnes Administratorteam pro Instanz konzipiert. Beispielsweise wird die Rolle „domain_admin“ einer der SP-Ressourcen zugewiesen, um alle Domäneneinstellungen für die Instanz zu verwalten und neue Domänen zu erstellen. Für alle domänenspezifischen Administratoraufgaben sollte der SP nach Bedarf neue „Kundenadministrator“-Rollen und Zugriffskontrollen erstellen, um seinen Kunden bestimmten Zugriff zu gewähren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt eine Übersicht über allgemeine Administratorfunktionen in verschiedenen Kategorien, die für einen Kunden sicher sind.



Kann Zugriff gewähren

Beispiele:

- CI-Datenverwaltung in der CMDB
- Berichterstellung
- Aktualisiert vorhandene Benutzerdaten oder neue Benutzer ohne Rollen
- Aktualisierung vorhandener Kerndatensätze wie Abteilung, Gruppe, Standort, Kostenstelle oder neue Gruppen ohne Rollen und neue Abteilungen/Kostenstellen/ Standorte.

Fahren Sie mit Vorsicht fort

Beispiele:

- Katalogelemente: Um kundenspezifische Katalogelemente zu erstellen, die vom Kunden aktualisiert werden können, können zwei Fähigkeiten zusammen verwendet werden: Die Domänentrennung für Katalogelemente (Domänentrennung und Service Catalog) ermöglicht es dem Instanzbesitzer, Elemente in der Domäne des Kunden zu erstellen. Der Instanzbesitzer kann eine Rolle erstellen, damit Kunden sichere Felder wie Preis, Beschreibung und Bilder aktualisieren können. Der Katalog-Generator (neu im Quebec-Release) gibt dem SP-Administratorteam die Möglichkeit, Elementvorlagen zu erstellen, die sicher an Kunden verteilt werden können, um innerhalb einer verbindlichen UI-Experience neue Elemente in ihrer Domäne zu erstellen.
- Benutzer-/Gruppenverwaltung: Es ist sicher, eine „Kundenadministrator“-Rolle zu erstellen, die Benutzerdatensätze erstellen und ändern kann, aber das Hinzufügen und Entfernen von Rollen kann sich auf Sicherheit und Lizenzierung auswirken. Im Basissystem gibt es keine Möglichkeit, Rollen zu unterteilen, die für einen Kunden sicher sind. Dasselbe gilt für die Erstellung und Änderung von Gruppen. Während die Gruppe selbst geändert werden kann, sollte das Hinzufügen oder Entfernen von Rollen kontrolliert werden.
- Flow Designer : ServiceNow Flow Designer ist das Erstellungstool zum Erstellen von Prozessen (Workflows) für Tabellen. Die Rolle „flow_designer“ ermöglicht Kunden den skriptfreien Zugriff auf Build-Flows. Sie können jeden Flow in Domänen über ihnen in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hierarchie lesen und klonen. Sie können Flows in ihrer Domäne erstellen und ändern. Dies kann jedoch nicht in einem Silos geschehen. Jeder, der den Prozess beeinflussen kann, muss dem globalen Administratorteam für Governance hinzugefügt werden, damit sich Prozesse nicht gegenseitig aufheben oder andere Konflikte verursachen.

Keinen Zugriff gewähren

Zu verstehen, wie Auswahlfelder funktionieren, ist hilfreich, um zu verstehen, warum sie nur vom SP-Administratorteam verwaltet werden sollten.

- Struktur eines Auswahlfelds: Auswahlfeldwerte werden in der Tabelle „sys_choice“ gespeichert und basierend auf folgenden Kriterien gruppiert: Tabelle, Domäne und Sprache.

  Beispielsweise ist das **Feld** Status in einer Aufgabe für jede Tabelle verfügbar, die eine Aufgabe erweitert. Das bedeutet, dass jede Tabelle eigene Werte haben kann, diese Werte mit der Domäne multipliziert werden können und die Domänenwerte mit der Sprache multipliziert werden können.

  Alle Werte für **Status** in allen Tabellen, Domänen und Sprachen werden als Werte für das **Feld** Status betrachtet.

- Funktionsweise von Änderungen an Auswahlfeldern: Wenn ein Auswahlfeld aktualisiert wird, wird eine Nutzlast mit allen Werten für dieses Feld (Tabellen, Domänen, Sprachen) erstellt. Wenn Sie diese Nutzlast in einer Instanz installieren, werden alle vorhandenen Werte für das Feld gelöscht und die neuen Werte geladen. Dadurch wird sichergestellt, dass keine doppelten Einträge oder verbleibenden Werte vorhanden sind, die nicht mehr gültig sind.

  Aus diesem Grund ist es unmöglich, einem Kunden in einer domänengetrennten Instanz die Möglichkeit zu geben, Auswahlfelder direkt zu aktualisieren, da dies Auswirkungen auf die gesamte Instanz haben würde. Darüber hinaus können Sie Auswahlmöglichkeiten nicht direkt in einer Produktionsinstanz aktualisieren, da alle importierten Update Sets, die sich auf dieses Feld auswirken, die vorhandenen Auswahlmöglichkeiten überschreiben würden. In einigen Fällen können Auswahlfelder Prozesse selbst steuern, die unterbrochen würden, wenn ein Kunde diese Felder ändern würde.

Weitere Informationen finden Sie unter:

- Exploring user administration
- Eine ACL-Regel erstellen
- Service Provider-Lernpfad auf ServiceNow University
- Domänentrennung für Service Provider
- Service Provider-Konzepte
- Anwendungssupport für Domänentrennung
- Versionshinweise zur Domänentrennung

Domänenzuweisung

Standardmäßig wird durch die Domänentrennung ein Domänenfeld zu Tabellen und ihren Erweiterungen hinzugefügt.

Sie können die Domänentrennung auch auf neu erstellte Tabellen ausweiten, indem Sie der Wörterbuchdefinition der Tabelle ein **sys_domain** -Feld hinzufügen. Standardmäßig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

trennt das System nur Plattform- und Baselineanwendungstabellen nach Domäne, sofern angemessen.

> **⚠ Warnung:**
> ServiceNow empfiehlt keine Domänentrennung von Plattformtabellen (alle Tabellen mit dem Präfix sys_, z. B. die Tabellen „Wörterbucheintrag“ [sys_dictionary] und „Überschreibung des Wörterbucheintrags“ [sys_dictionary_override]), da dies zu unerwarteten Ergebnissen führen kann.

Jedem Datensatz ist eine einzelne Domäne zugewiesen.Diese Domäne wird im Feld **sys_domain**gespeichert.Mehrere Tabellen haben standardmäßig die Spalte **sys_domain** und sind bereits domänengetrennt.

Der Wert des **Felds sys_domain** enthält die Domäne, die dem Datensatz von einem der folgenden Elemente zugewiesen wurde:

- Unternehmen, zu dem der Benutzer gehört
- Geschäftsregel beim Erstellen des Datensatzes
- Beim Erstellen des Datensatzes verwendetes Modul
- Formularvorlage, die beim Erstellen des Datensatzes verwendet wird
- Domäne des übergeordneten Datensatzes
- Domäne, die dem Benutzerdatensatz zugewiesen ist
- Domäne des Benutzers, der sie erstellt

Das System verhindert, dass die folgenden Tabellen nach Domänen getrennt werden:

- Zugriffssteuerung [sys_security_acl]
- Skripteinbindung [sys_script_include]
- Systemeigenschaft [sys_properties]
- Entitäten der Sicherheitsausschluss-/ -aufnahmeliste [sys_security_restricted_list]
- Dictionary-Eintrag [sys_dictionary]
- Überschreibung von Wörterbucheinträgen [sys_dictionary_override]

Zuweisen von Benutzern zu Unternehmen

Administratoren können Benutzer schnell einer Domäne zuweisen, indem sie sie einem Unternehmen zuweisen. Nachdem Benutzer einer Domäne zugewiesen wurden, erben Datensätze automatisch die Domäne des Benutzers.

Wenn Sie beispielsweise Bow Runneri dem ACME-Unternehmen zuweisen, wird er automatisch der ACME-Domäne zugewiesen. Wenn Sie Don Goodliffe dem Unternehmen Initech zuweisen, wird er automatisch der Domäne Initech zugewiesen. Alle von ihnen erstellten Datensätze werden automatisch der entsprechenden Domäne hinzugefügt.

Verwenden von Geschäftsregeln zum Zuweisen von Domänen

Administratoren können eine Geschäftsregel verwenden, um beim Erstellen eines Datensatzes automatisch einen Domänenwert festzulegen. Die Geschäftsregel muss einen Wert im Feld **sys_domain festlegen**. Administratoren müssen sicherstellen, dass für die Tabelle des Datensatzes eine **sys_domain-** Spalte verfügbar ist. Siehe Empfohlene Domain Separation-Verfahren für Service Provider für weitere Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden von -Modulen zum Zuweisen von Domänen

Administratoren können den URL-Parameter **sysparm_domain** verwenden, um neue Datensätze aus einem Modul automatisch einer bestimmten Domäne zuzuweisen. Administratoren müssen ein Modul mit dem folgenden **Argumentwert** erstellen: sysparm_domain=sys_ID of domain.

Verwenden von Formularvorlagen zum Zuweisen von Domänen

Administratoren können eine Formularvorlage verwenden, um neue Datensätze automatisch einer bestimmten Domäne zuzuweisen. Administratoren müssen dem Formular das Feld **sys_domain** hinzufügen und einen Domänenwert auswählen. Wenn Sie beispielsweise das Feld **sys_domain** auf die **TOP/ACME-Domäne** festlegen, werden alle Datensätze aus dieser Vorlage automatisch der TOP/ACME-Domäne zugewiesen.

Domänenvererbung für Tabellen

Standardmäßig erben zugehörige Datensätze die Domäne des übergeordneten Datensatzes. Beispiel:

- Ein Change-Aufgabendatensatz erbt die Domäne des übergeordneten Change Request-Datensatzes.
- Ein Problemdatensatz erbt die Domäne des übergeordneten Incident-Datensatzes.

Automatische Domänenzuweisung basierend auf Benutzerdomänen

Wenn keine anderen Domänenbedingungen gelten, erbt ein Datensatz automatisch die Domäne des Benutzers, der ihn erstellt.

Sichtbarkeitsdomänen und Enthält Domänen

Sichtbarkeitsdomänen steuern, was ein bestimmter Benutzer oder eine Gruppe von Benutzern sehen kann. „Enthält“-Domänen steuern, was eine ganze Domäne von Benutzern sehen kann.

Sichtbarkeitsdomänen

Das Element „Sichtbarkeitsdomänen“ bestimmt, ob Benutzer aus einer Domäne auf Datensätze aus einer anderen Domäne zugreifen können. Ordnen Sie dieses Element den Datensätzen „Benutzer“ [sys_user] und „Gruppe“ [sys_user_group] in zugehörigen Listen für diese Datensätze zu. Gruppen gewähren ihren Mitgliedern die Sichtbarkeitsdomänen der Gruppe. Wenn ein Benutzer eine Gruppe verlässt, verliert er die Sichtbarkeitsdomänen der Gruppe. Durch die Gewährung einer Sichtbarkeitsdomäne werden Benutzern alle Rechte für die Datensätze in dieser Domäne basierend auf ACL-Regeln (Zugriffssteuerungsliste) gewährt.

Eine Sichtbarkeitsdomäne:

- Ist eine Benutzer-zu-Domäne-Beziehung und wird explizit gewährt.
- Ist keine untergeordnete Domäne.
- Wird nicht durch die Auswahl in der Domänenauswahl gesteuert. Benutzer mit Zugriff auf eine Sichtbarkeitsdomäne sehen immer Daten in dieser Domäne und ihren untergeordneten Domänen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Eine übermäßige Verwendung von Sichtbarkeitsdomänen wird nicht empfohlen. Obwohl Transparenz eine Methode ist, um Benutzern den Zugriff auf Datensätze zu ermöglichen, ist es am besten, Domänen enthält für eine robustere Steuerung zu verwenden.

Enthält Domänen

Normalerweise definieren Übergeordnet-Untergeordnet-Beziehungen die Domänenhierarchie. Mit einer Domäne vom Typ „Enthält“ können Sie Domänen nach Bedarf verknüpfen, unabhängig von Beziehungen zwischen über- und untergeordneten Elementen. Enthält jedoch Domänen, gewähren nur Sichtbarkeit für Domänendaten. Prozesse bleiben von Beziehungen des Typs „Enthält“ unberührt.

Eine enthält Domäne:

- Ist eine Viele-zu-Viele-Domäne-zu-Domäne-Beziehung.
- Kann untergeordnete Domänen haben. Wenn eine Domäne ausgewählt ist, können Sie die Daten dieser Domäne und ihrer untergeordneten Elemente anzeigen.
- Wird durch die Auswahl in der Domänenauswahl gesteuert.

Hinweis:
Wenn Sie den Domänendatensatz öffnen, wird der Bereich auf die Domäne dieses Datensatzes festgelegt, sodass Sie nur untergeordnete Domänen sehen können. Wählen Sie im Menü die Option **Toggle Domain Scope** (Domänenbereich umschalten) aus, um die zugehörige Liste auszufüllen.

Enthält Domänenbeispiel

Wenn die Stammdomäne eines Benutzers A ist und die Domäne A die Domänen B und C enthält, werden sie alle zu Peer-Domänen. Das bedeutet, dass der Benutzer Daten aus den Domänen A, B und C sieht, während er sich in seiner Stammdomäne A befindet. Wenn Benutzer die Domäne mit der Domänenauswahl in Domäne B ändern, sehen sie nur Daten in Domäne B. Wenn Benutzer mit einem Datensatz aus Domäne B interagieren oder Domäne C direkt, sehen sie nur Daten für diese Domäne.

Beispiel für die Sichtbarkeitsdomäne

Wenn sich bei Verwendung der Domänentransparenz Don Goodliffe in der Datenbankdomäne und Bogen-Ruggeri in der Netzwerkdomäne befindet und sich keine Incidents in der globalen Domäne befinden, kann Don aufgrund der Datentrennung nicht auf die Incidents von Bow zugreifen.

Sichtbarkeitsdomänen werden basierend auf der Gruppenmitgliedschaft geerbt

Wenn Sie die Domänentabelle auf die Gruppentabelle [sys_user_group] festlegen, können Benutzer Sichtbarkeitsdomänen basierend auf ihrer Gruppenmitgliedschaft erben.

Zugehörige Informationen

Enthält Abfragen und Domänenzugriff

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenbereich

Der Domänenbereich definiert, auf was Benutzer zugreifen können und auf was nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder Benutzer hat zwei Domänenbereiche, wenn er eine Sitzung in einer domänengetrennten Instanz herstellt.

- Der*Sitzungsbereich* wird beim Einrichten der Sitzung auf die Domäne festgelegt, die im Benutzerdatensatz des Benutzers aufgeführt ist. Benutzer können ihren Sitzungsdomänenbereich manuell über die Domänenauswahl ändern.
- Der*Datensatzbereich* verwendet die Domäne des Datensatzes und ist aktiv, wenn das Formular eines Datensatzes angezeigt wird.

Standardmäßig hat der Datensatzbereich Vorrang vor dem Sitzungsbereich, sodass Benutzer in übergeordneten Domänen die Daten- und Prozessbeschränkungen jedes Datensatzes einhalten können. Diese Benutzer können jedoch den Domänenumfang erweitern oder einklappen, um Daten aus anderen Domänen anzuzeigen oder auszublenden. Zum Beispiel hat ein Benutzer in der Service Provider-Domäne (SP) auch Einblick in untergeordnete Domänen wie die ACME-Domäne. Beim Anzeigen eines Incident-Datensatzes aus der ACME-Domäne kann der Benutzer den Domänenbereich erweitern, um Werte aus der SP-Domäne anzuzeigen, oder den Domänenbereich reduzieren, um nur Datensatzwerte anzuzeigen, die der ACME-Domäne des Datensatzes entsprechen.

Hinweis:
Benutzer haben immer Zugriff auf Daten aus Domänen, die ihnen durch die Domänensichtbarkeit explizit gewährt wurden.

Benutzer mit der Benutzerrolle „ **domain_expand_scope** “ können den Domänenbereich aus der UI-Aktion Domänenbereich umschalten im Formular auswählen. Wenn der Datensatzbereich aktiv ist, klicken Sie auf die UI-Aktion, um den Sitzungsbereich zu erweitern und alle Daten anzuzeigen, die basierend auf der Domäne des Benutzers und den untergeordneten Domänen verfügbar sind. Wenn der Sitzungsbereich aktiv ist, klicken Sie auf die UI-Aktion, um den Datensatzbereich zu reduzieren und nur Daten anzuzeigen, die der Domäne des aktuellen Datensatzes entsprechen.

Hinweis:
Ein Datensatz zeigt die UI-Aktion zum Umschalten des Domänenbereichs nicht an, wenn sich der Datensatz in der globalen Domäne befindet oder die Domäne des Benutzers mit der Domäne des Datensatzes übereinstimmt.

Datensatzwertauswahl aus anderen Domänen

Benutzer, die mehrere Domänen anzeigen können, haben die Möglichkeit, Datensatzwerte aus einer Domäne auszuwählen, die sich von der Domäne des Datensatzes unterscheidet.

Beispielsweise möchten Service Desk-Mitarbeiter, die für einen Service Provider arbeiten, bestimmte Incidents sich selbst zuweisen, um Probleme im Namen ihrer Kunden zu lösen. Wenn dies der Fall ist, kann das Incident-Feld **Zugewiesen an** einen Benutzer aus der SP-Domäne enthalten, obwohl der Incident-Datensatz selbst einer untergeordneten Domäne wie ACME zugeordnet ist.

Wenn Sie einen Datensatzwert aus einer anderen Domäne auswählen, wird die Domäne des Datensatzes nicht geändert. Der Datensatz behält seine ursprüngliche Domäne bei. Wenn ein Benutzer einen Datensatz mit Werten aus mehreren Domänen anzeigt, bestimmt die Sichtbarkeit der Domäne des Benutzers, was ihm angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatzwertauswahl

Wenn diese Bedingungen erfüllt sind	Der Benutzer hat Zugriff auf diese UI-Elemente
Der Benutzer hat Zugriff auf die Domäne des aktuellen Datensatzes, auf den in einem Feld verwiesen wird.	Der Benutzer kann: • Siehe Referenzfeld-Anzeigewert. Beispiel: Sie sehen den Benutzernamen im Feld **Zugewiesen an**. • Zeigen Sie den zugehörigen Datensatz über das Referenzsymbol an. Beispiel: Sie sehen den Benutzerdatensatz für den Benutzer im Feld **Zugewiesen an**. • Wählen Sie Werte aus einer beliebigen sichtbaren Domäne aus. Beispielsweise kann Benutzer aus der SP- und der ACME-Domäne auswählen.
Der Benutzer hat keinen Zugriff auf die Domäne des aktuellen Datensatzes, auf den in einem Feld verwiesen wird.	Der Benutzer kann: • Referenzfeld-Anzeigewerte werden nicht angezeigt. (Dies ist der Fall, wenn die Domänentrennung in Madrid oder späteren Releases aktiviert wurde und der Benutzer keinen Zugriff auf die Domäne dieses Datensatzes hat.) • Wählen Sie nur Werte aus der Domäne des Datensatzes aus. Beispielsweise kann nur Benutzer aus der ACME-Domäne auswählen.

Domänen und zugehörige Unternehmen

Mit der Domänentrennung können Sie Änderungen, die Sie an einem Unternehmensdatensatz vornehmen, in der Domäne und anderen dem Unternehmen zugeordneten Datensätzen kaskadieren.

Standardmäßig weist das System Benutzer automatisch derselben Domäne wie ihr Unternehmen zu. Beispielsweise werden alle Benutzer des Unternehmens ACME automatisch Mitglieder der Domäne TOP/ACME.

Hinweis:
Benutzer mit der Administratorrolle können ihre eigenen Benutzerdatensätze und damit die Domäne ändern. Service Provider möchten möglicherweise die delegierte Verwaltung deaktivieren oder einen Genehmigungsprozess einrichten, um zu überprüfen, ob der Benutzer die Administratorrolle benötigt.

Wenn Sie die Domäne eines Unternehmens ändern, ändert die Instanz automatisch die Domäne der folgenden zugeordneten Datensätze, um sie an die neue Domäne des Unternehmens anzupassen.

- Standorte
- Abteilungen
- Gruppen
- Benutzer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Instanz ändert nicht automatisch die Domäne eines Datensatzes, in dem Sie das Kontrollkästchen **Verwaltete Domäne** aktiviert haben.

Domänendeaktivierung und zugehörige Unternehmen

Wenn Sie eine Domäne deaktivieren, führt die Instanz auch automatisch die folgenden Aktionen aus.

- Deaktiviert alle Unternehmen in der Domäne.
- Verhindert, dass sich alle Benutzer, die dem inaktiven Unternehmen zugewiesen sind, anmelden.

Hinweis:
Wenn ein Benutzer aus einem inaktiven Unternehmen versucht, sich anzumelden, wird dem Benutzer eine Fehlermeldung ähnlich der folgenden angezeigt: Unternehmen inaktiv – Ihr Zugriff auf diese Instanz ist nicht autorisiert.

Wenn Sie beispielsweise die ACME-Domäne aus den Beispieldaten deaktivieren, deaktiviert die Instanz auch das ACME-Unternehmen, und die drei Beispielbenutzer werden ausgesperrt.

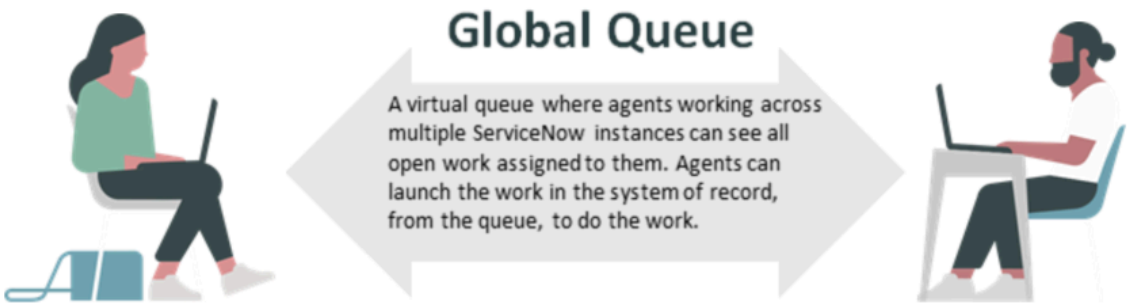
Konzepte für Service Provider

Diese Konzepte funktionieren mit den vorhandenen ServiceNow -Plattformfunktionen, um Sie bei der Lösung gängiger Anwendungsfälle zu unterstützen.

Globale Warteschlange v.2

Das Konzept der globalen Warteschlange bietet eine einzelne virtuelle Ansicht von Aufgaben, die sich in mehreren Instanzen befinden. Das Konzept erstellt eine benutzerdefinierte Anwendung, um eine Erfülleransicht der Arbeit bereitzustellen, die sich in mehreren Instanzen befindet, ohne Aufgaben oder Daten replizieren zu müssen.

Übersicht



Service Provider mit Service Desk-Mitarbeitern, die an Aufgaben aus mehreren Systemen arbeiten, integrieren die Daten in der Regel zurück in eine zentrale Instanz oder einen „Schwenkstuhl“ zwischen Instanzen. Diese Methode kann zwar in einigen Fällen angemessen sein, kann jedoch teuer und zeitaufwändig in der Erstellung und Wartung sein. Diese Methode öffnet den Anbieter auch für potenzielle Audits und Datenanforderungen wie die Datenschutz-Grundverordnung (DSGVO) in allen Instanzen, in denen sich die Daten jetzt befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

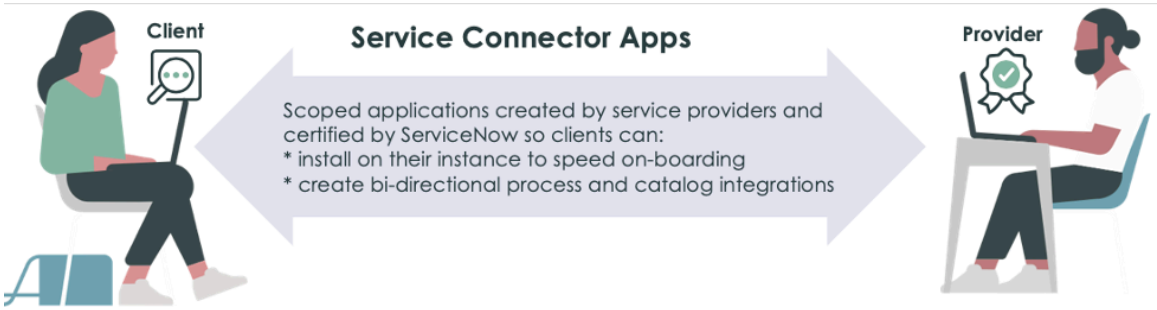
Globale Warteschlange v.2 ist eine Alternative: Mit dieser Methode können Service Desk-Mitarbeiter Daten anzeigen, die ihnen von einer einzelnen Instanz zugewiesen wurden, ohne dass souveräne Daten in der Instanz gespeichert werden, bei der sie angemeldet sind. In Fällen, in denen Clients beispielsweise Anforderungen an die Datenresidenz haben, aber den Zugriff durch Service Desk-Mitarbeiter aus anderen Ländern zulassen, kann der Anbieter einen „Follow-the-Sun“-Help Desk mit globaler Warteschlange v.2 verwenden.

Weitere Informationen zum Proof of Concept von Global Queue v.2 finden Sie auf der Wissenswebsite ServiceNow.

Hinweis:
Im Quebec-Release wurde der Proof of Concept von Global Queue auf Global Queue v. 2 aktualisiert.

Service Provider-Connector

Die Service Provider-Connector-Anwendung ist ein Referenzdesign zum Erstellen einer ServiceNow Store-Anwendung, die Kunden zur Integration in Ihre Systeme verwenden können. Service Provider-Anwendungen helfen Ihnen, das Onboarding zu beschleunigen und standardisierte Integrationen zu erstellen.

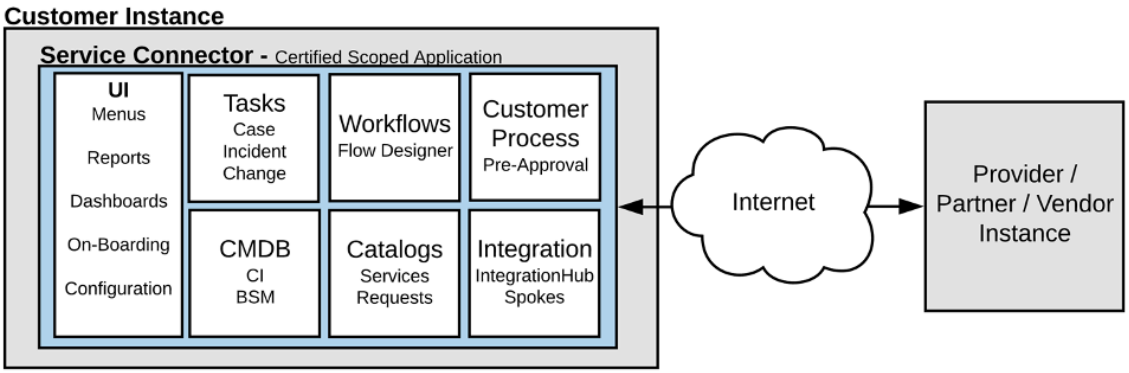


Vorteile von Service Connectors

Wenn Service Provider (Lieferanten, Lieferanten, Partner) Connectors veröffentlichen, ist das Onboarding von Kunden schneller, was eine schnellere Abrechnung bedeutet. Integrierte Instanzen steigern die Produktivität, erhöhen die Transparenz im ServiceNow -Ökosystem und bieten die Vorteile des Partnerprogramms. Spezifische Vorteile:

- Beseitigt benutzerdefinierte Integrationen, einschließlich der Kosten für Services, die für deren Bereitstellung und Wartung erforderlich sind.
- Services werden innerhalb ihrer ServiceNow -Instanzen vom Anbieter definiert, wodurch die Komplexität und Kosten benutzerdefinierter Integrationen überflüssig werden.
- Workflows und Kataloganforderungen können synchronisiert werden, wobei die Prozesse und Genehmigungen des Kunden den Prozessen des Anbieters vorausgehen, sodass Kunden ihre eigenen Prozesse verfolgen können.
- Alle Daten, die für den Kunden in der Instanz des Anbieters erstellt oder geändert (z. B. CIs) werden, können zur Sichtbarkeit und Verwendung in Prozessen wieder mit der Instanz des Kunden synchronisiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Schlüsselfunktionen

Funktion	Beschreibung
Benutzeroberfläche	Ein Service Connector sollte mindestens die folgenden UI-Komponenten enthalten: • Berichte/Dashboards: Von Personas vordefinierte Berichte und Dashboards helfen bei der Transparenz. • Menü und Module – Der Kunde sollte die Anwendung über das beschreibende Menü „ **Anbieter XYZ Services**“ finden können. • Rollen: Jeder Connector erfordert Benutzer- und Administratorrollen, um sicherzustellen, dass der Zugriff vom Kunden gesteuert werden kann. Beispiel: „x_snc_xyz_user“ oder „x_snc_xyz_admin“. • Onboarding: Schnelles Onboarding ist für eine gute Kunden-Experience unerlässlich und sollte über Playbook, Guided Setup oder Katalogelement so integriert werden, dass keine professionellen Services erforderlich sind, damit der Kunde live gehen kann. (Professional Services sind verfügbar, das Onboarding ist jedoch auch ohne sie möglich.) • Konfiguration: Datenpunkte sollten in Prozesse integriert werden, um den Großteil der normalen Prozesskonfiguration zu berücksichtigen, die ein Kunde erreichen muss. Dadurch werden professionelle Dienstleistungen so weit wie möglich eliminiert. • Dokumentation – Eine gründliche Dokumentation erhöht die Kundenzufriedenheit und die Benutzerfreundlichkeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
	• Support-Integration oder Kontaktinformationen: Der Kunde benötigt eine einfache Möglichkeit, bei Problemen, Fragen oder Anforderungen mit dem Service Provider in Kontakt zu bleiben.
Aufgaben	Die Verwendung der Anwendung Service Exchange (legacy) für Aufgaben wie Incidents, Fälle, Changes, Probleme usw. sollte im Connector vordefiniert sein. Diese Integrationen werden mit Flow Designer und IntegrationHub erstellt, um ein Höchstmaß an Resilienz und Leistung sicherzustellen.
CMDB	Die Synchronisierung von Kerndaten, z. B. die für ordnungsgemäße ITIL-Prozesse erforderlichen CIs, sollte zwischen Anbieter- und Kundeninstanzen synchron gehalten werden.
Workflows	Alle Workflows sollten in Flow Designer entworfen werden, um Resilienz und Leistung sicherzustellen.
Kataloge	Der Katalog des Anbieters, den der Kunde anfordert, muss als datensatzerzeugender Katalog in die Anwendung aufgenommen werden. Die vom Element in der Instanz des Kunden generierte Anforderung muss per eBonding mit den Instanzen des Anbieters verknüpft werden. Die Workflows des Anbieters halten die Anforderung auf dem neuesten Stand und synchronisieren sie mit der Instanz des Kunden.
Kundenprozesse	Alle Mechanismen zum Synchronisieren von Anforderungen mit der Instanz des Anbieters sollten es Kundenprozessen ermöglichen, mit den Anforderungen zu interagieren, bevor sie an die Instanz des Anbieters gesendet werden. Während der Provider-Verarbeitung können Genehmigungen bei Bedarf an die Instanz des Kunden gesendet werden.
Integration	Integrationen sollten mit Flow Designer und IntegrationHub erstellt werden, um ein Höchstmaß an Resilienz und Leistung sicherzustellen.

Mögliche Komponenten, die Sie in einen Service Connector aufnehmen können

Komponente	Beschreibung
Instanzdatenreplikation (IDR)	Wenn die Replikation das Ziel ist: • Kann für die Prozessintegration verwendet werden, kann jedoch je nach Komplexitätsintegrationslogik basierend auf dem Statusübergang zu unflexibel sein • Weitere Informationen finden Sie unter Instanzdatenreplikation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
IntegrationHub	Wenn die Prozessintegration das Ziel ist: • Einfacher in der Mitte eines Prozesses als Teil eines komplexen oder bedingten Schritts in der Mitte eines Flows zu injizieren • Weitere Informationen finden Sie unter IntegrationHub
Globale Arbeitswarteschlange (virtuell)	Wenn der Aufgabenverbund das Ziel ist und die externe Speicherung von Daten nicht akzeptabel ist: • Wird verwendet, wenn Service Desk-Mitarbeiter in mehreren ServiceNow Instanzen arbeiten und alle ihnen zugewiesenen offenen Arbeiten sehen müssen • Die zurückgegebenen Zeilen sollten auf weniger als 1000 beschränkt sein • Weitere Informationen finden Sie unter Globale Arbeitswarteschlange
Remotetabellen	Wenn die Verwendung externer Daten ohne Speicherung das Ziel ist: • Wird verwendet, um eine Instanz mit Quellen von Drittanbietern oder einer anderen Instanz zu verbinden, externe Daten abzurufen und optional im Speicher zwischenzuspeichern. Die Daten werden zu schreibgeschützten Zwecken wie Gruppieren, Sortieren, Aggregieren und Filtern als Tabelle in der Instanz behandelt. • Weitere Informationen finden Sie unter Externe Daten mit Remotetabellen und -skripts abrufen
Flow Designer	Wenn Prozessdesign das Ziel ist • Wird für die Automatisierung von Prozessen in einer einzelnen Designumgebung verwendet. Prozessverantwortliche können natürliche Sprache verwenden, um Genehmigungen, Aufgaben, Benachrichtigungen und Aufzeichnungsvorgänge ohne Codierung zu automatisieren. • Weitere Informationen finden Sie unter Flow Designer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Proof of Concept für Service Connector finden Sie auf der Wissenswebsite ServiceNow.

Wird mit Domänentrennung installiert

Bei der Domänentrennung werden mehrere Plattformkomponenten hinzugefügt oder geändert.

Rollen

Rolle	Beschreibung
domain_admin	Kann Domänen erstellen, bearbeiten und löschen.

Ergänzungen zu Feldern [sys_domain].

Das Feld sys_domain wird den folgenden Tabellen hinzugefügt:

Tabellen mit dem Feld sys_domain

Tabellen
sys_attachment
sys_user_has_role
sys_group_has_role
sys_email
sys_user_group
core_company
cmn_location
cmn_department
sys_anzeige
sys_report
kb_feedback
sysapproval_approver
sys_user_grmember

Feld für die Aufgabentabelle

MSP-Erweiterungen fügen der Aufgabentabelle ein task_for-Feld hinzu. Dieses Referenzfeld bezieht sich auf die Benutzertabelle.

Optionen für den Gruppentyp

MSP-Erweiterungen fügen dem Typfeld der Gruppentabelle mehrere neue Standardoptionen hinzu. Fügen Sie diese Typen nach Bedarf hinzu, oder aktualisieren Sie sie, um Ihre Domänen zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellen
Sicherheit
Support
Sichtbarkeit

Business-Regeln

Name	Tabelle	Beschreibung
Domäne: Aktivieren/ Deaktivieren	core_company	Aktiviert die zugehörige Domäne, wenn mindestens eines ihrer Unternehmen aktiv ist. Deaktiviert die zugehörige Domäne, wenn alle zugehörigen Unternehmen inaktiv sind.
Domäne: Unternehmen kaskadieren	core_company	Hält die Domäne eines Unternehmens mit seinen Benutzern, Gruppen, Abteilungen und Standorten synchron.
Domäne: kaskadierende Domäne – E-Mail	sys_email	Hält die Domäne einer E-Mail mit ihren Anhängen synchron.
Domäne: Domäne kaskadieren – Gruppe	sys_user_group	Hält die Domäne einer Gruppe mit ihren geerbten Rollen (sys_group_has_role-Datensätze) synchron.
Domäne: Domäne kaskadieren – Wissen	kb_knowledge	hält die Domäne eines Wissensartikels mit dem zugehörigen Feedback synchron.
Domäne: Domäne kaskadieren – Aufgabe	Aufgabe	Hält die Domäne mit zugehörigen Aufgaben für wf_context, wf_executing, wf_history, Anhänge, E-Mails, task_sla und ihren Workflow, sysapproval_approver und ihren Workflow sowie sysapproval_group und ihren Workflow synchron.
Domäne: Domäne kaskadieren – Anwender	sys_user	Hält die Domäne eines Benutzers mit den Datensätzen seiner Gruppenmitgliedschaft (sys_user_grmember) und Rolle (sys_user_has_role) synchron.
Domäne: Kaskadierte Domäne – Version	wf_workflow_version	Hält Domänen mit zugehörigen Workflow-Versionen für „wf_aktivität“ und „wf_transition“ synchron.
Domäne: Unternehmen deaktivieren	Domäne	Deaktiviert zugehörige Unternehmen, wenn eine Domäne deaktiviert wird.
Domäne – Standard – Aufgabe	Aufgabe	Legt die Aufgabendomäne basierend auf der Aufgabe für die Domäne des Anwenders fest. Wenn diese Domäne global wäre, wird die Domäne stattdessen auf Standard festgelegt.
Domäne – Standard – Anwender	sys_user	Legt die Domäne eines Benutzers auf Standard fest, wenn die Domäne andernfalls global wäre.
Domäne: Globaler Domänendatensatz nicht zulassen	Domäne	Verhindert die Erstellung einer Domäne mit dem Namen global.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Tabelle	Beschreibung
Domäne: Kopie überschreiben	sys_app_application	Wenn eine Anwendung für eine Domäne überschrieben wird, erstellt eine Kopie ihrer Module für die neue Anwendung.
Domäne: Kopie überschreiben	sys_data_policy2	Wenn eine Datenrichtlinie für eine Domäne überschrieben wird, erstellt eine Kopie der Datenrichtlinienregeln für die neue Datenrichtlinie.
Domäne: Kopie überschreiben	sys_anzeige	Wenn eine Anzeige für eine Domäne überschrieben wird, erstellt eine Kopie der Anzeigeanzahlen für die neue Anzeige.
Domäne: Kopie überschreiben	sys_ui_action	Wenn eine UI-Aktion für eine Domäne überschrieben wird, erstellt eine Kopie ihrer UI-Aktionsansichten für die neue UI-Aktion.
Domäne: Kopie überschreiben	sys_ui_list_control_embedded	Wenn ein eingebettetes Listensteuerelement für eine Domäne überschrieben wird, erstellt eine Kopie seiner Client- und Serverskripts für das neue eingebettete Listensteuerelement.
Domäne: Kopie überschreiben	sys_ui_policy	Wenn eine UI-Richtlinie für eine Domäne überschrieben wird, erstellt eine Kopie ihrer UI-Richtlinienaktionen für die neue UI-Richtlinie.
Domäne: Legen Sie die Domäne „Genehmigungen“ fest	sysapproval_approver	Legt die Domäne basierend auf der des genehmigten Datensatzes fest.
Domäne: Domäne festlegen – Anhang	sys_attachment	Legt die Domäne basierend auf der Domäne des übergeordneten Datensatzes fest.
Domäne: Domäne festlegen – CMDB_CI	cmdb_ci	Legt die Domäne eines CI auf die Domäne seines Unternehmens fest.
Domäne: Domäne festlegen – Abteilung	cmn_department	Legt die Domäne einer Abteilung auf die ihres Unternehmens fest.
Domäne: Legen Sie „Domäne – Domäne“ fest	Domäne	Legt die Domäne einer Domäne auf sich selbst fest.
Domäne: Domäne festlegen – E-Mail	sys_email	Legt die Domäne basierend auf der Domäne des übergeordneten Datensatzes fest. Der übergeordnete Datensatz einer E-Mail ist der im Instanzfeld angegebene Datensatz.
Domäne: Domäne festlegen – Feedback	kb_feedback	Legt die Domäne eines Wissensfeedbacks auf die Domäne seines Wissensartikels fest.
Domäne: Domäne festlegen – Gruppe	sys_user_group	Legt die Domäne einer Gruppe auf die ihres Unternehmens fest.
Domäne: Legen Sie die Domäne fest – Gruppengenehmigungen	sysapproval_group	Legt die Domäne basierend auf der des genehmigten Datensatzes fest.
Domäne: Domäne festlegen – Gruppenrolle	sys_group_has_role	Legt die Domäne einer Gruppenrolle auf die ihrer Gruppe fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Tabelle	Beschreibung
Domäne: Legen Sie „Domäne – Standort“ fest	cmn_location	Legt die Domäne eines Standorts auf die Domäne seines Unternehmens fest.
Domäne: Domäne festlegen – Aufgaben-SLA	task_sla	Legt die Domäne einer Aufgaben-SLA auf die Domäne ihrer Aufgabe fest.
Domäne: Domäne festlegen – Anwender	sys_user	Legt die Domäne eines Benutzers auf die Domäne seines Unternehmens fest.
Domäne: Domäne festlegen – Benutzerrolle	sys_user_has_role	Legt die Domäne einer Benutzerrolle auf die Domäne ihres Benutzers fest.
Domäne: Domäne festlegen – WF-Aktivitätsverlauf	wf_history	Legt die Verlaufsdomäne der Workflow-Aktivität basierend auf der Domäne des übergeordneten Workflow-Kontexts fest.
Domäne: Domäne festlegen – WF-Kontext	wf_context	Legt die Workflow-Kontextdomäne basierend auf der Domäne des referenzierten Datensatzes fest, falls vorhanden.
Domäne: Domäne festlegen – WF-Ausführungsaktivität	wf_executing	Legt die Domäne der Workflow-Ausführungsaktivität basierend auf der Domäne des übergeordneten Workflow-Kontexts fest.
Domäne – Aufgabe festlegen für – Change	Change-Anforderung	Legt beim Konvertieren eines Tickets in eine Change-Anforderung das Feld Angefordert von auf den Wert Aufgabe für des Tickets fest.
Domäne – Aufgabe festlegen für – Incident	Incident	Legt beim Konvertieren eines Tickets in einen Incident das Feld Anrufer auf den Wert Aufgabe für des Tickets fest.
Domäne: Standard validieren	Domäne	Stellt sicher, dass nur in einer Domäne das Kontrollkästchen Standard aktiviert ist.
Domäne: Primäre validieren	Domäne	Stellt sicher, dass das Kontrollkästchen Primär nur für eine Domäne aktiviert ist.
Mit dem Plugin „Domain Support“ installierte Business Rules		
Domänensatz ändern	sys_dictionary	Legt den Domänensatz auf die aktuelle Domäne fest.
Eigenschaften des Domänensupports	sys_properties	Legt die Systemeigenschaften so fest, dass sie der Domänenabfragemethode entsprechen (Domänenpfade oder Domänennummerierung).

Clientskripts

Client-Skript	Beschreibung
Domäne – Unternehmen und Standort festlegen (sys_script)	Überwacht das Incident-Anruferfeld auf Änderungen. Wenn die Felder „Unternehmen“ und „Standort“ noch keinen Wert enthalten, fügt das Skript diese Informationen aus dem Anruferdatensatz hinzu. Wenn die Felder „Unternehmen“ und „Standort“ bereits einen Wert haben, behält das Skript die vorhandenen Werte bei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client-Skript	Beschreibung
Deaktiviertes Skript	
(BP) Legen Sie Standort auf Benutzer fest	Überwacht das Incident-Standortfeld und legt das Standortfeld auf den Standort des Anrufers fest.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Anwendungssupport für die Domänentrennung

Viele ServiceNow Anwendungen unterstützen die Domänentrennung im Basissystem, aber nicht alle. Einige unterstützte Anwendungen enthalten Einschränkungen für die Daten und administrativen Einstellungen, die nach Domänen getrennt werden können. Diese Definitionen beschreiben die Supportstufen für die Domänentrennung aus der Perspektive der tatsächlichen Anwendungsfälle und der Personen, die sie verwenden.

Support-Stufen für Domänentrennung

ServiceNow Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und Datenweiterleitung, verfügen über eine erweiterte Geschäftslogiktrennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kundenebene). ServiceNow Anwendungen werden mit den folgenden inkrementellen Supportstufen definiert.

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Logik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- In der Anwendung berücksichtigen die Benutzeroberfläche, Cache-Schlüssel, Berichterstellung, Rollups, Zusammenfassungen usw. Domänen zur Produktionslaufzeit.
- Der Besitzer der Instanz muss in der Lage sein, die Anwendung so einzurichten, dass sie mandantenübergreifend funktioniert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Anwendungsfall: Wenn ein SP den Chat verwendet, um auf die Nachricht eines Mandanten zu antworten, muss der Client die Antwort des SP sehen können.

Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Prozesse können vom Service Provider (SP) pro Kunde erstellt oder geändert werden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss in der Lage sein, die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung zu konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, aber nicht für andere.

Verbessert

- Umfasst die Stufen **Basis** und **Standard**.
- Ein datengesteuerter Prozess ermöglicht es Service Provider-Kunden, die Geschäftslogik basierend auf definierten Anwendungsfällen zu ändern. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass Konfigurationen von einem Kunden sich nicht auf einen anderen auswirken können.
- Mandanten der Instanz müssen die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter für sich selbst konfigurieren können. Diese Logik und diese Parameter würden für die normale Funktion der Anwendung erwartet.

Beispiel-Anwendungsfall: Mandanten-Kunden einer gemeinsam genutzten Umgebung müssen in der Lage sein, die Auswirkungs-, Dringlichkeits- oder Prioritätsmatrix zu ändern, um die Priorität innerhalb ihrer Domäne festzulegen.

Hinweis:
Effektive Domäne (*)

Manchmal kann eine Plattformfunktion oder -anwendung SP-Anwendungsfälle auch ohne das Domänen-Framework effektiv unterstützen. Wenn dies der Fall ist, müssen die Anwendungsfälle die Unterstützung der Domänentrennung beschreiben. Ein Sternchen (*) nach der Supportstufe zeigt diese Art von Konfiguration an.

Unterstützte Funktion	Standard	Standard	Erweitert
Domänenspalte ist für Basissystem-Anwendungstabellen vorhanden.	●	●	●
Die domänenspezifische Konfiguration wird vom Instanzbesitzer verwaltet.	●	●	●
Mandantendomänen können ihre eigenen Anwendungsdaten verwalten.		●	●

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Funktion	Standard	Standard	Erweitert
Anwendungseigenschaften sind bei Bedarf domänenbezogen.			
Geschäftslogik und Prozesse können vom Instanzbesitzer domänengetrennt werden.			
Geschäftslogik und Prozesse können von der Mandantendomäne verwaltet werden.			

Supportstufen nach Anwendung

Produkt-Suite	Anwendung	Support-Stufe
Hyperautomation and low-code	App Engine Studio	Kein Support
	Automation Center	Standard
	Robotic Process Automation (RPA) Hub	Standard
	Table Builder	Standard
	App Engine Management Center	Kein Support
	Entscheidungsgenerator	Standard
	Integration von Enterprise Resource Planning	Kein Support
	Enterprise Resource Planning Customization Mining	Kein Support
	Next Experience UI Builder	Standard
Kundenservice-Management	Communities	Kein Support
	Kundenservice-Management	Standard
	Releasemanagement	Standard*
	Order Management für Customer Service Management	Standard
	Post-Sales Support	Standard
	Domain separation in Workforce Optimization for Customer Service	Standard
DevOps	DevOps	Kein Support
	DevOps Config	
Employee Service Management	HR Service Delivery	Standard*
	Arbeitsschutz	Standard
	Legal Service Delivery	Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Procurement Service Management (PSM)	Kein Support
	Safe Workplace-Suite	Weitere Informationen zu den einzelnen Anwendungssupportstufen finden Sie auf der Anwendungswebsite
	Connector für SharePoint Online-Suchen	Standard
	Universelle Anforderung	Standard
	UR-Aufgabe	Standard
	Personaloptimierung für HR	Standard
Environmental, Social, and Governance Management	ESG-Management	Standard
Field Service Management	Field Service Management	Standard
Governance, Risk und Compliance	Business Continuity Management	Standard
	Governance, Risk und Compliance (GRC)	Standard
	Operational Resilience	Standard
Branchenprodukte		
•	Financial Services Card Operations	Standard
	Financial Services Deposit Operations	Standard
	Financial Services Payment Operations	Standard
	Intelligent Servicing for Fraud	
	Sachwert- und Unfallversicherungs-Servicing	
	Lebensversicherungs-Servicing	
	Versicherungsansprüche	
	Financial Services Know Your Customer	
	Kreditvorgang für Finanzdienstleistungen	
	Financial Services Document Processor	Standard
• Gesundheitswesen und Biowissenschaften	EMR Help	Standard
	Healthcare and Life Sciences Service Management Core	Standard
	Pre-Visit Management	Standard
	Patientenunterstützungsservices	Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Vaccine Administration Management	Standard
• Fertigungsindustrie	Manufacturing Process Manager	Standard
	Operational Technology Manager	Standard
	Operational Technology Vulnerability Response	Standard
	Operational Technology Service Management	Standard
•Telekommunikation	Service Bridge	Standard
	Order Management für Telekommunikation, Medien und Technologie	Standard
	Telecommunications and Media Assurance Workflows	Standard
IT Asset Management	Cloud Insights	Kein Support
	Hardware Asset Management	Erweitert
	Software Asset Management	Erweitert
	Enterprise Assest Management	Standard
Strategic Portfolio Management	Agile Development	Standard*
	Alignment Planner Workspace	Standard
	Application Portfolio Management	Standard
	Cost Management	Kein Support
	Demand-Management	Standard
	Finanzmanagement	Kein Support
	Investment Funding	Standard
	Projektportfoliomanagement	Standard*
	Releasemanagement	Standard*
	Scaled Agile Framework (SAFe)	Standard*
	Test Management	Standard*
	Ziel-Framework	Standard
IT Operations Management	Cloud Provisioning and Governance	Standard
	Agent Client Collector	Standard
	Discovery	Standard
	Ereignismanagement	Standard
	Service Operations-Arbeitsbereich für ITOM	Standard
	Health Log Analytics	Standard

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Metric Intelligence	Standard
	Service-Zuordnung	Standard
	Bewertung der Cloud-Migration	Standard
	Aktionsbibliothek	Kein Support
	Cloud Configuration Governance	Kein Support
	Tag Governance	Standard
	Abrechnung für Cloud-Einblicke	Kein Support
	Cloud Provisioning and Governance: Google Cloud	Standard
	Cloud Provisioning and Governance Terraform	Standard
	Cloud Operation Workspace (Cloud-Vorgangsarbeitsbereich).	Standard
	Cloud-Discovery	Standard
IT Service Management	Benchmarks	Kein Support
	Change-Management	Standard
	Coaching	Standard
	Management kontinuierlicher Verbesserungen	Standard
	Vertragsmanagement	Kein Support
	Expense Line	Kein Support
	Incident-Kommunikationsmanagement	Standard
	Incident-Management	Standard
	Facilities Service Management	Standard
	Incident-Management	Standard
	On-Call Scheduling	Standard
	Asset-Management	Standard
	Problem-Management	Standard
	Procurement	Standard*
	Produktkatalog	Standard
	Anforderungsmanagement	Standard
	Service Catalog	Standard
	Service Desk Call	Standard
	Service-Level-Management	Standard
	Service Portfoliomanagement	Standard*
	Site Reliability Operations	Standard*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Nichtverfügbarkeit von Aufgaben	Standard
	Domain separation and Vendor Management Workspace	Kein Support
	Walk-up Experience	Standard
Konfiguration und Navigation für Mobile	Mobil	Standard
Now Intelligence	Dashboards	Standard
	Leistungsanalysen	Erweitert
	Process Optimization	Standard
	Reporting	Standard
	User Experience Analytics	Standard
Die Now Platform	,Administration ,App Engine, Benutzeroberfläche für Now Platform-Fähigkeiten	
	Domain separation and Agent Chat	Standard
	Advanced Work Assignment	Standard
	AI Search	Suchvorgänge berücksichtigen Domänenbeschränkungen aus indizierten Datensätzen
	App Engine Studio	Kein Support
	Application Management	Kein Support
	Bewertungen	Standard
	Automated Test Framework	Standard*
	ServiceNow Voice	
	Contextual Search	Standard
	Configuration Management (CMDB)	Standard
	Content-Management-System	Kein Support
	Anmeldeinformationen und Verbindungen	Standard
	Datenzertifizierung	Standard*
	Data Classification	Erweitert
	Datenschutz	Kein Support
	Datenverwaltung	Standard*
	Delegated Development	Kein Support
	Dependency Views	Standard
	Dokumentenservices	Kein Support
	Dynamische Übersetzung	Standard
	Edge Encryption	Kein Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Verschlüsselung auf Spaltenebene	Kein Support
	Column Level Encryption Enterprise	Kein Support
	Cloud-Verschlüsselung mit Schlüsselverwaltung	Basis-Support
	Feldnormalisierung	Kein Support
	Flow Designer	Standard*
	Geführtes Setup	Kein Support
	Homepage-Administration	Standard*
	IntegrationHub	Standard*
	Integrationen mit Anwendungen und Datenquellen von Drittparteien	Basis + Standard
	Knowledge Management	Standard
	Hermes Messaging Service	Kein Support
	Verwaltete Dokumente	Kein Support
	MetricBase	Standard
	Natural Language Understanding	Basis + Standard
	Benachrichtigungen	Standard
	ODBC-Treiber	Standard*
	Orchestration	Standard*
	Password Reset	Standard
	Platform-Sicherheit	Zielseite der Domänentrennung
	Datenschutz	Kein Support
	Predictive Intelligence	Standard
	Proaktive Auslöser	Standard
	Process Automation Designer	Standard
	Remotetabellen	Kein Support
	Zeitpläne	Standard
	Skript-Debugger	Standard
	Suchvorschläge	Kein Support
	Service Portal	Kein Support
	Domain separation and Sidebar	Standard
	Status-Flows	Kein Support
	Subscription Management	Standard*
	Umfragemanagement	Standard*
	Task Intelligence	Kein Support
	Zeitkarte	Standard*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	UI Builder	Standard
	Virtual Agent	Standard
	Visual Task Boards	Standard
	Webservices	Standard*
	Workflow	Standard*
	Arbeitsbereich	Standard
Security Operations	Configuration Compliance	Standard
	Configuration Data Management	Standard
	IBM QRadar Offense Ingestion	Standard
	Integration der Microsoft Graph-Sicherheits-API zur Warnungserfassung	Standard
	Security Incident Response	Standard
	Threat Intelligence	Standard
	Vertrauenswürdige Sicherheitskreise	Standard
	Vulnerability Response	Standard
Service Management	Facilities Service Management	Standard
	Geplante Wartung	Standard*
	Proaktive Auslöser	Standard
	NOW-Code-Editor	Kein Support
	Personaloptimierung für ITSM	Standard
	Vendor Management Workspace	Standard

Empfohlene Domain Separation-Verfahren für Service Provider

Sie können die Domänentrennung für Ihre Anwendungen und Services erstellen, implementieren und verwalten.

Domänengrundlagen

Mit der Domänentrennung (auch als ServiceNow Multi-Mandanten-Plattform-Architektur bezeichnet) können Sie die Anwendungsdaten, die Benutzeroberfläche und die Geschäftslogik in einer einzigen Kundeninstanz trennen, die die hierarchische Modellierung mit mandantenübergreifender Intelligenz unterstützt. Die Geschäftslogik beschreibt, wie die Domänentrennung konfiguriert wird und welche Regeln sich auf die Konfiguration auswirken.

Bevor Sie sich auf den Weg zur Domänentrennung machen, finden Sie hier einige bewährte Vorgehensweisen. Wählen Sie die gewünschten Themen aus, oder folgen Sie ihnen der Reihe nach, indem Sie auf die Links unter dem Bild klicken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erklärung der Domänentrennung

Mit der Domänentrennung können Sie Anwendungsdaten, UI und Geschäftslogik, z. B. Regeln oder Workflows, in einer einzigen Kundeninstanz trennen. Durch die Aufteilung dieser Elemente in logisch definierte Domänen werden bestimmte Hierarchien für alle Kunden unterstützt, die Ihre Anwendungen verwenden.

Domänengrundlagen

Domänentrennung, auch bekannt als ServiceNow Multi-Mandanten-Plattformarchitektur, fügt der Verwaltung einer Instanz einen erheblichen Overhead hinzu. Wenn Sie die Domänentrennung jedoch richtig verwenden, kann sie die Effizienz verbessern, die Sicherheit erhöhen und die Leistung der Instanzen Ihrer Kunden steigern.

Sie können einige globale Standards und Eigenschaften, z. B. Systemeigenschaften und Tabellenschema, nicht pro Mandant trennen.

Bevor Sie mit der Trennung von Domänen beginnen, lesen Sie die folgenden Richtlinien.

Möglichkeiten der Domänentrennung

- Datentrennung: Ermöglicht Mandanten der Domäne, nur Daten anzuzeigen, für die sie über Berechtigungen verfügen. Mandanten können Zugriff auf andere Mandantendaten erhalten, sie können jedoch keine Mandantendaten abfragen, auf die sie keinen Zugriff haben.
  - Wenn Sie Datensätze aktualisieren, werden keine Update Set-Datensätze generiert.
  - Benutzer, einschließlich der Kunden-Accounts, die für Integrationen verwendet werden, sehen nur die Daten in den Domänen, auf die sie zugreifen dürfen.
  - Kunden, Service Desk-Mitarbeiter und Erfüller sehen Daten, die sich auf die von ihnen unterstützten Kunden und Organisationen beziehen.
- UI-Trennung: Unterstützt eine mandantenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.

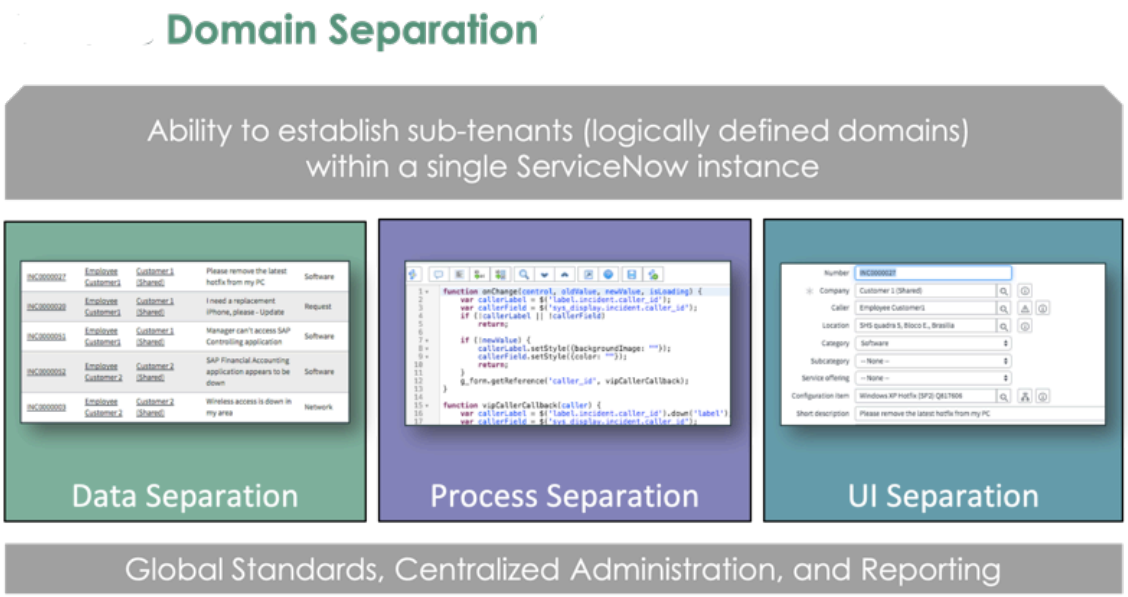
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können die browserbasierte Benutzeroberfläche überschreiben, einschließlich Anwendungsmenüs, Listen, Formulare und Dashboards. Sie können sie auch für eine bestimmte Domäne oder einen Satz von Domänen anpassen und dabei Ihre grundlegende Prozesslogik beibehalten.
- Service Provider können die angezeigten Branding- und UI-Elemente ändern, um die individuellen Kundenanforderungen zu erfüllen.

- Trennung der Geschäftslogik: Erstellt mandantenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Clientskripts, UI-Richtlinien und UI-Aktionen.
- Hierarchische Modellierung: Verschachtelt mehrere Mandanten, sodass übergeordnete Mandanten auf untergeordnete Mandantenressourcen zugreifen können. Die Geschäftslogik für übergeordnete Mandanten wird automatisch für untergeordnete Mandanten ausgeführt, die Sie auf jeder Ebene überschreiben können.
- Cross-Mandanten-Intelligenz: Verarbeitet automatisch Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten mit Zugriff auf zusätzliche Mandantendaten.

Domänentrennung auf einen Blick

Die folgende Grafik zeigt die Aufteilung von Daten, Prozess und UI-Trennung. Diese Konzepte werden im Abschnitt „Empfohlene Vorgehensweisen“ ausführlich erläutert.



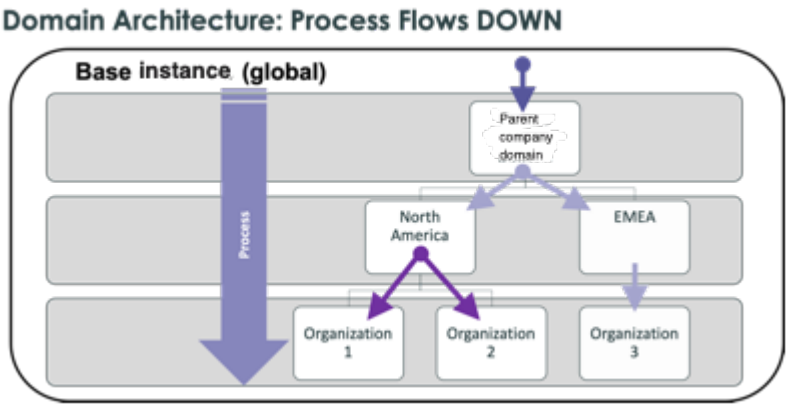
Domänenarchitektur

Benutzerdatensätzen wird ein Domänenwert zugewiesen, der die Stammdomäne des Benutzers darstellt. Benutzer haben keinen Zugriff auf Daten in übergeordneten Domänen, Peer-Domänen oder Domänen in anderen Zweigen der Hierarchie.

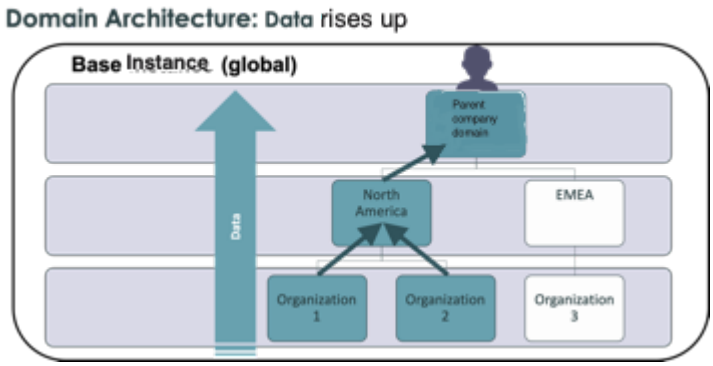
Unter Enthält Abfragen und Domänenzugriff finden Sie erweiterte Optionen, um zusätzliche Domänentransparenz zu gewähren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Diagramm zeigt, wie der Architekturprozess in die untergeordneten



Domänen übergeht.



Leistungsversprechen der Domänentrennung

Mit Domänentrennung können Service Provider über eine Multi-Mandanten-Instanzarchitektur verfügen, die ihren Clients Angebote effizient und sicher bereitstellt. Strenge universelle Prozessstandards, datengesteuertes Prozessdesign, strikte Governance und zentralisierte Verwaltung tragen dazu bei, diese Vorteile zu maximieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile der Domänentrennung

Die Mandanten einer Domäne profitieren von einer schnellen Kapitalrendite, einem geringeren Verwaltungsaufwand und der Nutzung von Geschäftsservices, die von Instanzbesitzern bereitgestellt werden.

Hier erhalten Sie einen Überblick über diese Vorteile.

Instanzbesitzer	Domänenmandanten
Mitarbeiterproduktivität von Service Providern	Erhöhte Sicherheit
Nur Prozess-Deltas beibehalten	Vorgefertigte Prozesse und Funktionen
Verwaltungseffizienzen	Reduzierter Personalbedarf
Weniger Client-Integrationen	Schnelleres Onboarding
Upgrade-Fähigkeit und Skalierbarkeit	Nutzung der neuesten Releases
Datentrennung	Vom Instanzbesitzer bereitgestellte Services
Globale Berichterstellung	

Definition der Domänentrennung

Mit der Domänentrennung (auch als ServiceNow® Multi-Mandanten-Plattform-Architektur bezeichnet) können Sie Anwendungsdaten, UI und Geschäftslogik in einer einzigen Kundeninstanz trennen, die die hierarchische Modellierung mit mandantenübergreifender (Kunden-) Intelligenz unterstützt.

Eigenschaften der Domänentrennung

Domänengetrennte ServiceNow Anwendungen werden mit den folgenden Eigenschaften definiert:

Datentrennung

Ermöglicht Kunden, nur die Daten anzuzeigen, für die sie über Berechtigungen verfügen. Kunden können Zugriff auf andere Kundendaten erhalten, können jedoch keine Kundendaten abfragen, wenn sie keinen Zugriff haben.

UI-Trennung

Unterstützt eine kundenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.

Trennung der Geschäftslogik

Unterstützt kundenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Client-Skripts, UI-Richtlinien und UI-Aktionen.

Hierarchische Modellierung

Unterstützt geschachtelte Mehrmandantenfähigkeit, sodass übergeordnete Mandanten (Kunden) auf untergeordnete Kundenressourcen zugreifen können. Die Geschäftslogik für übergeordnete Kunden wird automatisch für untergeordnete Kunden ausgeführt und kann auf jeder Ebene überschrieben werden.

Kundenübergreifende Intelligenz (Domänenbereich)

Verarbeitet automatisch die Daten, Metadaten, Geschäftslogik und den Verarbeitungskontext für Mandanten, die Zugriff auf zusätzliche Mandantendaten haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domain Separation-Hierarchien

Erstellen Sie beim Definieren einer Domänenarchitektur eine Hierarchie, um Ihre Prozesse und Workflows zu nachzuverfolgen.

Beispiele für Domain Separation-Hierarchien

Das folgende Diagramm ist ein guter Ausgangspunkt für die Definition der Domänenarchitektur. Es zeigt die Beziehung zwischen den TOP- und den untergeordneten Domänen und wie sich der Prozess, die Daten und die Geschäftsregeln auf die übergeordneten und untergeordneten Domänen auswirken.

- Im folgenden Beispiel ist TOP eine Prozessdomäne. Sie darf keine Benutzer enthalten. Eigentlich sollte TOP die neuen Prozesse enthalten, die die Eigentümer der Instanzen entwickeln, sowie die Überschreibungen zu diesen Prozessen aus der globalen Domäne.
- Nur der Service Provider (SP) hat Zugriff auf die Standarddomäne. Diese Domäne enthält keine aktiven Benutzer. Die Domäne enthält nur die „verlorenen“ Daten, die Sie der richtigen Domäne neu zuweisen müssen.

  Hinweis:
  Wenn Daten keiner bestimmten Domäne zugewiesen sind, werden sie in die Standarddomäne verschoben. Sie gehen vorübergehend „verloren“ und müssen der richtigen Domäne zugewiesen werden.

- Aufgaben und Benutzer ohne Domäne werden beim Erstellen oder Aktualisieren von Domänen automatisch in der Standarddomäne eingefügt. Sie können diese Aktion überschreiben, indem Sie entweder die Option **Standard** für diesen Datensatz deaktivieren oder die Option **Standard** für einen anderen Domänendatensatz auswählen. Wenn Sie noch keine Standarddomäne festgelegt haben, werden Aufgaben und Benutzer ohne Domäne in die globale Domäne verschoben.
  - Verschieben Sie keine Daten zwischen Domänen, während Sie die Instanz verwenden.
  - Wenn Daten in der Standarddomäne landen, bedeutet dies, dass Sie ein Konfigurations- oder Verfahrensproblem haben.

Das Wort „Global“ wird in diesem Diagramm nicht angezeigt, da keine globale Domäne vorhanden ist. Denken Sie daran, dass „global“ das Fehlen einer Domäne in einem Datensatz bezeichnet.

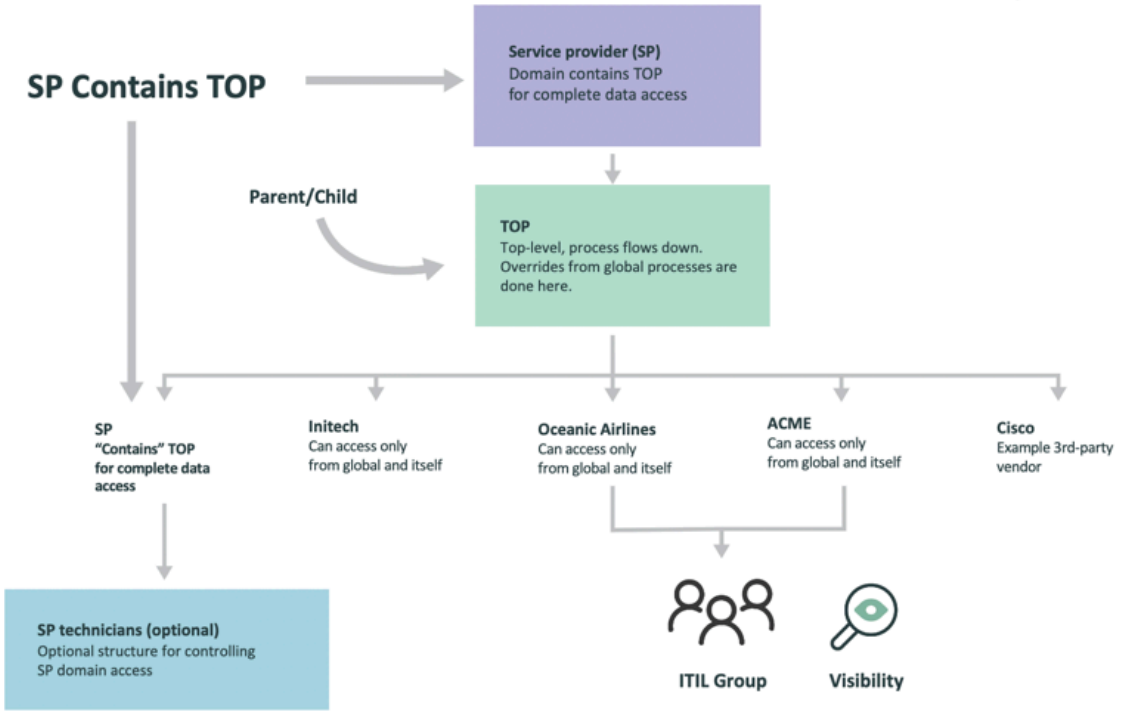
Eine Tabelle ohne Domänenfeld bedeutet beispielsweise, dass die Tabelle alle globalen Datensätze enthält. Eine Tabelle mit einem Domänenfeld bedeutet, dass jeder Datensatz ohne Domäne eine globale Domäne ist.

Das Wort „global“ befindet sich im Domänenfeld. Es wird automatisch dort platziert, wenn der Datensatz keine Domäne hat.

Globale Datensätze sind für alle Benutzer der Instanz verfügbar, sofern sie nicht durch Sicherheitskonfigurationen eingeschränkt werden.

- Verwenden Sie die Standarddomäne, um sicherzustellen, dass Datensätze nicht in der globalen Domäne in Tabellen landen, die niemals globale Datensätze enthalten dürfen.
- Die Besitzer eine Instanz müssen dann die Datensätze in der Standarddomäne selektieren und in die richtige Domäne verschieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Domänenhierarchien

- Über-/untergeordnet: betroffener Prozess und betroffene Daten
  - Design, das auf einem Prozess-Flow basiert.
  - Denken Sie daran, dass die übergeordneten Domänen auf alle Daten in den untergeordneten Domänen zugreifen können.
- Domäne „Enthält“: Nur Daten sind betroffen. Beispiel: Wenn SP im Diagramm „TOP“ enthält, werden Prozesse in SP nicht in der Domäne „TOP“ und abwärts ausgeführt.
  - Gewährt Personen in Gruppen Datenzugriffsrechte, die dedizierten Zugriff auf bestimmte Domänen erfordern.
  - Enthält Ursachen oder Bedingungen, die Datenbankabfragen hinzugefügt werden sollen, die Leistungsprobleme bei großen Domänen und Datensätzen verursachen können
- Sichtbarkeit: Hierarchie, die für Benutzer immer sichtbar ist, sobald Sie Zugriff gewähren. Nur die Daten sind betroffen, nicht die Prozesse.
  - Gewährt einer anderen Domäne, die beim Erstellen der über- und untergeordneten Hierarchie keinen Zugriff hatte, Datenzugriff auf eine Domäne
  - Ermöglicht es Benutzern, alle Daten in den Domänen zu sehen, für die sie Sichtbarkeitszugriff haben, und zwar jederzeit, unabhängig von dem Datensatz, an dem sie gerade arbeiten

Hinweis:
Gehen Sie sparsam damit um, da mit „Sichtbarkeit“ vollständiger Zugriff gewähren werden kann, was Sie möglicherweise nicht beabsichtigen.

Grundprinzipien der Definition einer Domänenhierarchie

Uneingeschränkte und eingeschränkte Anwendungsfälle für Domänentrennung.

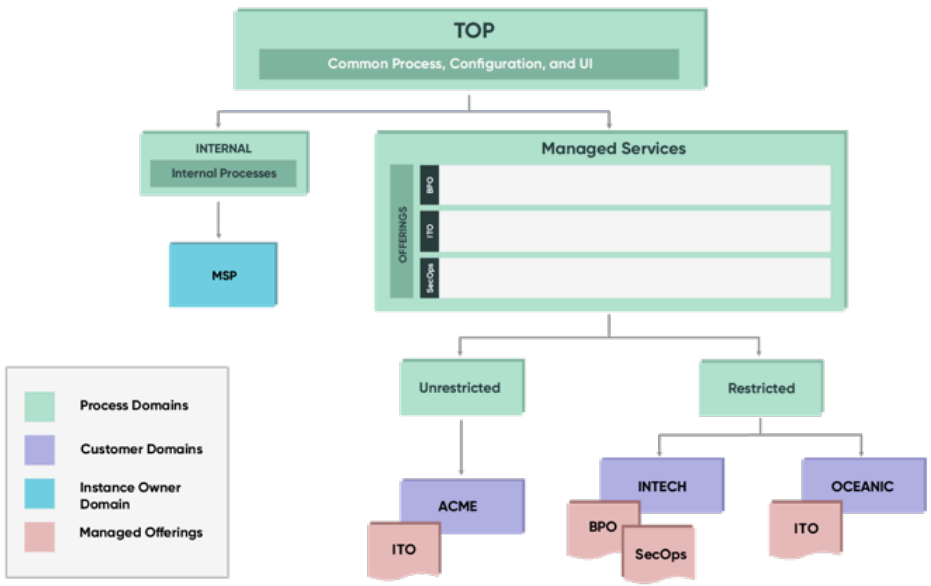
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Viele SPs haben Kunden, die implizit angeben, dass der Zugriff auf ihre Domänen streng reguliert werden muss, was die Verwendung der Funktion „Enthält“ in der TOP-Domäne einschränkt. Das folgende Diagramm erläutert, wie diese Regelung durch die Unterteilung der Domänen in eingeschränkte und unbeschränkte Domänen abgeschwächt werden kann.

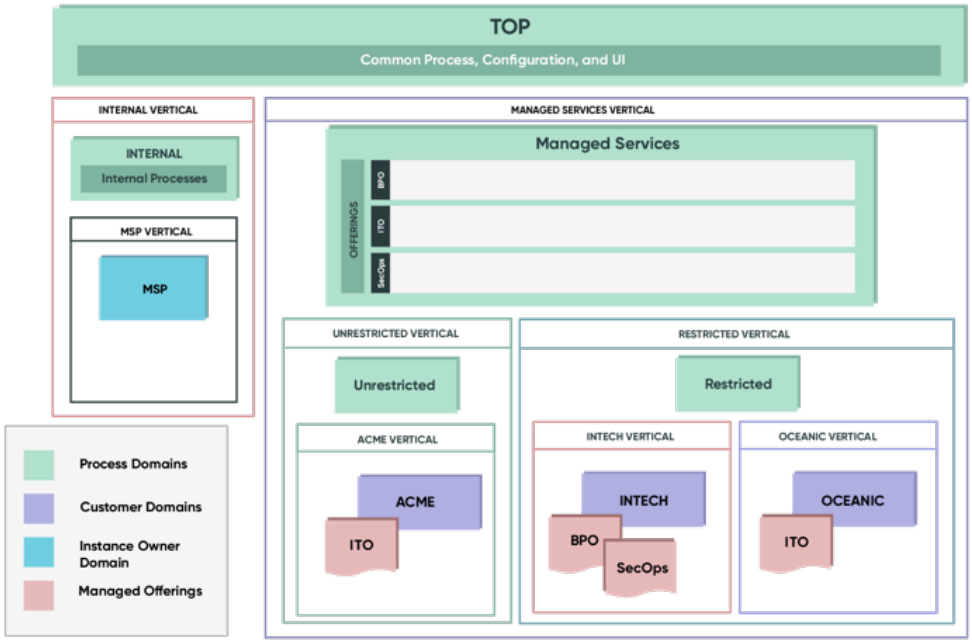
1. Kunden befinden sich in einer bestimmten „Vertikalen“ der Hierarchie der Domänentrennung. Dies bedeutet, dass sie nur Prozesse nutzen, die in ihrer Domäne und allen übergeordneten Domänen in der Hierarchie definiert sind. Alle Prozesse, die in Domänen definiert sind, die sich nicht in ihrer linearen Übergeordnet-Untergeordnet-Hierarchie befinden, gelten nicht.

   Hinweis:
   Kunden oder „Mandanten“ sind Entitäten, die vollständig voneinander getrennt sind, nicht wie Abteilungen oder Geschäftsbereiche, die Ressourcen gemeinsam nutzen.

2. Strikt vertikale Einheiten (beschränkt, Managerservices usw.) sind zulässig, solange die Kunden nur zu einer von ihnen gehören.
3. Services, Produkte oder Angebote, die für alle Kunden horizontal verfügbar sein müssen, werden nicht in separaten Domänenhierarchien definiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



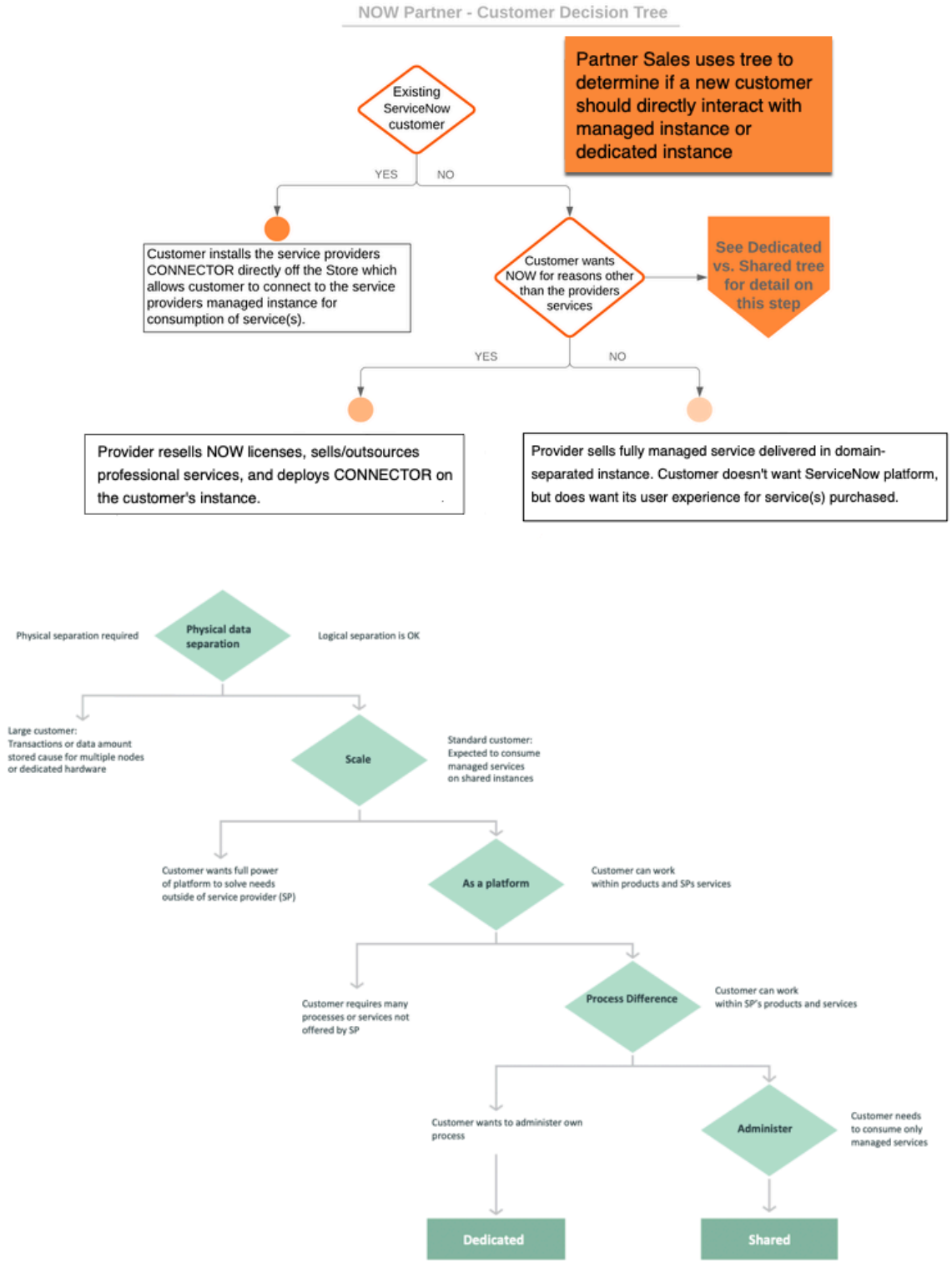
Hier sind einige beispielhafte Anwendungsfälle:

- Sie können beispielsweise unter TOP zwei Domänen erstellen: *Nicht beschränkt* und *Beschränkt*.
  - Platzieren Sie Kunden, die keine SP-Sichtbarkeitsbeschränkungen haben, zusammen mit ihren Domänen unter „Nicht beschränkt“.
  - Platzieren Sie Kunden, die diese Anforderung haben, zusammen mit ihren Domänen unter „Beschränkt“.
- Systemadministratoren können dann die Funktionen „Enthält“ und „Sichtbarkeit“ effizient und gezielt verwenden.
  - Wenden Sie „Enthält“ auf „Nicht beschränkt“ an, sodass ein einziges „Enthält“ den meisten Kunden Sichtbarkeit gewähren kann.
  - Wenden Sie die Domänensichtbarkeit bei Bedarf mithilfe von „Domänensichtbarkeitsgruppen“ auf bestimmte Domänen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kundenentscheidungsbäume

Das folgende Diagramm zeigt, wie Sie das richtige Hierarchiemodell auswählen. Sie können separate Hierarchien, Hybrid-Hierarchien oder freigegebene Hierarchien auswählen, je nachdem, welche Prozesse und Funktionen Sie in Ihren Domänenstrukturen benötigen.



Weitere Informationen zur Hierarchiearchitektur finden Sie unter Referenzarchitektur des Service Providers.

Automatische Übersetzung

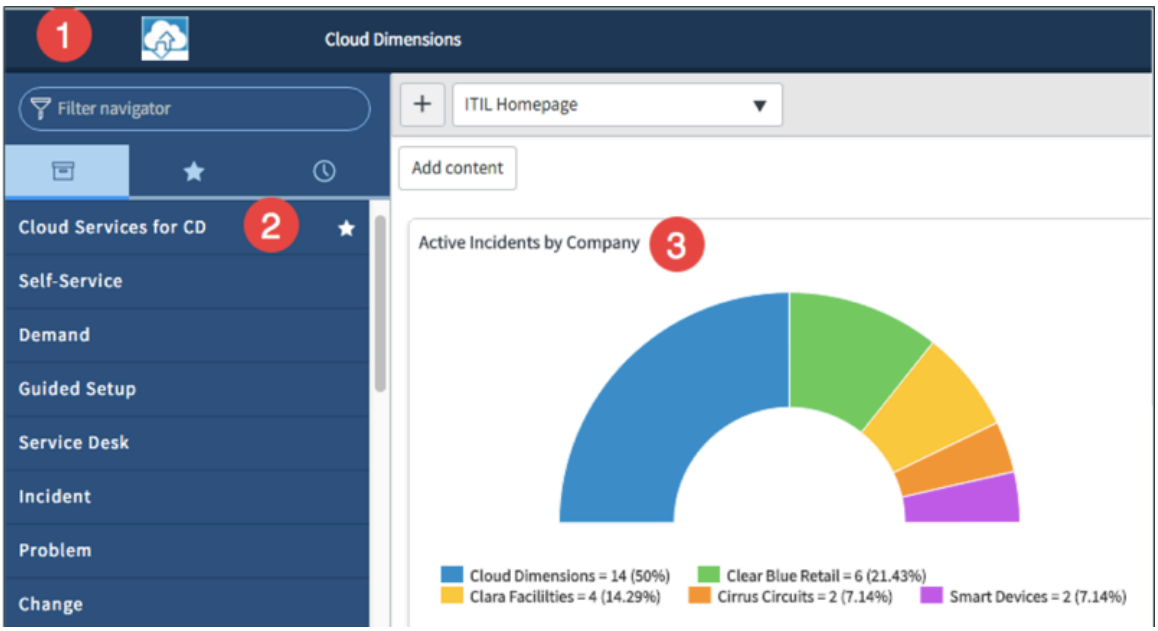
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontext- und Domänentrennung

Der Kontext einer Benutzersitzung bestimmt die Prozesse, Daten und Benutzeroberfläche (UI), während der Benutzer Listenansichten, Homepages, Berichte und Wissensartikel durchsucht. Der Kontext wird durch die von Ihnen erstellten Prozesse, die von Ihnen festgelegten Geschäftsregeln, Ihre Workflows und andere Faktoren bestimmt.

Benutzersitzungskontext

Viele Faktoren bestimmen den Kontext einer Benutzersitzung, z. B. Benutzerprofile, Gruppen, Unternehmenskriterien usw. Im folgenden Diagramm sehen Sie, dass die von einem Unternehmen erstellten Incidents Teil des Kontexts sind.



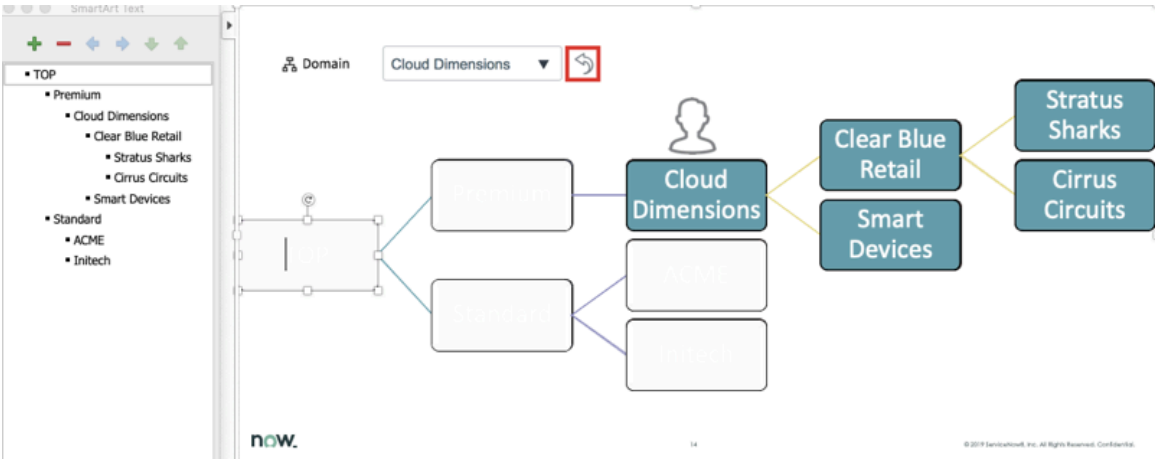
Der Benutzer in diesem Beispiel hat die Domäne „Cloud Dimensions“ (Cloud-Dimensionen).

1. Das Branding spiegelt die Einstellungen in der Domäne Cloud Dimensions und im Unternehmensdatensatz wider.
2. Der Anwendungsnavigator zeigt die Elemente, die von übergeordneten Domänen geerbt werden, sowie die Module, die in der Domäne „Cloud-Dimensionen“ definiert sind.
3. Die Homepages und Listendaten spiegeln die Daten wider, die für den Benutzer sichtbar sind. Diese Daten basieren auf dem Sitzungskontext des Benutzers. In diesem Fall kann der Benutzer in der Domäne „Cloud-Dimensionen“ die Daten in Cloud-Dimensionen, untergeordneten Domänen und der globalen Domäne anzeigen.

Der Benutzersitzungskontext beginnt in der Stammdomäne

Im folgenden Diagramm sehen Sie die Elemente des Kontexts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Systemadministrator legt die Stammdomänen der Benutzer in ihren Benutzerdatensätzen fest. Normalerweise wird die Heimdomäne eines Benutzers auf dieselbe Domäne wie die Domäne seines Unternehmens festgelegt. Wenn sich der Benutzer anmeldet, wird die Domänenauswahl automatisch auf die Stammdomäne des Benutzers festgelegt. Benutzer können jederzeit zu ihrer Stammdomäne zurückkehren, indem sie in der Domänenauswahl auf das Pfeilsymbol klicken.

Die Liste der Domänenauswahl enthält Domänen im Sitzungskontext des Benutzers. Benutzer können ihren Sitzungskontext weiter einschränken, indem sie mit der Auswahl untergeordnete Domänen auswählen.

Der Kontext der Benutzersitzung umfasst die Stammdomäne des Benutzers und alle untergeordneten Domänen. Dieser Satz von Domänen im Sitzungskontext des Benutzers wird automatisch an jede Abfrage angehängt, die an die Datenbank gesendet wird. Auf diese Weise sind die Ergebnisse auf die Daten in diesen Domänen und globale Daten beschränkt. Dieser Prozess ist in den kompilierten Code eingebettet, auf den nicht zugegriffen werden kann.

Servicekonten, die für Integrationen verwendet werden, haben auch einen Benutzersitzungskontext. Es gibt einen Benutzerkontext und einen Datensatzkontext, jeweils mit eigenen Daten in einer eigenen Domäne. Diese Kontexte wirken sich auf die Integrationen aus. Datenbankabfragen (Datensätze) sind auf die gleiche Weise eingeschränkt wie interaktive Benutzer (Benutzer), was bedeutet, dass sie wie gewohnt funktionieren, jedoch durch die vom Entwickler konfigurierten Einschränkungen eingeschränkt sind.

Weitere Informationen zum Hinzufügen von Domänen zum Sitzungskontext eines Benutzers finden Sie unter Referenzarchitektur des Service Providers.

Datensatzkontext

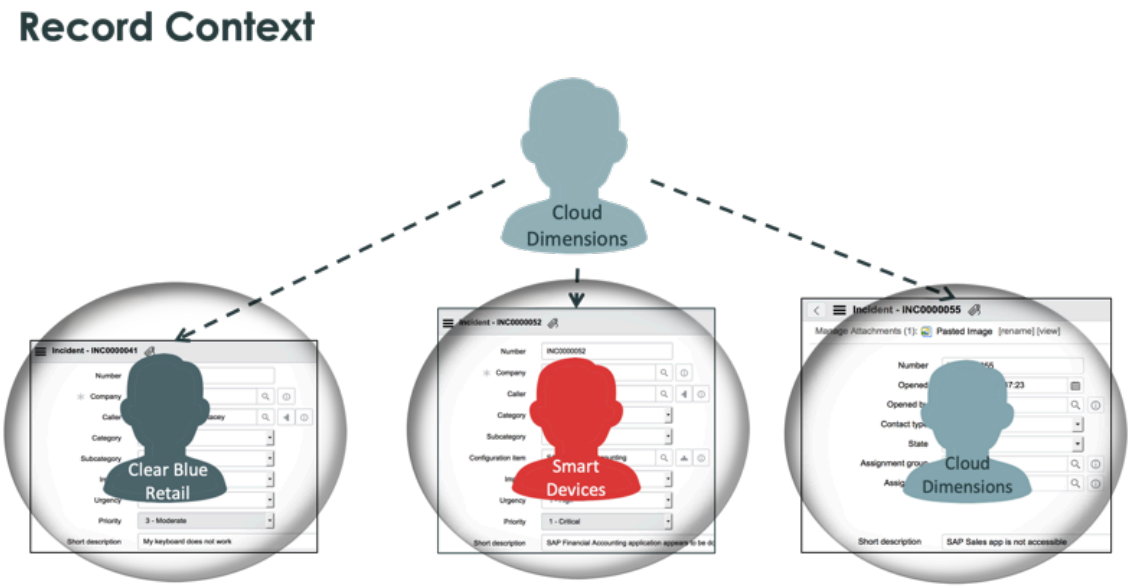
Wenn ein Benutzer einen Drilldown in einzelne Datensätze durchführt, wird der Datensatzkontext aktiviert. Der Datensatzkontext bestimmt die UI-Elemente und Prozesse, die auf den Datensatz angewendet werden sollen.

Die Domäne eines Datensatzes bestimmt den Prozess, die Daten und die Verfügbarkeit von UI-Elementen innerhalb des Datensatzes.

Hinweis:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Datensatzkontext bleibt bestehen, auch wenn sich die Domäne des Benutzers ändert.
- Benutzer können Datensätze gleichzeitig auf mehreren Browserregisterkarten anzeigen, während sie ihren eigenen Datensatzkontext beibehalten.

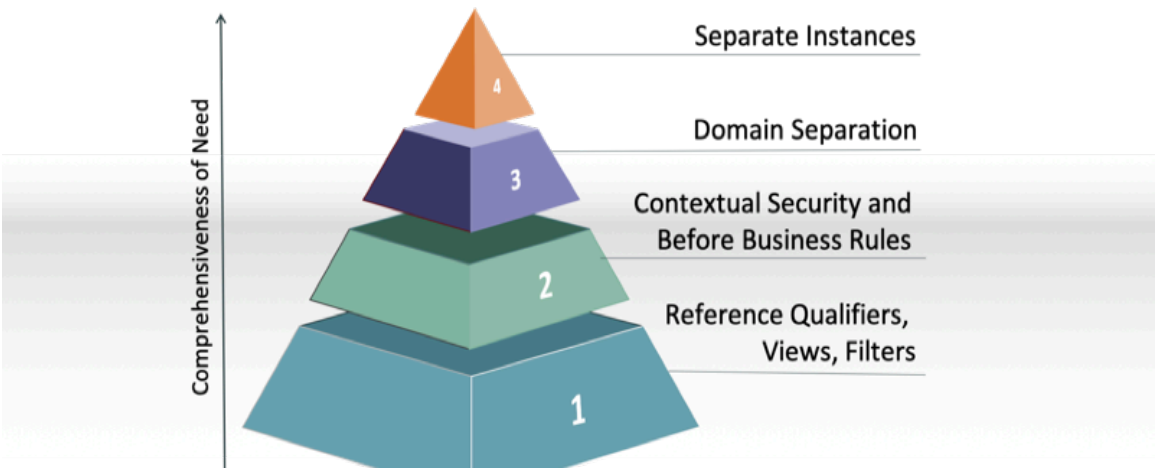


Daten durch Domänentrennung trennen und sichern

Sie können Daten auf der Plattform ServiceNow je nach Kundenanforderungen auf verschiedene Arten trennen und sichern.

Daten auf verschiedene Arten trennen

Das folgende Diagramm zeigt vier Möglichkeiten, wie Sie Daten trennen können. Sie können separate Instanzen, Domänentrennung, kontextbezogene Sicherheits- und Geschäftsregeln und die Referenzarchitektur selbst als Möglichkeiten zum Trennen von Daten verwenden.



Sie können Daten auf diese vier Arten trennen:

1. Die Referenzarchitektur mit Qualifizierern und Filtern anpassen, damit sich Abteilungen und Gruppen innerhalb eines Unternehmens auf ihre eigene Arbeit konzentrieren können. Durch die Trennung der Daten zwischen diesen Abteilungen oder Gruppen kann eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abteilung oder Gruppe die Datensätze einer anderen Abteilung oder Gruppe nicht anzeigen.

2. Kontextbezogene Sicherheit und Geschäftsregeln vom Typ „Vor Abfrage“ als zusätzliche Sicherheitsebenen zum Schutz vor Datenschutzverletzungen hinzufügen. Weitere Informationen zu Domänentrennung und Geschäftsregeln finden Sie unter Kontext- und Domänentrennung und Business Rules „Vor Abfrage“..
3. Eine weitere Sicherheitsebene in einem Unternehmen durch Domänentrennung hinzufügen Die Daten aus jeder Datenbankabfrage sind auf die Daten beschränkt, die in einer Domäne sichtbar sind, bevor kontextbezogene Sicherheits- und Geschäftsregeln ausgeführt werden.
4. Separate Instanzen verwenden, um die Daten auf Datenbank- und Anwendungsebene zu trennen.

Separate Instanzen, Domänentrennung, kontextbezogene Sicherheits- und Geschäftsregeln und die Referenzarchitektur sind Möglichkeiten, Daten zu trennen. Diese vier Möglichkeiten beziehen sich aufeinander, wie durch den Pfeil „Umfangsumfang des Bedarfs“ im Diagramm angezeigt. Wie die einzelnen Ebenen mit den anderen Ebenen interagieren, hängt davon ab, wie Sie die Konfiguration der Domänentrennung einrichten.

Nicht alle Organisationen erfordern eine Domänentrennung. Möglicherweise finden Sie andere Alternativen, z. B. separate Instanzen oder eine einzelne Instanz ohne Domäne. Weitere Informationen zu diesen Alternativen finden Sie unter Bewertung der Notwendigkeit einer Domänentrennung.

Mandantenübergreifende Intelligenz

In einer Multi-Mandanten-Architektur haben Sie eine einzelne Instanz, die mehrere Mandanten bedient. Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten werden automatisch beim Zugriff auf zusätzliche Mandantendaten behandelt.

Einzelmandanten vs. mehrere Mandanten

Einzelmandanten-Instanz

Sie sind Kunde von ServiceNow, haben die Lizenzen erworben und können entscheiden, welche Services Sie benötigen. Sie können jederzeit ein Upgrade durchführen, eine Vorschau der großartigen neuen Funktionen anzeigen und Ihre Instanz sofort konfigurieren. Einzelmandanten haben folgende Vorteile und Einschränkungen:

- Sie haben höhere Vorlaufkosten und einen höheren Verwaltungsaufwand, aber Sie haben mehr Spielraum für Umgestaltung und Erweiterung.
- Sie haben höhere Kosten für die Anschaffung und Wartung der Instanz und des Versorgungsverwaltungspersonals. Sie können die Umgebung zwar nach Bedarf erstellen, müssen jedoch die empfohlenen Vorgehensweisen und Standards von ServiceNow einhalten.

Instanz mit mehreren Mandanten

Eine andere Person besitzt die Instanz, möglicherweise ein Service Provider mit mehreren Kunden. Sie aktualisieren, wann immer sie möchten, und fügen der Instanz neue Services hinzu, wenn sie möchten. Wenn Sie Kunde eines Service Providers sind, befinden Sie sich höchstwahrscheinlich in dessen Instanz, weil Sie das Angebot des Service Providers haben möchten. Mehrere Mandanten haben die folgenden Vorteile und Einschränkungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein zentraler Mitarbeiter verwaltet Konfigurationen, Integrationen und Upgrades.
- Der Instanzbesitzer stellt hinzugefügte Services bereit.
- Domänenmandanten haben geringere Vorlaufkosten für die Verwendung der Plattform ServiceNow, niedrigere monatliche Kosten, da sie sie mit vielen Mandanten teilen, und müssen kein Personal für die Verwaltung der Umgebung einstellen.
- Vorteile, die aus Anforderungen oder Änderungen resultieren, die von anderen Mandanten initiiert werden.

Alternativen zur Domänentrennung

Sie können für Ihre Kunden eine separate Instanz als Alternative zur Domänentrennung verwenden. Eine separate Instanz bietet Ihnen die Flexibilität, die Anforderungen für Datentrennung innerhalb der Gruppen und Abteilungen in einer Organisation mit geringen oder gar keinen Auswirkungen auf andere zu erfüllen.

Separate Instanzen

Vor- und Nachteile separater Instanzen

Separate Instanz	Einzelinstanz – ohne Domäne
Vorteile	**Vorteile**
Konzipiert für jeden Kunden/jedes Unternehmen	Kann einfache Szenarien behandeln
Minimieren Sie die Auswirkungen der Anpassung auf andere	Kosten
Release-Zeitplankoordination	**Nachteile**
Separate Trennung	Umfangreiche Änderungen am Baselinecode
Wählen Sie die Region RECHENZENTRUM aus	Geänderter Basissystemcode, der während Upgrades übersprungen wurde
Nachteile	Muss auch alle sekundären und unterstützenden Tabellen adressieren
Kosten	Umfangreiche Tests erforderlich
Ausrichtung der Instanzen	Kein ServiceNow Produktteam, um Ihren benutzerdefinierten Code weiterzuentwickeln
Testaufwand für Upgrades	
Doppelter Aufwand	
Integrationen erforderlich	

Sie können Upgrades und Releases für jede Instanz separat planen. Wenn Sie sich jedoch für die Verwendung separater Instanzen entscheiden, müssen Sie sich intensiv mit anderen Personen abstimmen, die Instanzen verwalten. Durch die Konfiguration einer Instanz mit kontextbezogener Sicherheit, Formularansichten, Referenzqualifizierern, Filtern und robusten Bedingungen müssen Sie in Ihrem Unternehmen keine Domänentrennung verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit einer separaten Instanz können Sie die Daten- und Prozesstrennung in Angriff nehmen, aber Ihre Instanzbesitzer müssen die umfangreichen Anpassungen verwalten, die für separate Instanzen erforderlich sind.

Zugehörige Informationen

Kontext- und Domänentrennung

Referenzarchitektur des Service Providers

Bewertung der Notwendigkeit einer Domänentrennung

Möglicherweise stellen Sie fest, dass die Domänentrennung für die Organisationen Ihrer Kunden nicht immer funktioniert. Am besten stützen Sie Ihre Entscheidung für die Domänentrennung auf die Bedürfnisse Ihrer Kunden.

Bewertung der Notwendigkeit einer Domänentrennung

Gründe für die Domänentrennung

Diese Faktoren können Ihnen bei der Entscheidung für die Domänentrennung für die Organisationen Ihrer Kunden helfen:

- Ihre Kunden haben eine moderate Ausrichtung von Prozessen und allgemeinen Plattformanforderungen.
- Ihre Kunden planen, Aufgaben als Erfüller und nicht als anfordernde Personen zu bearbeiten.
- Ihre Kunden haben eine vertragliche Vereinbarung, die die Isolierung von Datensätzen erfordert, aber Ihr Instanzbesitzer hat festgestellt, dass die Anforderung an anderer Stelle in der Konfiguration geklärt werden kann.
- Die Instanzbesitzer Ihres Unternehmens verfügen über ganze Entitäten, die als physisch getrennte Organisationen fungieren und keine Daten gemeinsam nutzen. Eine vollständige Berichterstellung ist jedoch weiterhin erforderlich. Getrennte Domänen ermöglichen bei korrekter Konfiguration Datentransparenz.

Gründe dafür, dass keine Domänentrennung erfolgt

Die folgenden Faktoren können auf Gründe hinweisen, warum die Organisationen Ihrer Kunden die Domänentrennung möglicherweise nicht einrichten möchten:

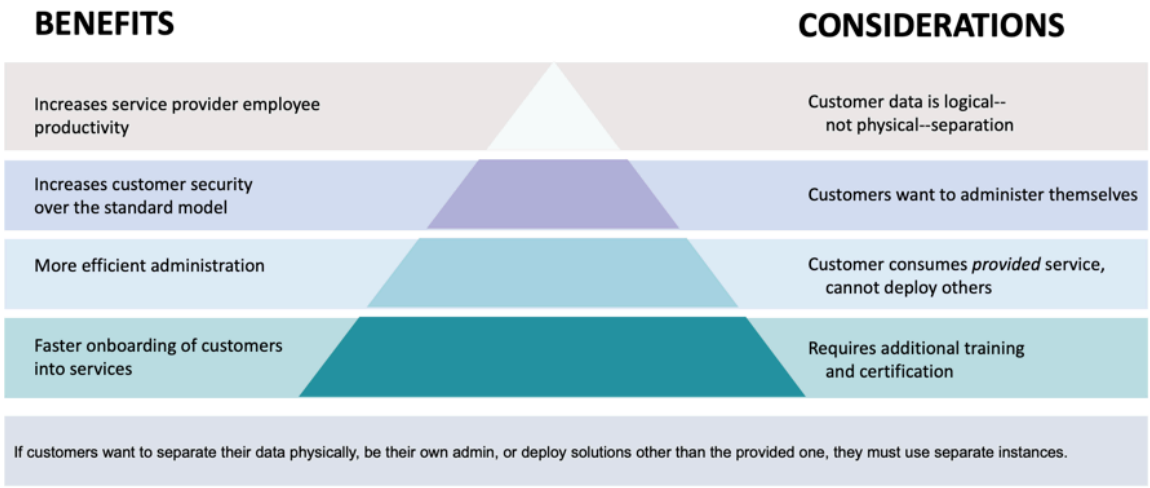
- Ihre Kunden möchten ihre Umgebung verwalten, sie vollständig besitzen und die Roadmap für die Erweiterung festlegen.
- Ihre Kunden verlangen, dass die Daten und Prozesse auf physischer Ebene oder Datenbankebene vollständig isoliert sind.

Hinweis:

Domänengetrennte Instanzen enthalten eine gemeinsam genutzte Datenbank, sodass die Isolationsanforderung unterminiert wird.

- Abteilungen in der Organisation Ihrer Kunden möchten Datensätze isolieren. (Zugriffskontrollen können ausreichen.)
- Ihre Kunden möchten alle ihre eigenen Prozesse, Geschäftsregeln und Workflows.
- Die Unternehmenskultur ist eine der Nicht-Zusammenarbeit zwischen den Organisationen Ihrer Kunden.
- Ihre Kunden interagieren nur als Endbenutzer mit der Plattform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

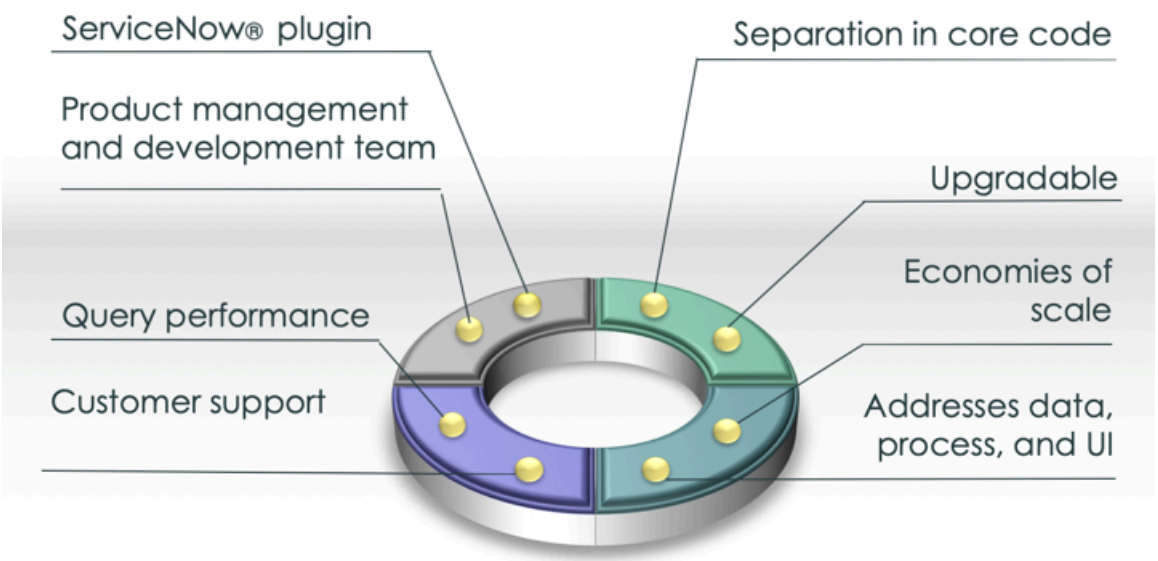


Vorteile der Domänentrennung

Die Domänentrennung funktioniert möglicherweise für die Organisationen Ihrer Kunden besser als jede andere Methode zur Trennung der Daten zwischen Gruppen und Abteilungen.

Vorteile der Domänentrennung auf einen Blick

Sie können die Domänentrennung mit einem ServiceNow -Plugin aktivieren, dessen Funktionalität in die Kernplattform integriert ist. Die Konfiguration der separaten Domänen wird von einem Produktmanager verwaltet, der von einem Entwicklungsteam unterstützt wird. Erweiterungen und Korrekturen für die Funktion zur Domänentrennung sind in den Releases ServiceNow enthalten und können von Kunden verwendet werden. Zur Unterstützung der Domänentrennung können Ihre Instanzbesitzer Kundenservice und Support -Ressourcen verwenden, z. B. das Service Portal .



Funktionsweise einer Datenbankabfrage mit Domänentrennung

Durch die Verwendung von Datenbankabfragen mit Domänentrennung in den Anwendungen Ihrer Kunden können diese ihre Daten schützen. Diese Abfragen beschleunigen dann die Konfigurations- und Build-Prozesse.

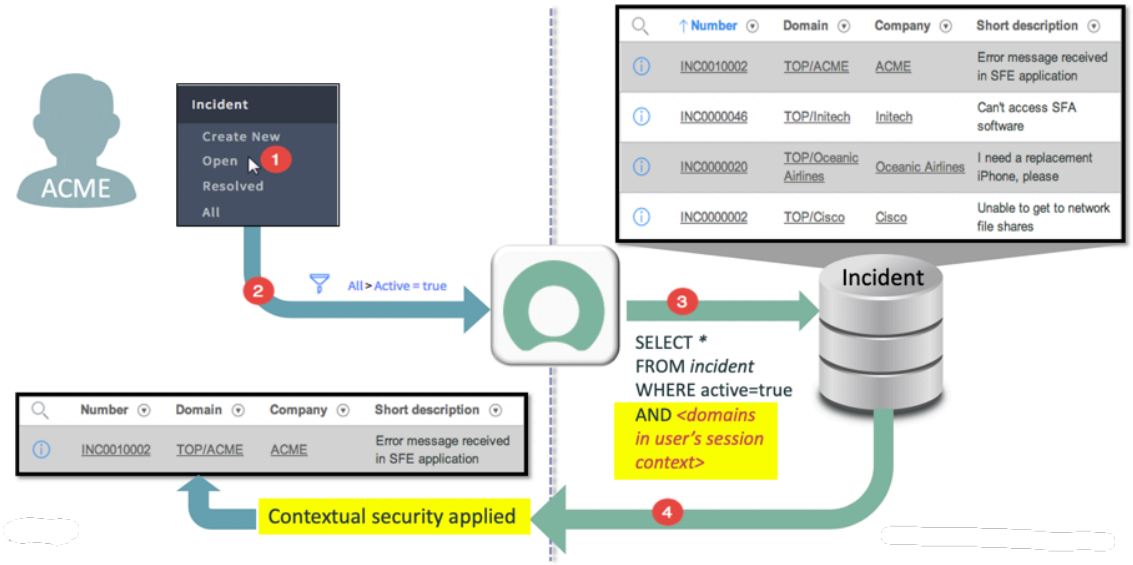
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So schützt die Domänentrennung Daten

In der folgenden Abbildung verfügt die Incident-Tabelle [Incident] über ein Domänenfeld, das von der Aufgabe des Incident geerbt wird. Wenn Sie dieses Domänenfeld sehen, wissen Sie, dass die Datensätze in der Tabelle Domänenzuweisungen haben können.

Wenn sich Benutzer anmelden, wird ihre Heimdomäne mit den Domänen angezeigt, auf die sie zugreifen können. Dies wird als Sitzungskontext des Benutzers bezeichnet. Weitere Informationen zu Sitzungskontexten finden Sie unter Kontext- und Domänentrennung.

Datenbankabfrage mit Domänentrennung



1. In einem Browser wählt der Benutzer eines der Unternehmen, Acme, das Modul „Offene Incidents“ aus, um alle Incidents anzuzeigen, bei denen aktiv = wahr ist.
2. Der Filter active=true wird an die Anwendung übermittelt.
3. Die Anwendung sendet dann eine Abfrage an die Datenbank, indem eine WHERE-Klausel an active=true angehängt wird. Die WHERE-Klausel begrenzt die Incident-Datensätze, die zurückgegeben werden, auf die Datensätze, die sich in der Domäne des Benutzers oder in den Domänen befinden, auf die der Benutzer zugreifen kann. Nur die Datensätze in diesen Domänen werden zur Verarbeitung an die Anwendung zurückgegeben.
4. Kontextbezogene Sicherheit wird angewendet, wodurch die Daten, die an den Benutzer zurückgegeben werden, weiter eingeschränkt werden. Die Incident-Datensätze werden in der Liste „Offene Incidents“ angezeigt.

Hinweis:

Wenn Sie kontextbezogene Sicherheit anwenden, erstellen Sie Grenzwerte für die Daten, die an den Benutzer zurückgegeben werden. Diese Grenzwerte schützen andere Inhalte, die Benutzer möglicherweise nicht sehen sollen.

Weitere Informationen zur kontextbezogenen Sicherheit finden Sie unter Kontext- und Domänentrennung.

Hinweis:

Diese Verarbeitungslogik gilt für alle Abfragen an die Datenbank, einschließlich der Abfragen, die mithilfe von Integrationen ausgelöst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufen für Domänentrennung

Wählen Sie aus drei Kategorien für die Domänentrennung einer Anwendung für die Organisationen Ihrer Kunden.

Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und Datenweiterleitung, verfügen über eine erweiterte Trennung der Geschäftslogik oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kundenebene). Diese Definitionen beschreiben die Supportstufen aus der Perspektive der tatsächlichen Anwendungsfälle und der Personen, die sie implementieren.

Inkrementell ServiceNow Supportstufen

Ebene	Typ	Zusammenfassung
Kein Support		• Das Domänenfeld kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden. • Diese Ebene gilt nicht als domänengetrennt.
Standard	Kundendatenverwaltung	• Geschäftslogik: Stellt sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Service Providers der Anwendung übertragen werden. • In der -Anwendung berücksichtigen Benutzeroberfläche, Cache-Schlüssel, Berichterstellung, Rollups, Zusammenfassungen usw. die Eigenschaften der Domäne zur Laufzeit. • Ihre Instanzbesitzer müssen in der Lage sein, die Anwendung so einzurichten, dass sie für mehrere Mandanten normal funktioniert. Anwendungsfall: Wenn ein Service Provider den Chat verwendet, um auf die Nachricht eines Kunden zu antworten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ebene	Typ	Zusammenfassung
		muss der Client die Antwort sehen können.
Standard	Customer Process Management	• Enthält die Basis-Stufe • Geschäftslogik: Prozesse können vom Service Provider pro Kunde erstellt oder geändert werden. Die Anwendungsfälle spiegeln wider, wie die Anwendung von mehreren Service Provider-Kunden in einer einzigen Instanz verwendet wird. • Ihre Instanzbesitzer müssen in der Lage sein, die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Kunde für die spezifische Anwendung zu konfigurieren. Anwendungsfall: Der Administrator muss in der Lage sein, Kommentare erforderlich zu machen, wenn ein Datensatz für einen Kunden geschlossen wird, aber nicht für einen anderen Kunden.
Erweitert	Selbstverwaltete Konfiguration des Kunden	• Enthält Basis- und Standard-Ebenen • Ermöglicht Service Provider-Kunden, Geschäftslogik zu ändern, die auf definierten Anwendungsfällen basiert. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass sich Konfigurationen durch einen Kunden nicht auf einen anderen Kunden auswirken können. • Die Instanzkunden müssen in der Lage sein, die MVP-Geschäftslogik und -Datenparameter selbst zu konfigurieren. Anwendungsfall: Der Kunde einer freigegebenen Umgebung muss in der Lage sein, Änderungen entsprechend Auswirkung, Dringlichkeit oder Priorität innerhalb einer Domäne vorzunehmen.
Effektive Domäne*		In einigen Fällen kann eine Plattformfunktion oder -anwendung Anwendungsfälle von Service Providern unterstützen, auch wenn das Domänen-Framework nicht verwendet wird. Die Anwendungsfälle müssen detailliert beschrieben werden, um die Domänentrennung zu unterstützen. Ein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ebene	Typ	Zusammenfassung
		Sternchen (*) nach der Supportstufe zeigt diese Art von Konfiguration an. Anwendungsfall: Vor dem New York-Release hatte Servicekatalog keinen Domänensupport, aber die Instanzbesitzer konnten mithilfe von Benutzerkriterien separate Kataloge und Elemente für jeden Mandanten in einer domänengetrennten Instanz konfigurieren. Das Ergebnis war, dass jeder Mandant Service Catalog auf einer Standardebene verwenden konnte.

Informationen zum Anzeigen aller Anwendungen nach Support-Stufe finden Sie unter Anwendungssupport für die Domänentrennung.

Zusammenfassung

Die Domänentrennung ist ein Framework, das Sie verwenden müssen, um Ihre Anwendungen auf die Kunden aufmerksam zu machen.

Berücksichtigen Sie die Fähigkeiten des Domänen-Frameworks, die Geschäftsanwendungsfälle Ihrer Anwendungen, die Personas und die Verwendung der Anwendung, bevor Sie das Framework verwenden können, um Ihre Anwendung unterstützt zu machen.

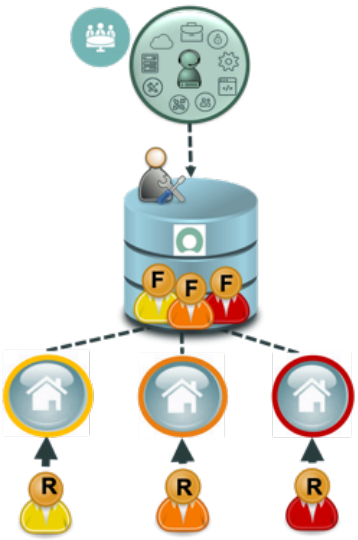
Referenzarchitektur des Service Providers

Ihre Kunden können über ein Portal, mit dem sie ihre domänengetrennte Instanz erreichen können, auf Services von Service Providern (SP) zugreifen.

Grundlegende Attribute der Service Provider-Referenzarchitektur

- Sie weisen einer Domäne keine Erfüller zu. Stattdessen geben Sie sie domänenübergreifend frei. Dadurch wird es schwieriger zu prüfen, wie viele Erfüller Sie pro Domäne haben.
- Sie können die Domänenverwaltung freigeben und nutzen. Das bedeutet, dass es keinen Overhead gibt und Sie die Lizenzen optimieren können.
- Die Anzahl der Benutzer in der Instanz kann sich ändern, wenn Sie einen neuen Kunden gewinnen. Ein neuer Kunde kann zu zehn- oder sogar hunderttausend neuen Benutzern im System führen. Die Gesamtanzahl der Benutzer in einer gemeinsam genutzten Umgebung ist praktisch unbegrenzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- SP customers access SP services via a portal to the SP Domain Separated instance
- SP uses ServiceNow shared instance(s) to manage their service delivery
- SP could have a shared instance per region to support data sovereignty requirements

Legend:

Centralized governance at the SP

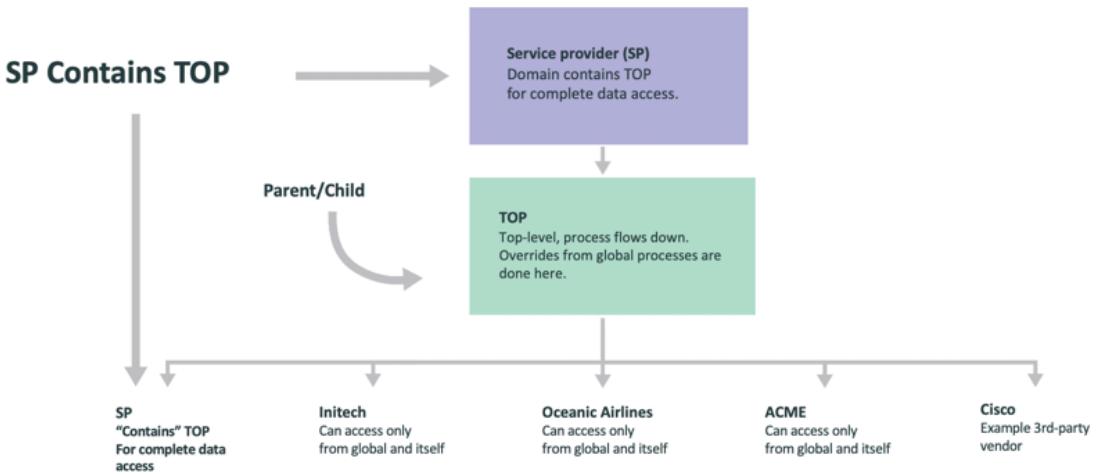
Centralized administration at the SP. Shared business requirements and configurations

Both SP and customer fulfillers on one instance

Customer requesters on each instance

Das Portal für SP-Services ist für die freigegebene SP-Instanz dediziert oder freigegeben. Service Provider verwenden ServiceNow gemeinsam genutzte Instanzen, um ihre Servicebereitstellung zu verwalten.

Referenzhierarchie für domänengetrennte Instanzen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SP-Referenzarchitekturvergleich

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

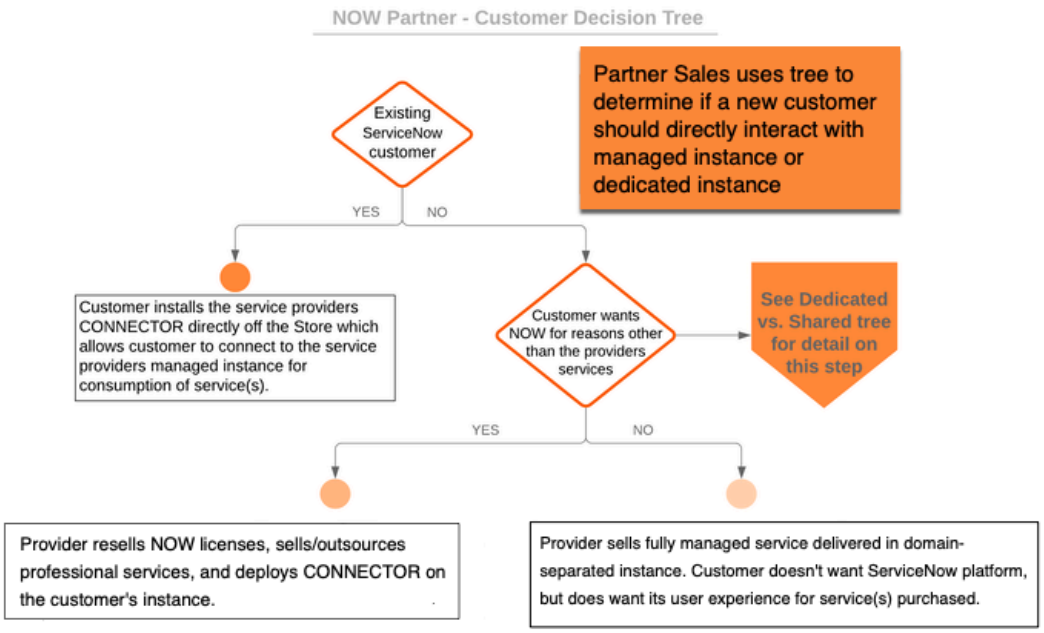
Entscheidungsstrukturen der Service Provider-Referenzarchitektur

Sie können Entscheidungsstrukturen und ein Vergleichsdiagramm verwenden, um zu bestimmen, ob ein neuer Kunde zu einer freigegebenen Instanz oder zu seiner eigenen dedizierten Instanz hinzugefügt werden soll.

Entscheidungsstrukturen

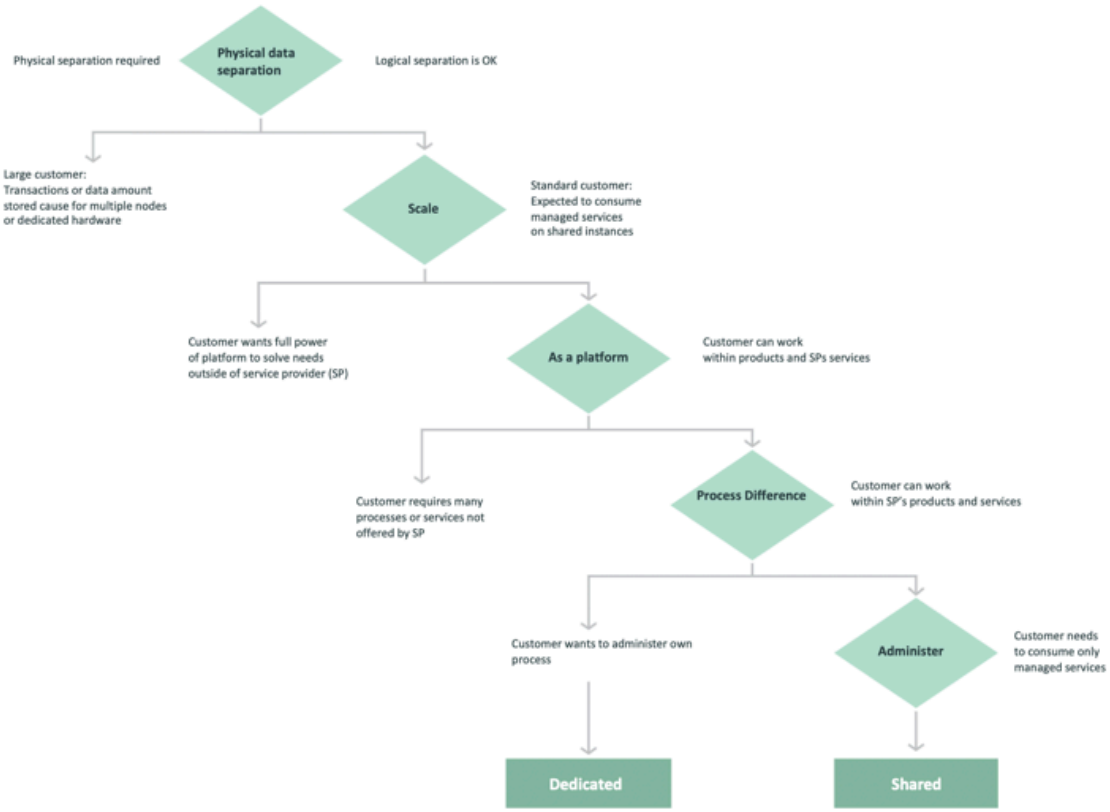
Verwenden Sie diese Entscheidungsstrukturen, um Ihren Kunden bei der Entscheidung zu helfen, ob eine verwaltete oder eine dedizierte Instanz verwendet werden soll.

Entscheidungsstruktur des Kunden



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



SP-Referenzarchitekturvergleich

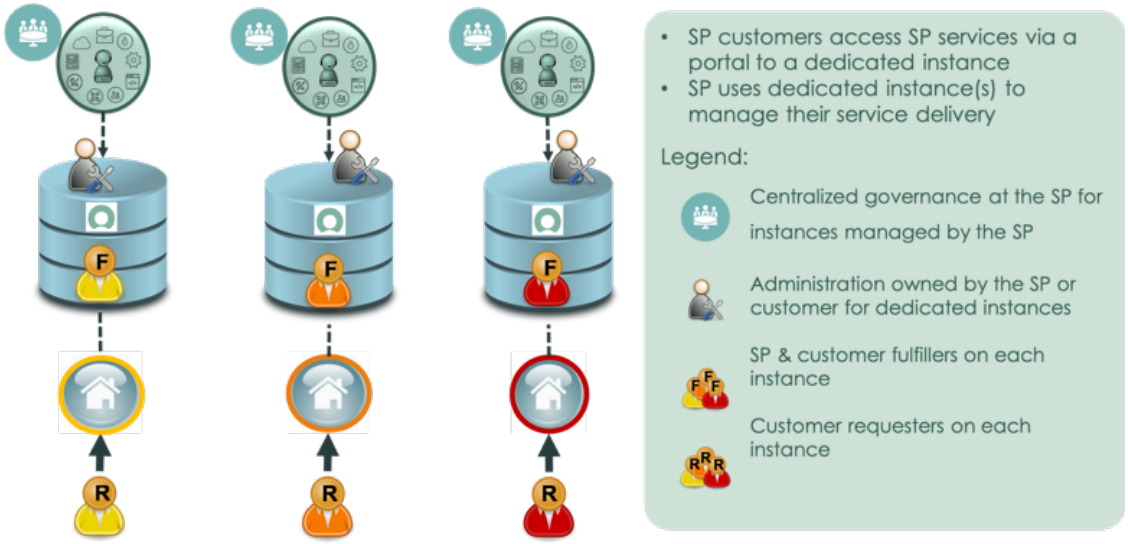
Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Service Provider-Referenzarchitektur für dedizierte Instanzen

Kunden von Service Providern (SP) können über ein Portal zu einer dedizierten Instanz auf SP-Services zugreifen. SPs verwenden diese dedizierten Instanzen, um ihre Servicebereitstellung zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dedizierte Instanzen



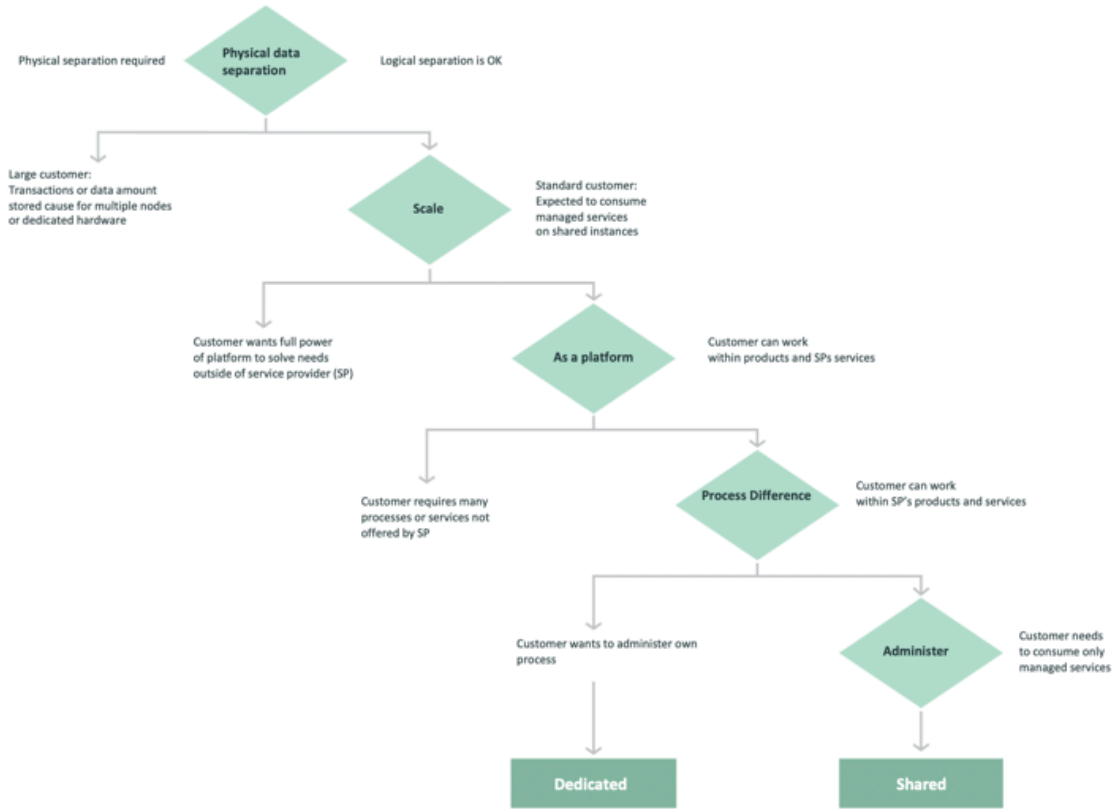
Attribute

- Dedizierte Instanzen erfordern eine separate Verwaltung und dedizierte Teams. Sie benötigen mehrere Lizenzen für die Administratoren und Entwickler, die sich bei mehreren Instanzen anmelden.
- Jede Instanz hat eine begrenzte Anzahl von anfordernden Personen und Erfüllern. Wenn Sie einen neuen Kunden gewinnen, müssen Sie eine Instanz beschaffen, die auf der Größe und dem Umfang des Unternehmens Ihres Kunden basiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Freigegebene Instanz

Dedizierte vs. gemeinsam genutzte Instanz



SP-Referenzarchitekturvergleich

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Service Provider-Referenzarchitektur für Hybrid

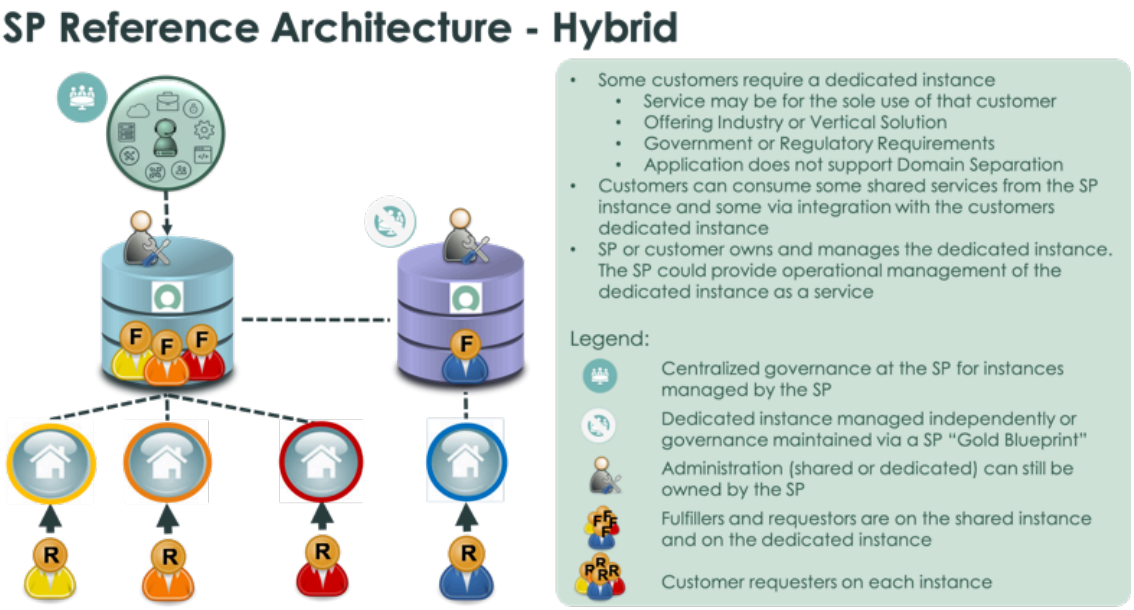
Verwenden Sie die Referenzarchitektur des hybriden Service Providers (SP) für eine benutzerdefinierte Lösung. Ihre Kunden benötigen eine dedizierte Instanz für einen bestimmten Service. Sie können die gemeinsam genutzte SP-Instanz weiterhin für andere Services verwenden, dies erfordert jedoch die Integration jeder Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hybride Architektur

Ihr Kunde ist möglicherweise direkt für die Bereitstellung dieses zusätzlichen Service verantwortlich. Sie müssen eine Hybridlösung mit mehreren Attributen erstellen, die Ihr Kunde bereitstellen kann.



Attribute

- Sie können die Verwaltung der Instanz freigeben und nutzen. Das bedeutet, dass es keinen Overhead gibt und Sie die Lizenzen optimieren können.
- Wenn es eine neue Instanz für eine dezentrale Umgebung gibt, ist das Programmteam verantwortlich und wird entsprechend als dedizierte Administratorbenutzer für diese Instanz finanziert. In einer zentralisierten Umgebung, in der alle Instanzen aus einer Blaupause stammen, benötigen Sie doppelte Verwaltungslizenzen.
- Sie weisen einer Domäne keine Erfüller zu. Stattdessen können Sie sie domänenübergreifend freigeben.
- Wenn ein Kunde sowohl eine freigegebene als auch eine dedizierte Umgebung gemeinsam nutzt, benötigt er einen Erfüller in beiden Umgebungen. Dies bedeutet mehr Arbeit für jedes Team, da die Prozesse für freigegebene und dedizierte Instanzen unterschiedliche Arbeit für jede Instanz erfordern.
- Die Anzahl der Benutzer in der Instanz kann sich ändern, wenn Sie einen neuen Kunden gewinnen. Ein neuer Kunde kann zu zehn- oder sogar hunderttausend neuen Benutzern im System führen. Die Gesamtanzahl der Benutzer in einer gemeinsam genutzten Umgebung ist praktisch unbegrenzt.
- Jede Instanz hat eine begrenzte Anzahl von anfordernden Personen und Erfüllern. Wenn Sie einen neuen Kunden gewinnen, müssen Sie eine Instanz beschaffen, die auf der Größe und dem Umfang des Unternehmens Ihres Kunden basiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SP-Referenzarchitekturvergleich

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

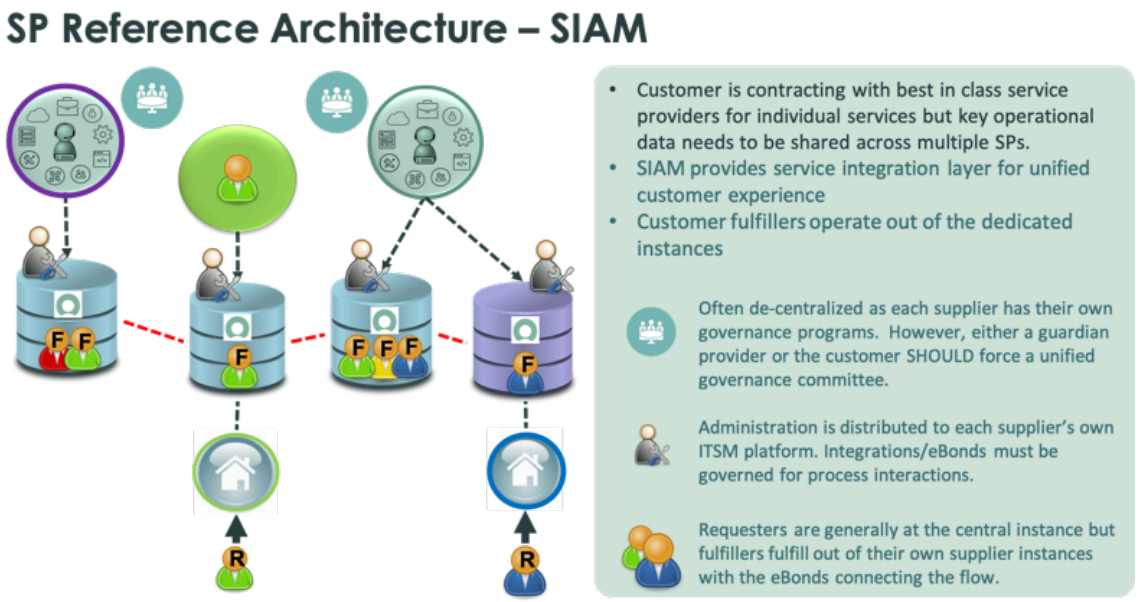
Service Provider-Referenzarchitektur für Service Integration and Management (SIAM) (SIAM)

Die Architektur Service Integration and Management (SIAM) Service Integration and Management (SIAM) für Service Provider (SP) integriert Services für eine einheitliche Kunden-Experience.

Attribute der SIAM-Architektur

- Kunden greifen auf SP-Services über ein dediziertes oder freigegebenes Portal zur freigegebenen SP-Instanz zu.
- SPs verwenden ServiceNow gemeinsam genutzte Instanzen, um ihre Servicebereitstellung zu verwalten.

SIAM-Architektur auf einen Blick



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SP-Referenzarchitekturvergleich

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

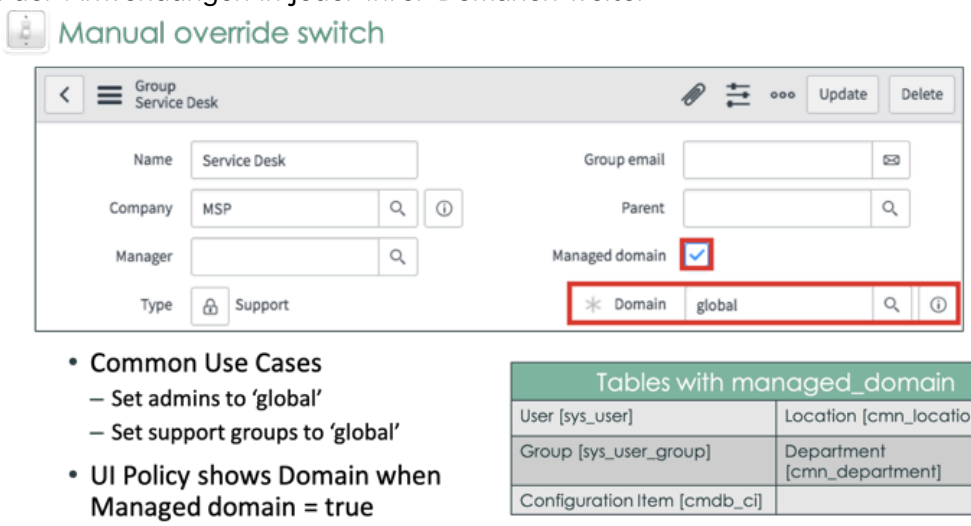
Bedingungen für Domänentrennung

Mit einer ServiceNow -Instanz können Sie die Effizienz verbessern, die Sicherheit erhöhen und die Leistung für Ihre Kundenorganisationen steigern. Es ist hilfreich, einige der häufigsten Begriffe zu verstehen, wenn Sie Ihre Konfigurationen erstellen.

Verwaltete Domäne

In einer verwalteten Domäne können Domänenadministratoren im Feld **Verwaltete Domäne** manuell eine Domäne für den Benutzer-, Gruppen-, Abteilungs-, Standort- oder CI-Datensatz auswählen, anstatt die Domäne zu verwenden, die automatisch aus dem Unternehmensdatensatz zugewiesen wird.

Wenn Sie diese Eigenschaften ändern möchten, können Sie sie überschreiben, um die Funktionen der Anwendungen in jeder Ihrer Domänen weiter



- Common Use Cases
  - Set admins to 'global'
  - Set support groups to 'global'
- UI Policy shows Domain when Managed domain = true

Tables with managed_domain	
User [sys_user]	Location [cmn_location]
Group [sys_user_group]	Department [cmn_department]
Configuration Item [cmdb_ci]	

anzupassen.

Prozesstabellen

Wenn in Prozesstabellen ein Wert im Feld Überschreibungen **[sys_overrides] angezeigt** wird, ist ein Prozessüberschreibungsdatensatz vorhanden. Das bedeutet, dass die delegierte Verwaltung in Kraft ist, mit der Administratoren domänenspezifische Richtlinien

Automatische Übersetzung

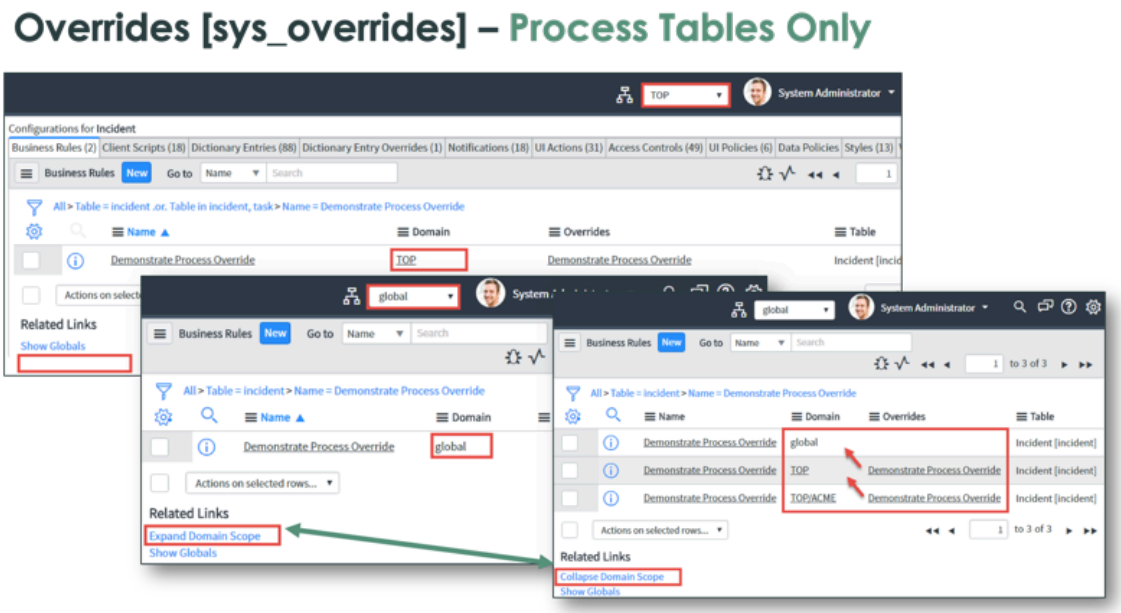
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

festlegen können. Administratoren in der globalen Domäne können den zugehörigen Link Domänenbereich **erweitern/reduzieren** verwenden, um Überschreibungsdatensätze anzuzeigen.

Hinweis:
Berichte sind in Domänen unterteilt und enthalten ein **Überschreibungsfeld**. Um alle Berichte aus der globalen Domäne anzuzeigen, verwenden Sie den zugehörigen Link **Domänenbereich erweitern**.

Wenn Sie Prozesstabellen aus einer Domäne anzeigen, werden nur die relevanten Prozessdatensätze für die ausgewählte Domäne angezeigt. Wenn Sie eine Prozesstabelle aus der globalen Domäne anzeigen, wird der zugehörige Link **Domänenbereich erweitern** angezeigt, damit Sie alle Prozessdatensätze einschließlich Überschreibungen anzeigen können. Um nur die relevanten Prozessdatensätze für global anzuzeigen, verwenden Sie den zugehörigen Link **Domänenbereich reduzieren**.

Die Domänenbereichsfunktion wird nur für Prozesstabellen verwendet und bewirkt, dass sich die Sichtbarkeit von Daten in der Tabelle in die entgegengesetzte Richtung verschiebt. Beispielsweise kann ein Datensatz in der übergeordneten Domäne in der untergeordneten Domäne angezeigt werden, ein übergeordnetes Element kann jedoch keinen untergeordneten Datensatz sehen. Dadurch kann der Prozess in untergeordnete Domänen fließen.



Typen von Domänen

Verschiedene Arten von Domänen können Ihnen helfen, Ihre Prozesse und Daten und ihre Funktionsweise in der Anwendung oder Funktion zu organisieren.

Kundendomäne

In der Domäne des Kunden befindet sich die Benutzeroberfläche sowie der Prozess, der steuert, wie die Daten verwendet werden.

Die ACME-Domäne in der folgenden Abbildung ist eine Kundendomäne.

Prozessdomäne

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie erstellen Prozesse dafür, wie die Daten verwendet werden und was sie in der Domäne tun. Diese Prozesse müssen die folgenden Attribute aufweisen:

- Spezifische Prozesse und UI-Einstellungen für eine Reihe von Domänen
- Keine Kerndaten jeglicher Art (z. B. bestimmte Benutzerdaten).
- Die TOP-Domäne in der folgenden Abbildung ist eine Prozessdomäne.

Datendomäne

Die Datendomäne enthält Daten, die für mehrere Kunden relevant sind. Diese Daten können freigegeben werden, ohne die tatsächlichen Kundendomänen freizugeben. Jeder Kunde hat eine eigene Datendomäne und kann darauf zugreifen.

Hinweis:

Diese Art von Domäne ist nicht üblich und kann bei übermäßiger Verwendung zu Leistungsproblemen führen. Konsultieren Sie vor der Verwendung einen SP-Architekten.

Beispiel: Die Domäne enthält möglicherweise Aufgaben, mit denen ACME, Cisco und der SP alle interagieren müssen.

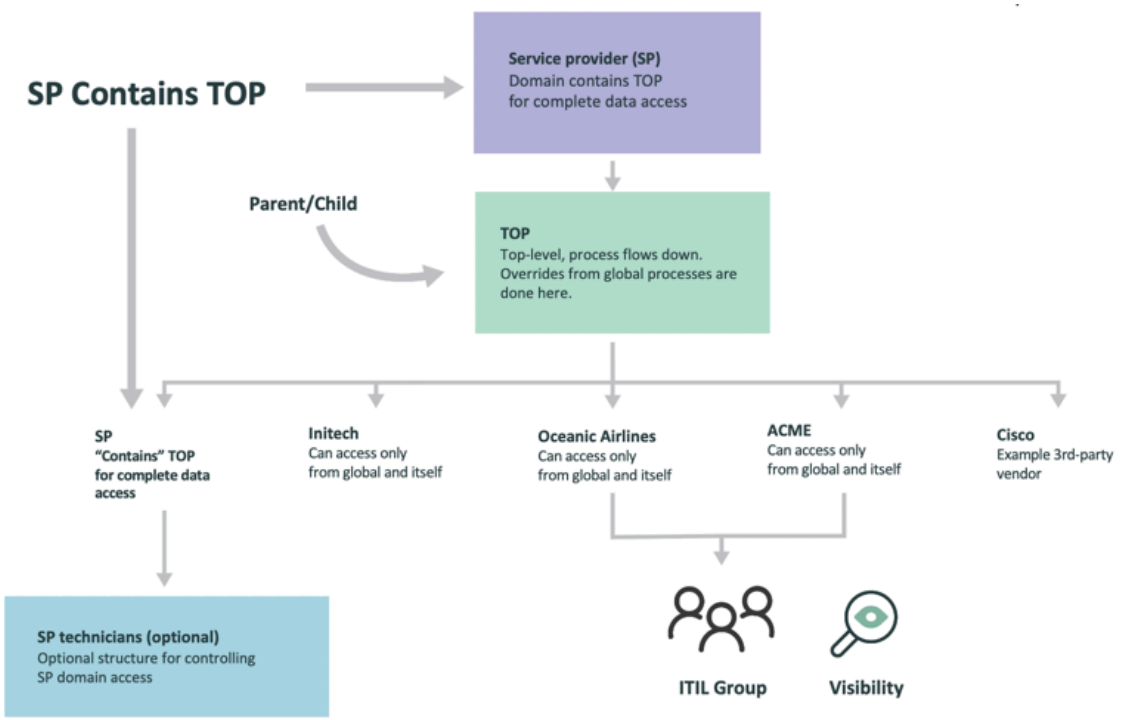
Die Standarddomäne in der folgenden Abbildung ist eine Datendomäne.

Benutzerdaten

Benutzerdatensatzdaten gehören niemals in die globale Domäne oder eine der Prozessdomänen. Benutzer werden hauptsächlich in Kundendomänen erstellt und können gelegentlich in Datendomänen erstellt werden.

Administratorkonten sind etwas Besonderes, da sie nicht als normale Benutzer der Instanz verwendet werden sollten und sich in der globalen Domäne befinden sollten, um administrative Funktionen zu erleichtern.

Domänenhierarchie



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen, Administrator, globaler Prozess

Listen

Wenn Sie in der globalen Domäne mit der rechten Maustaste auf die Bezeichnung eines Auswahlfelds klicken, Auswahlmöglichkeiten **konfigurieren**auswählen und dann eine neue Auswahl hinzufügen, wird die Auswahl automatisch in alle domänenspezifischen Listen für dieses Feld verschoben. Wenn die neue Option als **Ausgewählt**markiert ist, wird sie als aktiv hinzugefügt. Wenn die neue Option als **Verfügbar**markiert ist, wird sie als inaktiv hinzugefügt.

Instanzenverwaltung

Die Administratoren des Instanzbesitzers müssen die normale Erstellung, Änderung und Wartung von Prozessen in einer domänengetrennten Instanz durchführen. Einzelne Domänenmanager können einige Teile datengesteuerter Prozesse verwalten. Die Typen von Domänenmanagern verwalten die Benutzerverwaltung, unterstützen Gruppenmitgliedschaften und Standorte oder verwalten Anwendungen, die für die Mandantenverwaltung entwickelt wurden.

Globaler Prozess/Parameter

Sie können den Prozess erstellen und verwalten, der sich auf die globale Domäne auswirkt, und die Parameter festlegen. Diese Eigenschaften gelten für alle Benutzer einer domänengetrennten Instanz.

Beispiele: Systemeigenschaften, Außerkraftsetzung des Wörterbuchs, sys_documentation (Feldbezeichnungen), Datenmodell (Klassen, CI-Typen usw.), Tabellen und Felder [sys_dictionary] (Zugriff kann eingeschränkt werden), Indizierung (Textverzeichnisse sowie Datenbank) , ACLs, Installationsausgänge, eingehende Aktionen, öffentliche Seiten und Interceptors.

Trennen Sie eine benutzerdefinierte Tabelle nach Domänen

Möglicherweise müssen Sie benutzerdefinierte Tabellen in separaten Domänen erstellen. Dieses Thema behandelt sowohl das Verfahren als auch das Konzept hinter der Domänentrennung einer benutzerdefinierten Tabelle.

1. Erstellen Sie ein sys_domain-Feld

Hinweis:
Wenn eine Systemtabelle oder eine Tabelle nicht vom Plugin „Domain Separation“ nach Domänen getrennt wurde, ist es am besten, sie nicht nach Domänen zu trennen.

Verwenden Sie diese Punkte als Leitlinie, um ein sys_domain-Feld zu erstellen.

- Erstellen Sie ein neues Feld als Typ *domain_id*.
  - Spaltenname: sys_domain
  - Andere Attribute: Automatisch definiert
- Sys_domain_path wird automatisch erstellt.

Der Spaltenname **sys_domain** ist in Now Platformreserviert, was bedeutet, dass das System ihn erkennt und automatisch den entsprechenden Feldtyp und die entsprechenden Attribute für Sie anwendet. Diese automatische Konfiguration erstellt auch ein entsprechendes Feld **sys_domain_path**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie den Spaltennamen auf `sys_domain` fest, anstatt die Bezeichnung zu verwenden.
- Domänentrennung ist nicht für jede Tabelle geeignet. Wenn eine Tabelle Teil der Basisinstanz ist und diese Tabelle kein **sys_domain** -Feld enthält, sollten Sie dies im Allgemeinen so belassen.

Ein Feld **sys_domain** wird automatisch erstellt, wenn Sie ein Feld vom Typ „domain_id“ mit dem Namen „sys_domain“ erstellen.

2. Fügen Sie eine Geschäftsregel hinzu, um die Domäne festzulegen

Ohne Geschäftsregeln

Die Domäne wird auf die aktuelle Domäne des Benutzers festgelegt, der den Datensatz erstellt.

Mit Geschäftsregeln

Die Domäne wird mithilfe von geskripteter Logik zugewiesen, in der Regel basierend auf dem Feld „Unternehmen“.

Zusätzlich zu einem `sys_domain`-Feldbenötigen benutzerdefinierte Tabellen eine Geschäftsregel ähnlich wie **Domäne - Domäne festlegen - Aufgabe**, um den Wert des Domänenfelds festzulegen. Darüber hinaus benötigen Sie **Domäne – Standard – Aufgabe**, das Datensätze ohne Domäne in die Standarddomäne verschiebt, wenn die erste Regel keine Domäne zuweist.

Überprüfen Sie in der Aufgabentabelle die Geschäftsregeln für die Domäne. Achten Sie besonders auf das Feld Reihenfolge. Die Priorität der Ausführung wird durch das Feld Reihenfolge von niedrig nach hoch angegeben.

Die erste ausgeführte Regel, **Domäne – Domäne festlegen – Aufgabe**, versucht, die Domäne des Datensatzes basierend auf der Domäne des Unternehmens des Datensatzes festzulegen.

Wenn die erste Regel keine geeignete Domäne findet, wird die zweite Regel **Domäne – Standard – Aufgabe**ausgeführt. Diese Regel legt die Domäne des Datensatzes auf die Standarddomäne fest.

Wenn sich schließlich die Domäne eines Aufgabendatensatzes ändert, ändert die Geschäftsregel **Domäne – Kaskadierende Domäne – Aufgabe** die Domäne für alle Datensätze, die sich auf die Aufgabe beziehen, z. B. Workflows, Metriken, SLAs und Anhänge.

3. Fügen Sie eine Geschäftsregel hinzu, wenn Schritt 2 fehlgeschlagen ist

Wenn die anfängliche Geschäftsregel keine Domäne festlegen kann und die Domäne noch leer oder global ist, wird eine zweite Geschäftsregel ausgeführt. Diese Regel untersucht das Feld `task_for`, das auf dem Feld caller oder `requested_for` basiert. Diese Regel überprüft, ob Sie die Domäne des Datensatzes basierend auf der Domäne des Benutzers festlegen können. Wenn nicht, legt die Geschäftsregel die Domäne auf die Standarddomäne fest.

Es folgt ein Beispielskript für die Geschäftsregel:

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
  set the domain to the default domain
*/
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Domäne – kaskadierende Domäne – Aufgabe

Aufgaben können viele zugehörige Tabellen haben, die für Geschäftsziele zusammenarbeiten. Zu diesen zugehörigen Datensätzen gehören Workflow, SLA, Genehmigungen, Anhänge und E-Mail. Wenn sich die Domäne einer Aufgabe ändert, muss sich auch die Domäne der zugehörigen Datensätze ändern, damit sie für Benutzer in der neuen Domäne sichtbar bleiben.

Diese Kaskadenregel wird häufig ausgelöst, wenn Sie Datensätze aus der Standarddomäne löschen.

Die zugehörigen Datensätze für eine im Skript enthaltene kaskadierende Domäne werden ähnlich wie im folgenden Beispiel angezeigt:

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

Domäneneigenschaften und -designs anpassen

Sie können die Unternehmenseigenschaften und Designs Ihrer Kunden innerhalb der von Ihnen konfigurierten Domänen anpassen. Durch die Anpassung werden die Instanzen an das allgemeine Erscheinungsbild des Unternehmens angepasst.

Anpassen von Unternehmensdesigns und -logos

Im Unternehmensdatensatz können Sie bestimmte Designthemen und Logos für jedes Unternehmen anpassen.

Passen Sie die Domäne an

Wenn Sie das Service Provider-Plugin installiert haben, bewirken die in den Kerntabellen enthaltenen Standardgeschäftsregeln standardmäßig, dass die Domäne des Datensatzes auf die Domäne des Unternehmens festgelegt wird, das dem Datensatz zugeordnet ist. Das Unternehmen kann die Tabellen wie Aufgabe, Benutzer, Gruppe, Standort, Abteilung usw. steuern.

Mit allen dieser Tabellen, mit Ausnahme der Aufgabentabelle, können Sie die Domäne überschreiben, in der ein Datensatz erstellt wird. Dadurch haben Sie weitere Anpassungsoptionen.

Domänentrennung für bestimmte Verwendungszwecke verwalten

Sie können separate Domänen für E-Mail-Benachrichtigungen einrichten und die Eigenschaften von Katalogen, Tabellen, Benutzern, Gruppen und Ansichten anpassen. Auf diese Weise können Sie spezifischeres Verhalten in jeder Domäne bereitstellen, was Ihren Kunden mehr Flexibilität gibt.

E-Mails

Sie können separate Domänen für E-Mail-Benachrichtigungen und Überschreibungen verwenden. Wenn Sie separate Domänen für Benachrichtigungen verwenden, können Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Überschreibung durchführen, die nur auf der Domäne des angehängten Datensatzes und nicht auf der gesamten Domäne des Benutzers basiert.

Servicekatalog

Der Servicekatalog ist jetzt domänengetrennt, sodass Ihre Kunden den Katalog anzeigen und darauf zugreifen können. Elemente werden als ODER-Bedingungen verarbeitet, wenn mehrere Elemente verwendet werden. Service Provider sollten die Kategorien und Elemente selbst verwalten, damit sie speziell auf ihre eigenen Kriterien abgestimmt sind.

Benutzer und Gruppen

Verwenden Sie nur Administratorkonten in der globalen Domäne, da Administratoren Zugriff auf alle Domänen benötigen. Führen Sie alle Anwendungstests in einer tatsächlichen Domäne durch, nicht in der globalen Domäne. Überschreibungen werden in der globalen Domäne nicht ordnungsgemäß verarbeitet. Administratoren sollten auch Benutzerkonten in der Produktion erhalten, wenn sie die Anwendung verwenden sollen.

Mit Feldern arbeiten

Bei der Arbeit mit Feldern sind mehrere Punkte zu beachten. Achten Sie genau auf diese Felder, da sie viele Variationen aufweisen können, die sich auf Ihre Konfigurationen auswirken.

Lists

Es gibt persönliche, globale und Domänenlisten sowie jeweils mehrere Ansichten.

Formulare

Es gibt globale und Domänenlisten sowie jeweils mehrere Ansichten.

Eine Datenbank

Alle von Ihnen erstellten Felder sind für alle Benutzer in einer Datenbank vorhanden. Berücksichtigen Sie die globalen Auswirkungen, bevor Sie eine erstellen.

Hinweis:
ACL-Skripts können nicht verhindern, dass ein Feld in einer Liste angezeigt wird, da sie nicht ausgeführt werden. Sie können eine Lese-ACL hinzufügen, um ein Feld für Benutzer auszublenden, wenn die ACL nur rollenbasiert ist.

Erstellen von Tabellen

Wenn Sie eine Tabelle erstellen, sollten Sie ein `sys_domain-` oder ein `sys_overrides` -Feld hinzufügen. Jede Tabelle, die Daten enthält, auf die Ihre Instanzbenutzer zugreifen müssen, benötigt das Feld `sys_domain`. Tabellen, die Prozesse erweitern oder unterstützen und in untergeordnete Domänen weitergegeben werden müssen, benötigen auch das Feld `sys_domain`.

Domänentrennung mit der Domänenauswahl konfigurieren

Verwenden Sie die Domänenauswahl mit Bedacht, und denken Sie an den 80/15/5-Ansatz, damit Sie nicht zu viel anpassen und die Leistung Ihrer Instanz beeinträchtigen.

Überprüfen Sie Ihre Domäne, bevor Sie Änderungen vornehmen

Die Domänenauswahl erfasst alle Domänen in einer Liste, aus der Sie auswählen können.

Wenn in Ihrer Sitzung eine Zeitüberschreitung auftritt, greift Ihre Sitzung auf die Domäne in Ihrem Benutzerdatensatz zurück, auch wenn Sie sich nicht abgemeldet haben. Gleichzeitig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verlieren Sie auch alle erhöhten Rollen. In diesem Fall zeigt Ihre Domänenauswahl möglicherweise immer noch die letzte von Ihnen ausgewählte Domäne an, wenn der obere Frame der Liste nicht neu geladen wurde. Aus diesem Grund sollten Sie Ihre Liste vollständig neu laden, wenn Sie die Instanz längere Zeit verlassen haben.

Konfiguration in der TOP-Domäne oder der globalen Domäne

Die Domänentrennung funktioniert am besten, wenn Sie Services für Kunden bereitstellen, die in ihrer Konfiguration sowie Benutzer- und Gruppendefinition größtenteils Standard sind. Je mehr Sie „einmalige“ Lösungen anpassen und erstellen, desto größer ist die Fehlertoleranz. Wenn Sie Ihre Prozesse und Geschäftslogik erstellen, sollten sich alle Variationen in Eigenschaften befinden, die für jeden Kunden automatisch funktionieren. Prozesse können zwar noch nach Bedarf angepasst werden, aber entscheiden Sie mit großer Sorgfalt, wann und in welchem Umfang Sie eine eindeutige Konfiguration für einen einzelnen Kunden erstellen möchten.

Sie müssen bei der Konfiguration Ihrer Domänen einen „80-15-5“-Ansatz verwenden, um einen zu großen Spielraum für die Anpassung und damit Fehler zu vermeiden.

- Empfohlener Ansatz für die Konfiguration:
  - **80 %** oder mehr **Standard**
  - **15 %** oder mehr **parametrisch**
  - Weniger als **5 % Konfiguration**
- Legen Sie fest, ob eine vorgeschlagene Änderung eine globale oder eine konfigurierbare Eigenschaft sein soll.
- Überdimensionieren Sie nicht, indem Sie immer mehr Anpassungen hinzufügen, die verwaltet werden müssen. Gehen Sie stattdessen wie folgt vor:
  - Beginnen Sie mit den Basissystemfunktionen, und überprüfen Sie alle Lücken, bevor Sie Änderungen vornehmen.
  - Suchen Sie nach Lösungen ohne Code.
  - Verwenden Sie serverseitige Skripts, erstellen Sie modulare APIs, und erstellen Sie domänengetrennte Eigenschaften.
  - Wenn Sie Client-Skripting verwenden müssen, verwenden Sie nur ServiceNow -APIs. Begrenzen Sie „synchrone“ Aufrufe (diejenigen, die von Client zu Server hin und her gehen, auch als AJAX bezeichnet).
  - Schreiben Sie alle Skripts logisch, um sie einfach und effektiv zu halten. Erzwingen Sie Peer-Reviews von Codeänderungen, und stellen Sie sicher, dass alle dem Empfohlene Domain Separation-Verfahren für Service Provider in diesem Abschnitt folgen.

Überlegungen zur Leistung der Domänentrennung

Berücksichtigen Sie beim Konfigurieren der Domänentrennung in Ihrer Anwendung und Ihren Services die Anzahl und die Eigenschaften der von Ihnen erstellten Domänen. Zu viele Eigenschaften-lastige Domänen können Auswirkungen auf die Leistung Ihrer Instanz haben.

Eigenschaftsreiche Domänen begrenzen

Sie können beliebig viele Domänen erstellen, stellen Sie jedoch sicher, dass Sie keine unnötigen Domänen auf der Instanz erstellen. Wenn Sie zu viele Domänen in der Instanz mit vielen Eigenschaften gewichten, kann dies Auswirkungen auf die Leistung Ihrer Instanz haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anzahl der Domänen wirkt sich nicht auf die Leistung aus, sondern auf deren Inhalt. Zu viele Eigenschaften können die Domänenauswahlverlangsamen, was dann die allgemeine Benutzer-Experience Ihrer Kunden verlangsamt. Wenn Sie die Domänenauswahl laden und bereits eine große Anzahl von Domänen mit vielen Eigenschaften haben, muss die Domänenauswahl alle Domänen laden, bevor Sie die Steuerung in der Sitzung übernehmen. Dieser Prozess kann zu einem Ausfall führen, bei dem Sie bis zum Abschluss der Domänenauswahl auf nichts in der Instanz zugreifen können. Bevor Sie neue Domänen erstellen, navigieren Sie zur Domänenhierarchie unter **Domänenadministrator** > **Domänenzuordnung** und stellen Sie sicher, dass Sie tatsächlich eine neue Domäne erstellen müssen oder ob eine vorhandene Domänenhierarchie funktionieren kann.

Verwenden der Core-UI Domänenauswahl

Die Domänenreferenzauswahl ist in Core-UIverfügbar. Mit der Referenzauswahl laden Sie nicht alle Domänen auf einmal, sondern die Domäne wird durchsucht, wenn Sie mit der Eingabe des Namens Ihrer Domäne in die Domänenauswahl beginnen.

Aktivieren Sie die Domänenreferenzauswahl in Core-UI, indem Sie die folgenden Schritte ausführen:

1. Geben Sie im Anwendungsnavigator `sys_properties.list` ein.
2. Legen Sie die Eigenschaft *`glide.ui.domain_reference_picker.enabled`* auf „Wahr“ fest.
3. Aktualisieren Sie den Browser.

Hinweis:
Laden Sie keine große Anzahl von Domänen (über 30) über Integrations- oder Import Sets hoch, ohne vorher einige Tests durchzuführen, da sonst Ihre Instanz heruntergefahren werden könnte.

Einrichten von Domänenhierarchien

Sie können Verlangsamungen und Auswirkungen auf die Leistung in Ihrer Instanz vermeiden, indem Sie wissen, wie Domänenhierarchien funktionieren, und sie richtig einrichten.

Basierend auf der Domänenhierarchie haben Benutzer Zugriff auf die Daten in ihrer Stammdomäne und allen untergeordneten Domänen. Der Prozess-Flow wird in die untergeordneten Domänen übertragen, und die Daten werden nach oben gerichtet.

Nehmen Sie nur bei Bedarf Änderungen an der vorhandenen Domänenhierarchie vor. Wenn Sie das übergeordnete Element einer Domäne aktualisieren, stellt das System die übergeordnete Domäne mit allen untergeordneten Domänen wieder her, die die Domänenhierarchie ändern. Wenn die Domänenhierarchie aktualisiert wird, löst das System eine kaskadierende Aktualisierung für alle Tabellen aus, die sich auf Domänen für die in dieser Domäne erstellten Datensätze beziehen. Daher muss auch eine große Anzahl von unterstützenden Tabellen aktualisiert werden.

Führen Sie aus den gleichen Gründen niemals eine Massenaktualisierung durch, auch wenn Sie die Domänenhierarchie ändern müssen. Stellen Sie sich die Anzahl der Abfragen vor, die das System ausführen muss, um die Domänenhierarchie zu ändern. Führen Sie Aktualisierungen immer in kleinen Batches durch. Bevor Sie den nächsten Aktualisierungsbatch starten, stellen Sie sicher, dass DWR-Datensätze (Domain Work Request) verarbeitet werden. DWRs sind Berichte, die anzeigen, ob Fehler vorhanden sind, nachdem Sie die Domänenhierarchie geändert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachverfolgung von DWR-Datensätzen

Suchen Sie in der Tabelle „syslog_domain“ in der Spalte „Nachricht“ nach einem Informationseintrag für **DWR-Ausführung abgeschlossen.**, um zu bestätigen, dass DWR abgeschlossen ist.

Domänenprotokolle werden auf Fehler und Warnungen überprüft

Überprüfen Sie die Domänenprotokolle auf Fehler oder Warnungen in Ihren Domänenpfadprozessen und Hierarchiekonfigurationen.

Sie finden die Domänenprotokolle in der Tabelle „Domänenprotokoll“ [syslog_domain]. Wenn die Domänenhierarchie aktualisiert wird, löst das System eine geplante Aufgabe aus, um die Domänenpfade neu zu berechnen. In der Tabelle „Domänenprotokolle“ werden die Ergebnisse erfasst.

Suchen Sie in dieser Tabelle nach Fehlern und Warnungen. Nach der Überprüfung dieser Tabelle müssen Sie diese Fehler beheben und die Domänenpfadvalidierung erneut ausführen.

In diesem Beispiel eines Protokolls hat das System zehn verwaiste Datensätze in der Tabelle „sys_ui_list“ erkannt. Die Fehler in diesen Datensätzen müssen behoben werden, bevor der Domänenpfad erfolgreich ausgeführt werden kann.

Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again.	com.glide.domain.validator
Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again. Entries causing the error are as follows:sys_id:1d13ae40470002007f47563dbb9a7170, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:22e34b23470002007f47563dbb9a718c, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:4c85fa809f233100fc6cd4b4232e706b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:94648b23470002007f47563dbb9a711b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a0844b23470002007f47563dbb9a71ef, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a95ff2c09f233100fc6cd4b4232e7096, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:bd25f4719f233100fc6cd4b4232e70da, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:c1263e809f233100fc6cd4b4232e70f6, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:d8a72c45475002007f47563dbb9a71bb, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:e4c3ce39eb10020045e1a5115206fea0, sys_domain:60e014f69f013100fbf01f80a57fcf00	com.glide.domain.validator

Weitere Informationen zu Domänentrennungsfehlern finden Sie unter Beheben Sie Fehler bei der Domänentrennung.

Wichtigkeit der Standarddomäne

Die Organisation Ihrer Domänen ist ein wichtiger Teil des Domänentrennungsprozesses. Wenn Sie keine Standarddomäne festlegen, werden neue Aufgaben und Benutzerdatensätze in die globale Domäne verschoben. Jeder kann die Datensätze in der globalen Domäne sehen, was bedeutet, dass Daten eingesehen werden können, wenn dies nicht vorgesehen ist.

Wenn Sie die Standarddomäne festlegen, sind deren Datensätze nur für Administratoren sichtbar.

Hinweis:
Der Standardzugriff kann geändert werden, indem Benutzern Einblick in die Standarddomäne oder die übergeordnete Domäne gewährt wird.

Sie sollten immer eine Standarddomäne für die Domänendatensätze in Ihrer Instanz festlegen. Die Standarddomäne ist die, in der das System automatisch Aufgaben- und Benutzerdatensätze zuweist, die noch keiner Domäne zugewiesen sind.

Wenn Sie eine Standarddomäne über den Bildschirm „Domänenverwaltung“ erstellen, fügen Sie im Feld **Name** den Namen Standard hinzu, um sie von anderen Domänen zu unterscheiden. Aktivieren Sie das Kontrollkästchen **Standard** für den Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie die Datensätze, die Sie in der Standarddomäne erstellen, regelmäßig, und verschieben Sie sie in die richtigen Domänen. Wenn Datensätze häufig in der Standarddomäne angezeigt werden, müssen Sie möglicherweise untersuchen, warum. Idealerweise sollten Sie sicherstellen, dass alle Datensätze in den entsprechenden Domänen erstellt werden (nicht in globalen oder Standarddomänen).

Enthält Abfragen und Domänenzugriff

Verwenden Sie eine Abfrage vom Typ „Enthält“ nur in besonderen Fällen, z. B. wenn Benutzer oder Gruppen Daten aus einer Domäne anzeigen müssen, auf die sie keinen Zugriff haben, Sie diese Benutzer jedoch nicht in eine Domäne verschieben möchten. Das Erstellen einer Domäne „enthält“ und Benutzer- oder Gruppenzugriff für eine Domäne sollte eine Ausnahme sein und nur dann erfolgen, wenn dies unbedingt erforderlich ist.

„Enthält“ ist eine m:n-Beziehung von Domäne zu Domäne, die keine Auswirkungen auf den Prozessfluss hat. Wenn Sie eine große Anzahl von Domänenbeziehungen erstellen, die „enthält“, oder einen weiten Zugriff bereitstellen, generieren Sie Abfragen mit zu vielen ODER-Bedingungen. OR-Bedingungen sind langsam und wirken sich auf die Leistung Ihrer Instanz aus. Anstatt zu viele „enthält“-Beziehungen zu verwenden, richten Sie Ihre Domänenhierarchie wie folgt ein:

Beispielabfrage

```
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name`
= 'incident' AND (task0.`sys_domain_path` = '/' OR task0.`sys_domain_path` LI
KE '!!$/!!(/%' OR task0.`sys_domain_path` LIKE '!!$/!!$/!!&/%') ORDER BY task
0.`number` DESC limit 0,20
```

Bevor Sie Benutzer in eine Domäne verschieben, stellen Sie sicher, dass sie wirklich Zugriff auf diese Domäne haben sollen. Wägen Sie die Vorteile und Einschränkungen ab. Die obige Abfrage bezieht sich nur auf eine Beziehung vom Typ „Enthält“. Wenn Sie eine Domäne haben, die eine andere Domäne enthält, und diese Domäne einer Reihe anderer Domänen übergeordnet ist, haben Sie viel mehr OR-Bedingungen. Seien Sie vorsichtig, wenn Sie eine Domänenzuordnung erstellen, damit die Leistung Ihrer Instanz nicht beeinträchtigt wird.

Abfragemethode für Domänenpfade

Sie können effektive Abfragen mit Domänenpfaden erstellen.

Verwenden Sie Domänenpfade anstelle von Domänen-Spooling (`sys_domain`) oder Domänennummerierung. Abfragen, die Domänenpfade verwenden, sind viel schneller als Spooling oder Nummerierung.

Domänenpfade sind die Standardabfragemethode für Instanzen, für die die Domänentrennung aktiviert ist.

Wenn Sie die Abfragemethode in Ihrer Instanz überprüfen möchten, suchen Sie im Administrator-Dashboard nach den folgenden Systemeigenschaften:

- *`If domain path is enabled`*: In der Tabelle „Systemeigenschaften“ wird `glide.sys.domain.provider=domain_paths` und `glide.sys.domain.paths.installed=true` angezeigt.
- *`If domain path is not enabled`*: In der Tabelle „ `Systemeigenschaften“ wird` `glide.sys.domain.provider != domain_paths,glide.sys.domain.paths.installed=false` angezeigt

Langsame Abfragen und SQL-Debugging

Das Debuggen von SQL und langsamen Abfragen kann Ihnen helfen, Langsamkeitsprobleme in einer Instanz zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine Instanz debuggen, können Sie entweder das SQL-Debugging aktivieren, um nach langsamen Abfragen zu suchen, oder Sie können nach langsamen Abfragen suchen, indem Sie die Tabelle „Langsame Abfragen“ [sys_query_pattern] überprüfen, indem Sie zu **Systemdiagnose > Statistiken > Langsame Abfragen**navigieren. In dieser Tabelle werden alle langsamen Abfragen in der Instanz gespeichert.

Suchen Sie beim Durchsuchen der Tabelle nach Abfragen, die „domain_path“ enthalten, um festzustellen, ob langsame Abfragen auf den Domänenpfad in Ihrer Instanz zurückzuführen sind.

Wenn Sie langsame Abfragen finden, versuchen Sie zu analysieren, warum sie langsam sind.

Häufige Gründe für langsame Abfragen

- Eine Abfrage weist zu viele OR-Bedingungen auf (weitere Informationen finden Sie unter Enthält Abfragen und Domänenzugriff). Platzieren Sie in der Domänenhierarchie den Benutzer oder eine Domäne auf einer Hierarchieebene, auf der keine Sichtbarkeit von enthält oder erforderlich ist.
- Die Abfragemethode ist nicht die Abfragemethode des Domänenpfads (weitere Informationen finden Sie unter Abfragemethode für Domänenpfade): Wenn Sie nicht die Abfragemethode des Domänenpfads verwenden, wenden Sie sich an Kundenservice und Support.
- Für eine Abfrage muss eine Datenbank indiziert werden, damit Sie schnell sehen können, was sich in der Datenbank befindet. Wenn Sie die langsame Abfrage identifizieren können, führen Sie „plan erklären“ aus, um zu sehen, ob Optionen für die Indizierung verfügbar sind. Der „Erklärungsplan“ ist eine Funktion von SQL, die die Abfrage und ihre Vorgänge anzeigt.

Business Rules „Vor Abfrage“.

Sie können eine Geschäftsregel vom Typ „Vor Abfrage“ verwenden, um die Datentrennung für eine Instanz zu unterstützen. ServiceNow Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und Datenweiterleitung, verfügen über eine erweiterte Geschäftslogiktrennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kundenebene).

Eine Geschäftsregel vom Typ „Vor Abfrage“ ist ein zusätzlicher Code, den Sie zur Unterstützung der Datentrennung in domänengetrennten Umgebungen verwenden.

Warnung:
Verwenden Sie nicht die Geschäftsregel „Vor Abfrage“ anstelle des Plugins „Domain Separation“. Diese Geschäftsregel verhindert Datenverlust nicht so sicher wie das Plugin.

Verwenden der Geschäftsregel „Vor Abfrage“ für Datentrennung

Sie können die Geschäftsregel „Vor Abfrage“ mit Datentrennung in den folgenden Situationen verwenden:

- Wenn die Domänentrennung von einer ServiceNow -Anwendung nicht unterstützt wird und Sie Tabellen- oder Zeilenzugriff für einen oder mehrere nicht interne Kunden außerhalb der Service Provider-Organisation gewähren oder einschränken müssen.

Hinweis:
Bevor Sie mit der Entwicklung beginnen, wenden Sie sich an den Kundensupport von ServiceNow, um Informationen zur Anwendungs-Roadmap für dieses Produkt zu erhalten. Verbesserungen des Domänensupports sind möglicherweise für bevorstehende Releases geplant.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn eine Tabelle domänengetrennt ist, der Zugriff auf ihre Zeilen jedoch basierend auf bestimmten Bedingungen, die nur für eine Reihe von Domänen im System gelten, gewährt oder eingeschränkt werden muss.

Hinweis:
Zum Beispiel hat ein Kunde in der X-Domäne mehrere Lieferanten, die diese Domäne unterstützen, und diesen Lieferanten wird Zugriff gewährt, um nur die Datensätze anzuzeigen, die ihnen zugewiesen sind.

Punkte, die vor dem Erstellen von Business Rules vom Typ „Vor Abfrage“ zu beachten sind

Sie können Business Rules vom Typ „Vor Abfrage“ skripten, um den Zugriff auf übergeordnete und untergeordnete Tabellen basierend auf einer Kombination aus Benutzerinformationen, Gruppenmitgliedschaften, Unternehmen, Rollen oder datensatzspezifischen Feldbedingungen zu verhindern. Business Rules vom Typ „Vor Abfrage“ werden in separate Domänen eingeteilt und erstellt, um global auf eine bestimmte Verzweigung einer Domänenhierarchie angewendet zu werden.

- Erstellen Sie nach Möglichkeit Vorabfrage-Business Rules am niedrigstmöglichen Teil der Domänenhierarchie, damit die Regel nur für Benutzer ausgeführt wird, für die sie gilt.
- Beachten Sie, dass es Szenarien im System gibt, in denen Business Rules möglicherweise nicht ausgeführt werden oder in denen eine vom Benutzer ausgelöste Interaktion die Ausführung einer Business Rule nicht auslöst. Zum Beispiel wird eine Business Rule nicht ausgeführt, wenn Sie Transformationszuordnungen mit Business Rules ausführen deaktiviert haben oder Skripts mit deaktiviertem Workflow haben.
- Füllen Sie immer das Bedingungsfeld aus, um anzugeben, wann die Regel ausgeführt wird. Sie können beispielsweise angeben, ob die Geschäftsregel nur für bestimmte Lieferanten in einer Domäne gilt.

Warnung:
Begrenzen Sie beim Entwerfen und Codieren von Geschäftsregeln (insbesondere Abfragen von Geschäftsregeln) OR-Klauseln und Suchen in nicht indizierten Feldern. Zu viele OR-Klauseln und Suchvorgänge in nicht indizierten Feldern können Abfragen verlangsamen oder die Leistung Ihrer Instanz beeinträchtigen.

- Verwenden Sie Business Rules vom Typ „Vor Abfrage“ nur bei Bedarf. Zu viele Vor-Abfrage-Regeln können sich auf die Leistung Ihrer Instanz auswirken.

Business Rules vom Typ „Vor Abfrage“ werden vor Zugriffssteuerungslisten (ACLs) ausgeführt und weisen im Allgemeinen eine bessere Leistung auf. Dies gilt insbesondere, wenn Sie die zurückgegebenen Ergebnisse auf die Benutzer in Service Provider-Umgebungen (SP) beschränken, die Zugriff auf mehrere Domänen im System haben.

Hinweis:
Das Filtern der Daten ist transparent (im Gegensatz zu ACLs) für Benutzer, die die Meldung „Datensicherheit beschränkt…“ nicht sehen. bei der Interaktion mit Daten.

Wann keine Business Rules und ACLs vom Typ „Vor Abfrage“ zu verwenden sind

Seien Sie vorsichtig, wenn Sie Geschäftsregeln vom Typ „Vor Abfrage“ und ACLs verwenden, um Kundendaten zu trennen. Wenn Sie sowohl Business Rules als auch ACLs verwenden, erstellen Sie Anpassungen, die Sie dann pflegen müssen. Anpassungen können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

potenziell Leistungsprobleme verursachen. Ihre Entwicklungsteams sollten Prozesse erstellen, um sicherzustellen, dass das System nicht beschädigt wird.

Die Domänentrennung bietet Skalierbarkeit und Governance mit der aktuellen Domänenpfad-Abfragemethode (v3), einem weithin unterstützten Framework. Die Plattform- und App-Teams von ServiceNow sind für die Wartung des Frameworks verantwortlich und entlasten den Kunden.

Für Unternehmen mit vielen Kunden in vielen Instanzen kann die übermäßige Verwendung von Vor-Abfragen und ACLs dazu führen, dass die Datenbankabfragen nicht ordnungsgemäß funktionieren.

Wie die Domänentrennung aktiviert wird

Sie können die Domänentrennung mit einem ServiceNow -Plugin aktivieren. Ein Produktmanager, der von einem Entwicklungsteam unterstützt wird, verwaltet die Funktionalität. Verbesserungen und Korrekturen für die Funktion zur Domänentrennung sind in den Releases ServiceNow enthalten. Instanzbesitzer können Kundenservice und Support -Ressourcen konsultieren, z. B. Serviceportal, unter https://support.servicenow.com , um Unterstützung bei der Domänentrennung zu erhalten.

Domänenpfade in Skripts werden vermieden

Domänenpfade können dazu führen, dass sich die Werte Ihres Skripts ändern oder sogar brechen. Verwenden Sie sie daher nicht in Skripts.

Ihr Skript sollte nicht vom Domänenpfad abhängig sein, da der Domänenpfad neu berechnet wird und sich sein Wert ändert, wenn Sie die Domänenhierarchie ändern. In diesem Fall sind Ihre Skripts nutzlos oder können Fehler auslösen oder abbrechen. Die beste Strategie besteht darin, Ihre Skripts nicht basierend auf Domänenpfaden zu schreiben.

Verwenden Sie das Feld **sys_domain** in Ihren Skripts, anstatt vom Domänenpfad abhängig zu sein. Wenn Sie die Domänenhierarchie ändern, wird der Domänenpfad neu berechnet, und sein Wert ändert sich, was dazu führen kann, dass Ihre Skripts unbrauchbar sind, Fehler auslösen oder abbrechen. Suchen Sie nach Basissystem-Business Rules, die das **sys_domain** -Feld verwenden, um einige Ideen zu erhalten, bevor Sie Ihre eigenen Skripts erstellen.

Die ServiceNow -Plattform erfasst die sys_domain_path-Werte in einem Update Set nicht, um Probleme mit Unterschieden in der Domänenhierarchie für jede Instanz zu vermeiden. Daher sollten Sie die Domänenhierarchie nach dem Import eines Update Sets validieren, um sicherzustellen, dass die Domänenpfadwerte für Ihre Datensätze korrekt sind.

Weitere Informationen zum Domänenpfad finden Sie unter Domänentrennung anfordern und Domain Separation Center.

Domänenzuweisungen

Wie Sie eine Domäne zuweisen, wirkt sich auf den Wert des Felds sys_domain aus. Die Zuweisungen enthalten Designs und Geschäftseigenschaften, die sich auf die Funktionsweise der Anwendung in jeder Domäne auswirken.

Wert des Felds sys_domain

Der Wert des **Felds sys_domain** enthält die Domäne, die dem Datensatz von einem der folgenden Elemente zugewiesen wurde:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unternehmen, zu dem der Benutzer gehört
- Geschäftsregel, die beim Erstellen des Datensatzes verwendet wird
- Modul, das beim Erstellen des Datensatzes verwendet wird
- Formularvorlage, die beim Erstellen des Datensatzes verwendet wird
- Domäne des übergeordneten Datensatzes
- Domäne, die dem Benutzerdatensatz zugewiesen ist
- Domäne des Benutzers, der sie erstellt

Stellen Sie sicher, dass Ihre Domänenzuweisungsstrategien und -designs gut dokumentiert und getestet sind, damit Sie Datensätze erstellen, wenn diese Strategien und Designs in die richtige Domäne eingefügt werden. Auf diese Weise können Sie sehen, dass die Eigenschaften jeder Domäne dupliziert oder geändert werden müssen.

Domänentrennung und das Plugin Kundenservice-Management (Customer Service Management, CSM) .

Um das beste Ergebnis zu erzielen, sollten Sie wissen, wie die Eigenschaften im CSM -Plugin funktionieren. Wenn das Plugin aktiviert ist, können Sie den Status Ihrer Datensätze in Ihren Domänen anzeigen.

Instanzbesitzer sollten sich an [] wenden, um die Eigenschaft `csm_auto_account_domain_generation`Kundenservice und Support zu aktivieren.

Hinweis:
Diese Basissystemeigenschaft befindet sich in der Tabelle „Systemeigenschaften“ und ist verfügbar, nachdem CSM-Plugins aktiviert wurden.

Was die Eigenschaft tut

Immer wenn ein neuer Account in der Anwendung Customer Service erstellt wird, wird eine Domäne erstellt und unter der TOP-Domäne platziert. Wenn das übergeordnete Feld im Account-Formular ausgefüllt wird und ein neuer Datensatz eingefügt wird, wird dieser Account als Subdomäne des übergeordneten Elements erstellt.

Was geschieht, wenn diese Eigenschaft nicht „wahr“ ist und die Domäne aktiviert ist?

Neue Account-Datensätze in einer domänengetrennten Umgebung werden automatisch in der Standarddomäne platziert.

In der Kopfzeile sehen Sie den Status der Datensätze mit aktiviertem Plugin.

Hilfe zur Domänentrennung

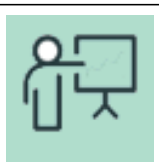
Zusätzliche Unterstützung bei der Domänentrennung

Videoübersicht über die Domänentrennung

Erkunden, lernen, entwickeln

Empfohlene Vorgehensweisen

Tipps und Tricks zum sinnvollen Erstellen



Supportstufen nach Anwendung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und Entwickeln Ihrer Domänenstruktur

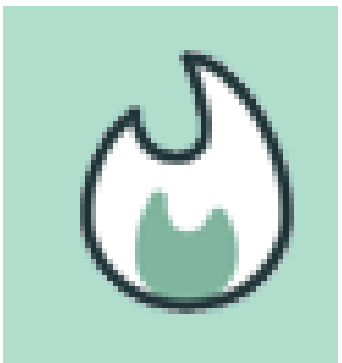
Konzepte für Service Provider

Konzepte, die mit der Plattform ServiceNow funktionieren, um Sie bei der Lösung gängiger Anwendungsfälle zu unterstützen

Wird Ihre Anwendung für Domänentrennung unterstützt? Siehe Supportstufen und Anwendungsfälle.

Klassen

- Für Entwickler: ServiceNow Domänentrennung für Entwickler-Site
- Für Service Provider: Domänentrennung für Service Provider (Anmeldung für ServiceNow University erforderlich)



Safe Workplace-Suite und Domänentrennung

ServiceNow Safe Workplace-Anwendungen helfen Ihnen, Ihre Arbeitsplätze wieder zu öffnen und die Gesundheit und Sicherheit Ihrer Mitarbeiter nach Notfällen und Pandemien wie COVID-19 zu unterstützen. Die Suite verfügt über viele Anwendungen, die Ihr Unternehmen bei der Mobilisierung, Wiederherstellung und dem Neuaufbau unterstützen.

Setup und Verwaltung

- Upgrades
- Domänentrennung anfordern
- Erstellen Sie eine Domäne
- Konfiguration, die an interne oder externe Kunden delegiert werden kann

Problembehandlung

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- In der Community Fragen stellen oder beantworten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einrichtung und Verwaltung der Domänentrennung

Das Einrichten der Domänentrennung umfasst das Anfordern der Aktivierung eines Plugins, das Festlegen von Optionen und das Zuweisen von Benutzern und Datensätzen zu Domänen.

Gehen Sie wie folgt vor, um die Domänentrennung einzurichten:

1. Domänentrennung anfordern
2. Erstellen Sie eine Domäne
3. Fügen Sie einer Tabelle ein Domänenfeld hinzu

Sie können diese grundlegenden administrativen Aufgaben auch für Domänen ausführen:

- Aktivieren oder deaktivieren Sie eine Domäne
- Zeigen Sie Domänenbeziehungen an
- Domänenbereich erweitern
- Erstellen Sie eine domänenspezifische Auswahlliste

Unter Erweiterte Verwaltung der Domänentrennung finden Sie eine Liste der Aufgaben, die nach der Einrichtung der Domänentrennung und der grundlegenden Administration ausgeführt werden müssen.

Konfiguration, die an interne oder externe Kunden delegiert werden kann

DieDomänentrennung soll ServiceNow® Service Providern (SPs) die Möglichkeit geben, die Services zu konfigurieren, die sie ihren Kunden anbieten. Es ist nicht so konzipiert, dass Kunden von diese Services selbst verwalten können, mit Ausnahme einiger Bereiche, auf die in diesem Thema näher eingegangen wird.

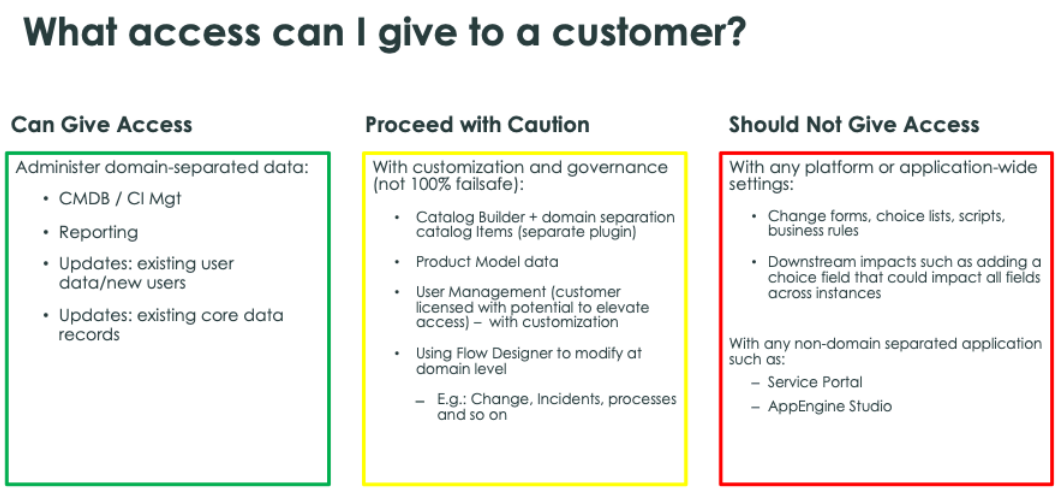
Übersicht

Für SP-Kunden ist es sicher, Daten in ihrer Domäne selbst zu verwalten, die sich nicht auf die Lizenzierung oder andere Kunden auswirken. Beispielsweise ist es für einen Kunden sicher, neue Berichte zu erstellen oder Konfigurationselemente zu verwalten, aber es ist nicht sicher, Felder, Auswahlmöglichkeiten, Geschäftsregeln und andere Prozesse anzupassen, bei denen dies Auswirkungen auf andere Kunden in derselben Instanz haben kann.

Die administrativen Rollen des [ServiceNow -Basissystems und ihre Zugriffskontrollen auf der ServiceNow -Plattform sind für ein einzelnes Administratorteam pro Instanz konzipiert. Beispielsweise wird die Rolle „domain_admin“ einer der SP-Ressourcen zugewiesen, um alle Domäneneinstellungen für die Instanz zu verwalten und neue Domänen zu erstellen. Für alle domänenspezifischen Administratoraufgaben sollte der SP nach Bedarf neue „Kundenadministrator“-Rollen und Zugriffskontrollen erstellen, um seinen Kunden bestimmten Zugriff zu gewähren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt eine Übersicht über allgemeine Administratorfunktionen in verschiedenen Kategorien, die für einen Kunden sicher sind.



Kann Zugriff gewähren

Beispiele:

- CI-Datenverwaltung in der CMDB
- Berichterstellung
- Aktualisiert vorhandene Benutzerdaten oder neue Benutzer ohne Rollen
- Aktualisierung vorhandener Kerndatensätze wie Abteilung, Gruppe, Standort, Kostenstelle oder neue Gruppen ohne Rollen und neue Abteilungen/Kostenstellen/ Standorte.

Fahren Sie mit Vorsicht fort

Beispiele:

- Katalogelemente: Um kundenspezifische Katalogelemente zu erstellen, die vom Kunden aktualisiert werden können, können zwei Fähigkeiten zusammen verwendet werden: Die Domänentrennung für Katalogelemente (Domänentrennung und Service Catalog) ermöglicht es dem Instanzbesitzer, Elemente in der Domäne des Kunden zu erstellen. Der Instanzbesitzer kann eine Rolle erstellen, damit Kunden sichere Felder wie Preis, Beschreibung und Bilder aktualisieren können. Der Katalog-Generator (neu im Quebec-Release) gibt dem SP-Administratorteam die Möglichkeit, Elementvorlagen zu erstellen, die sicher an Kunden verteilt werden können, um innerhalb einer verbindlichen UI-Experience neue Elemente in ihrer Domäne zu erstellen.
- Benutzer-/Gruppenverwaltung: Es ist sicher, eine „Kundenadministrator“-Rolle zu erstellen, die Benutzerdatensätze erstellen und ändern kann, aber das Hinzufügen und Entfernen von Rollen kann sich auf Sicherheit und Lizenzierung auswirken. Im Basissystem gibt es keine Möglichkeit, Rollen zu unterteilen, die für einen Kunden sicher sind. Dasselbe gilt für die Erstellung und Änderung von Gruppen. Während die Gruppe selbst geändert werden kann, sollte das Hinzufügen oder Entfernen von Rollen kontrolliert werden.
- Flow Designer : ServiceNow Flow Designer ist das Erstellungstool zum Erstellen von Prozessen (Workflows) für Tabellen. Die Rolle „flow_designer“ ermöglicht Kunden den skriptfreien Zugriff auf Build-Flows. Sie können jeden Flow in Domänen über ihnen in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hierarchie lesen und klonen. Sie können Flows in ihrer Domäne erstellen und ändern. Dies kann jedoch nicht in einem Silos geschehen. Jeder, der den Prozess beeinflussen kann, muss dem globalen Administratorteam für Governance hinzugefügt werden, damit sich Prozesse nicht gegenseitig aufheben oder andere Konflikte verursachen.

Keinen Zugriff gewähren

Zu verstehen, wie Auswahlfelder funktionieren, ist hilfreich, um zu verstehen, warum sie nur vom SP-Administratorteam verwaltet werden sollten.

- Struktur eines Auswahlfelds: Auswahlfeldwerte werden in der Tabelle „sys_choice“ gespeichert und basierend auf folgenden Kriterien gruppiert: Tabelle, Domäne und Sprache.

  Beispielsweise ist das **Feld** Status in einer Aufgabe für jede Tabelle verfügbar, die eine Aufgabe erweitert. Das bedeutet, dass jede Tabelle eigene Werte haben kann, diese Werte mit der Domäne multipliziert werden können und die Domänenwerte mit der Sprache multipliziert werden können.

  Alle Werte für **Status** in allen Tabellen, Domänen und Sprachen werden als Werte für das **Feld** Status betrachtet.

- Funktionsweise von Änderungen an Auswahlfeldern: Wenn ein Auswahlfeld aktualisiert wird, wird eine Nutzlast mit allen Werten für dieses Feld (Tabellen, Domänen, Sprachen) erstellt. Wenn Sie diese Nutzlast in einer Instanz installieren, werden alle vorhandenen Werte für das Feld gelöscht und die neuen Werte geladen. Dadurch wird sichergestellt, dass keine doppelten Einträge oder verbleibenden Werte vorhanden sind, die nicht mehr gültig sind.

  Aus diesem Grund ist es unmöglich, einem Kunden in einer domänengetrennten Instanz die Möglichkeit zu geben, Auswahlfelder direkt zu aktualisieren, da dies Auswirkungen auf die gesamte Instanz haben würde. Darüber hinaus können Sie Auswahlmöglichkeiten nicht direkt in einer Produktionsinstanz aktualisieren, da alle importierten Update Sets, die sich auf dieses Feld auswirken, die vorhandenen Auswahlmöglichkeiten überschreiben würden. In einigen Fällen können Auswahlfelder Prozesse selbst steuern, die unterbrochen würden, wenn ein Kunde diese Felder ändern würde.

Weitere Informationen finden Sie unter:

- Exploring user administration
- Eine ACL-Regel erstellen
- Service Provider-Lernpfad auf ServiceNow University
- Domänentrennung für Service Provider
- Service Provider-Konzepte
- Anwendungssupport für Domänentrennung
- Versionshinweise zur Domänentrennung

Domänentrennung anfordern

Alle Domänen-Support-Funktionen werden mit einem Plugin namens „ **Domain Support – Domain Extensions Installer**“ aktiviert. Administratoren können die Aktivierung dieses Plugins anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager kann die Aktivierung des Plugins `com.glide.domain.msp_extensions.installer` in den Produktions- und Test- und Entwicklungsumgebungsinstanzen Ihrer Organisation veranlassen, in der Regel innerhalb weniger Tage.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

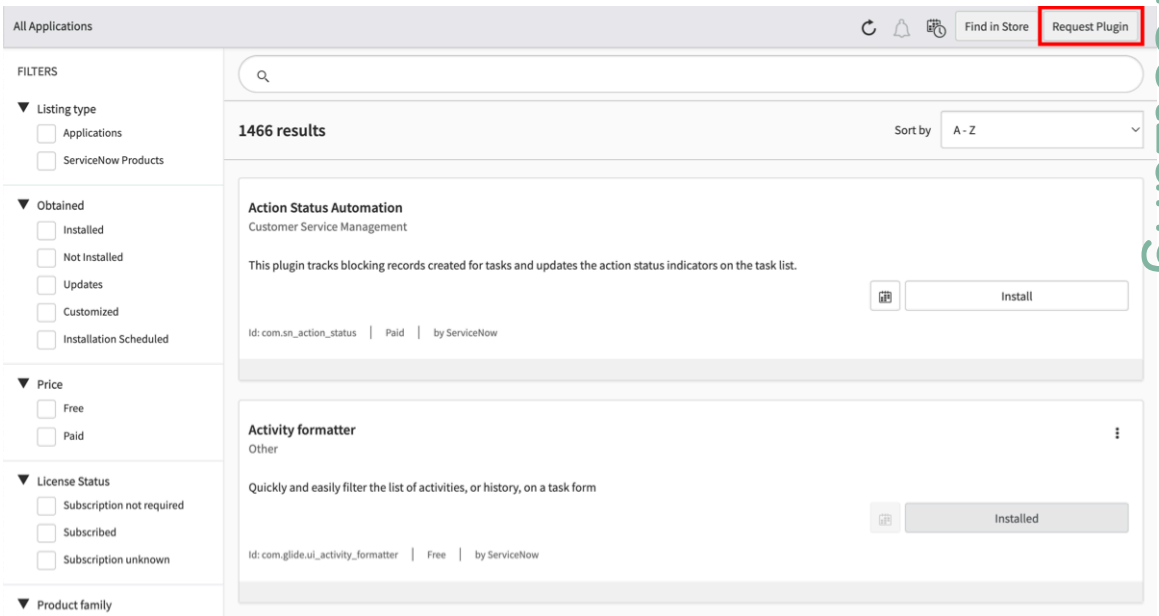
Wenn das Plugin „Domain Support – Domain Extensions Installer“ bereits aktiv ist, werden Inhalte im Plugin „Domain Support – Domain Extensions Installer“ nicht installiert, um einen potenziellen Konflikt mit einer vorhandenen Implementierung zu vermeiden.

Domänentrennung ersetzt Unternehmenstrennung. Ab dem Helsinki-Release kann das Plugin „Company Separation“ nicht mehr aktiviert werden. Wenn jedoch die Unternehmenstrennung bereits aktiv ist, wenn Sie die Domänentrennung aktivieren, sind beide Plugins gleichzeitig aktiv. Sie können den Aktivierungsstatus der Unternehmenstrennung mit der Eigenschaft `glide.db.separation.field` steuern.

Hinweis:
Domänenpfade werden für alle Kunden ab Helsinki verwendet. Die Domänennummerierung wird nicht mehr verwendet. Kundenservice und Support kann beim Upgrade helfen.

Prozedur

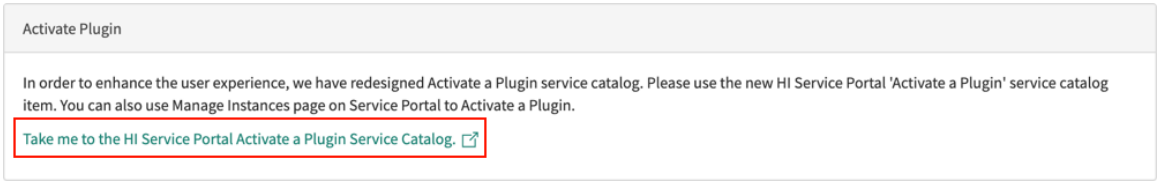
1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

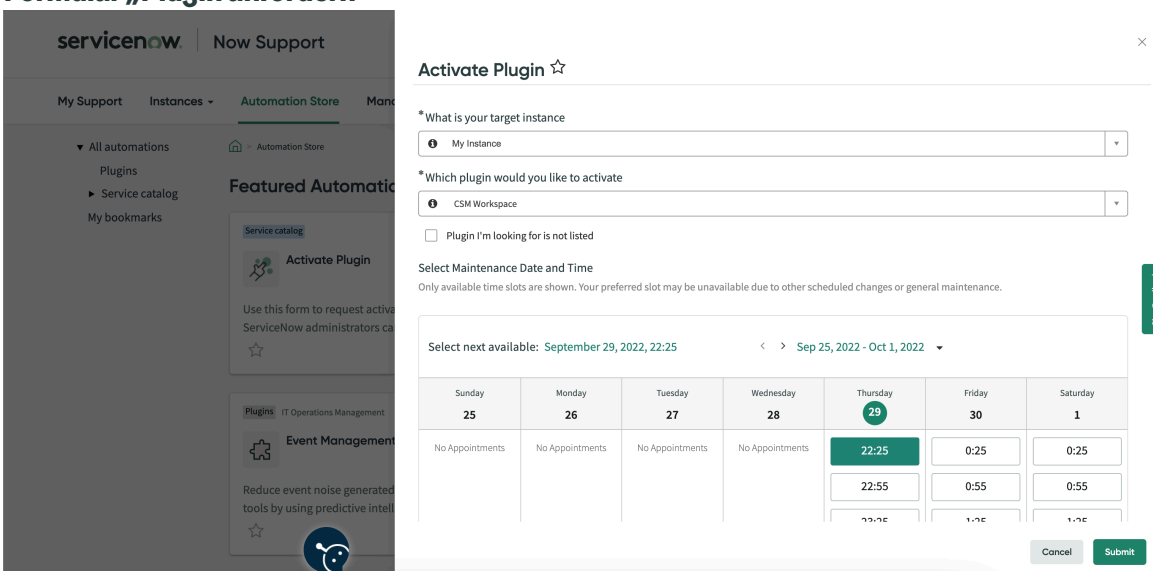
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Plugins aus dem Servicekatalog anfordern [KB0751715] im Now Support Knowledge Base.

Ergebnisse

Durch die Aktivierung des Plugins „Domain Extension Installer“ werden die folgenden Funktionen aktiviert:

- Die Domänentrennung basiert auf der Domänentabelle [sys_domain].
- Durch die delegierte Verwaltung kann jede Domäne über eine separate Richtlinie verfügen.
- Alle Datensätze sind Teil der globalen Domäne.
- Die Domäne des aktuellen Benutzers bestimmt die Domäne, die beim Anzeigen oder Bearbeiten eines Datensatzes in einer anderen Domäne verwendet werden soll.

Zugehörige Informationen

Plugin für Domänentrennung

Plugin für Domänentrennung

Das Plugin „Domain Support – Domain Extensions Installer“ aktiviert mehrere Funktionen und Eigenschaften der Domänentrennung gleichzeitig. Dieses Plugin wird normalerweise als das Plugin „Domain Separation“ bezeichnet.

Empfohlene Vorgehensweise für die Aktivierung des Plugins „Domain Separation“.

Im Rahmen der Entwicklung der Domänentrennung müssen Administratoren die Aktivierung dieses Plugins anfordern. Um die besten Ergebnisse zu erzielen, aktivieren Sie das Plugin „Domain Separation“ zu Beginn des Entwicklungsprozesses, vorzugsweise bevor ein anderes Plugin aktiviert wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Fordern Sie die Aktivierung des Plugins „Domain Extensions Installer“ (com.glide.domain.msp_extensions.installer) an, bevor Sie die Domänentrennung (Plugin com.snc.pa.domain_support) aktivieren.

Wenn Sie die Domänentrennung gegen Ende der Implementierung von ServiceNow aktivieren oder nachdem eine Instanz live gegangen ist, ist Ihre Anwendung sowohl hinsichtlich Leistung als auch Prozess gefährdet. Bei etablierten Instanzen kann das Risiko für die Plattform und ihre Verwendbarkeit hoch sein, je nachdem, wie die Dinge in der Entwicklung strukturiert wurden. Weitere Informationen zum Domänentrennungsprozess finden Sie unter Domänentrennung erkunden.

Wenn beispielsweise das Plugin „Domain Separation“ aktiviert ist, wird die Spalte **Domäne** (sys_domain) der Aufgabentabelle hinzugefügt, und jeder vorhandene Datensatz wird automatisch in **global**platziert. Um ein Skript zu verwenden, um alle Datensätze den richtigen Domänen zuzuweisen, ist eine eingerichtete über-/untergeordnete Hierarchie erforderlich. Diese Arten von Skriptaktionen riskieren Datenbeschädigung oder -verlust und mögliche Produktionsausfälle, wenn große Datenmengen verschoben werden. Ein Großteil des Plattformcodes wird auch in **globalen**platziert, z. B. Business Rules, Client-Skripts, Formularansichten und Workflows.

Wenn ein Kunde Code erstellt oder Code von ServiceNow ändert, besteht ein Risiko für Leistung und Benutzerfreundlichkeit der Plattform. Instanzbesitzer können bei dieser Art von Ansatz ihre Implementierung erheblich verzögern oder lange Ausfallzeiten erleben.

Funktionen des Plugins „Domain Separation“.

Diese Funktionen werden aktiviert, wenn Sie das Plugin aktivieren:

- Die Domänentrennung basiert auf der Domänentabelle [sys_domain].
- Durch die delegierte Verwaltung kann jede Domäne über eine separate Richtlinie verfügen.
- Alle Datensätze sind Teil der globalen Domäne.
- Die Domäne des aktuellen Benutzers bestimmt die Domäne, die beim Anzeigen oder Bearbeiten eines Datensatzes in einer anderen Domäne verwendet werden soll.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänensystemeigenschaften und Benutzereinstellungen

Administratoren haben Zugriff auf Eigenschaften und Benutzereinstellungen, die den Domänenbereich steuern.

Eigenschaften

Bei neuen Aktivierungen der Domänentrennung wird der Domänenbereich für alle zugehörigen Daten oder Prozesse automatisch auf die Domäne des Datensatzes beschränkt. Wenn der Benutzer einen Datensatz in einem Formular anzeigt, sind die zugehörigen Daten des Datensatzes (z. B. Referenzauswahl und zugehörige Listendaten) und angewandte Prozesse (z. B. Business Rules und Client-Skripts) auf den Domänenbereich des Datensatzes beschränkt. Wenn Datensätze auf mehreren Registerkarten vorhanden sind, hat jede Registerkarte einen eigenen Domänenbereich basierend auf dem Datensatz, der auf dieser Registerkarte geöffnet wurde. Die folgenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften beschränken den Domänenbereich auf die Domäne des Datensatzes und die aktuelle Sitzungsdomäne des Benutzers.

Domänensystemeigenschaften

Eigenschaft	Details
glide.sys.domain.use_record_domain_for_processes	Beschränkt den Domänenbereich für alle Prozesse auf die Domäne des Datensatzes. Diese Eigenschaft gilt nicht für Business Rules. Business Rules werden immer aus dem Domänendatensatz verarbeitet. • *Typ*: true | false • *Standardwert*: true • *Speicherort*: Tabelle „Systemeigenschaft“ [sys_properties]
glide.sys.domain.use_record_domain_for_data	Beschränkt den Domänenbereich für alle Daten auf die Domäne des Datensatzes. • *Typ*: true | false • *Standardwert*: „true“ bei neuen Domänenaktivierungen ab Fuji (Upgrades von Instanzen, die älter als Fuji sind, haben diese Eigenschaft nicht in der Tabelle). • *Speicherort*: Tabelle „Systemeigenschaft“ [sys_properties]

Wenn die Eigenschaft `glide.sys.domain.use_record_domain_for_processes` oder `glide.sys.domain.use_record_domain_for_data` auf **true**festgelegt ist, werden die folgenden Eigenschaften unabhängig von ihrer Einstellung nicht verwendet:

- `glide.sys.domain.use_record_domain`
- `glide.sys.domain.use_record_domain_for_client_scripts`
- `glide.sys.domain.domain_change_notify`
- `glide.sys.domain.no_change_roles`

Eine vollständige Liste der Eigenschaften finden Sie unter Verfügbare Systemeigenschaften .

Hinweis:

Bei neuen Aktivierungen der Domänentrennung ab dem Jakarta-Release bestimmt die Sitzungsdomäne die Geschäftsregeln, die für die Domänentabelle ausgeführt werden. In früheren Versionen wurden Business Rules, die für die Domänentabelle ausgeführt wurden, basierend auf der Hierarchie der neu erstellten Domäne festgelegt. Dieses Verhalten wird durch die Eigenschaft `glide.sys.domain.skip_domain_insert_businessrules` geändert. Wenn diese Eigenschaft auf „true“ festgelegt wird, wird die Leistung beim Einfügen von Domänen erheblich verbessert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenbereichseigenschaften für Business Rules, die in der Domänentabelle ausgeführt werden

Eigenschaft	Details
glide.sys.domain.skip_domain_insert_businessrules	Gibt den Domänenbereich für Business Rules an, die in der Domänentabelle ausgeführt werden. Bei neuen Aktivierungen der Domänentrennung lautet der Standardwert der Eigenschaft „true“, und die Geschäftsregeln werden von der Sitzungsdomäne bestimmt. In vorhandenen Implementierungen ist der Eigenschaftsstandard „false“, und die Business Rules werden durch die Hierarchie der neu erstellten Domäne bestimmt. • *Typ*: true | false • *Standardwert*: „Wahr“ in neuen Domänenaktivierungen, die mit Jakarta beginnen. False in vorhandenen Implementierungen.
glide.sys.domain.skip_non_global_businessrule_if_nodomain	Stellt sicher, dass nur „bus.rules“ aus der globalen Domäne ausgeführt wird, wenn „queryNoDomain()“ verwendet wird oder wenn die Tabelle nicht domänengetrennt ist, sodass Sie alle anderen Business Rules überspringen können • *Typ*: true | false • Wenn die Eigenschaft auf „false“ festgelegt wird, wird das alte Verhalten wiederhergestellt und entspricht nicht den empfohlenen Vorgehensweisen von ServiceNow®. • Empfohlen: Trennen Sie Ihre Tabellen nach Domänen. Versuchen Sie immer, die Domäne des Datensatzes anstelle der Sitzungsdomäne zu verwenden.

Benutzereinstellungen

Darüber hinaus können Benutzeradministratoren die folgenden Benutzereinstellungen global oder pro Benutzer festlegen:

Benutzereinstellungen für den Domänenbereich

Einstellungen	Kategorie	Aktualisiert von	Details
glide.domain.session_scope	Domäne	Nur Administrator	Bei „true“ wird der Standardbereich auf die Sitzungsdomäne des Benutzers und nicht auf die Domäne des

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzereinstellungen für den Domänenbereich (Fortsetzung)

Einstellungen	Kategorie	Aktualisiert von	Details
			Datensatzes festgelegt. Bei „false“ ist der Standardbereich die Domäne des Datensatzes. Benutzer mit der Benutzerrolle „domain_expand_scope“ können den Domänenbereich weiterhin nach Bedarf ändern. • **Typ**: true | false • **Standardwert**: false
glide.domain.session_scope_notification	Domäne	Nur Administrator	Bei „true“ wird ein visueller Hinweis angezeigt, dass Datensatzwerte einen erweiterten Domänenbereich enthalten. Bei „false“ wird die Benachrichtigung ausgeblendet. • **Typ**: true | false • **Standardwert**: true

Zugehörige Informationen

Eigenschaften der Anwendung zur Domänentrennung

Erstellen Sie eine Domäne

Sie können eine Domäne erstellen, indem Sie einen Datensatz in der Tabelle [Domäne] erstellen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Beachten Sie beim Erstellen einer neuen Domäne Folgendes:

- Nur eine Domäne kann die Standarddomäne sein.
- Nur eine Domäne kann die primäre Domäne sein.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die erforderlichen Felder aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.

Felder des Domänenformulars

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Domäne ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	Wählen Sie einen Domänentyp aus, der die Domäne beschreibt. Standardmäßig lauten die *Domänentypen Lieferant*, *Kunde*und *MSP*. Sie können auch Ihre eigenen Auswahlmöglichkeiten hinzufügen.
Primär	Aktivieren Sie das Kontrollkästchen, wenn diese Domäne die oberste Domäne in der Hierarchie sein soll. Die Domäne der obersten Ebene hat nur untergeordnete Domänen und keine übergeordneten Domänen.
Standard	Wählen Sie diese Option aus, wenn diese Domäne die Standarddomäne für Ihre Hierarchie sein soll.
Übergeordnet	Wählen Sie den Namen der Domäne weiter oben in der Hierarchie aus, die diese Domäne enthält. Dieses Feld muss einen Wert haben, damit die Domäne in der Domänenzuordnung angezeigt wird.
Aktiv	Aktivieren Sie die Checkbox, um die Domäne zur Verwendung verfügbar zu machen. Sie müssen diese Option auswählen, damit diese Domäne in der Domänenzuordnung angezeigt wird.
Beschreibung	Geben Sie eine Beschreibung für die Domäne ein.

Jeder Domänendatensatz kann auch mehrere zugehörige Datensätze haben:

- Unternehmen
- Enthält Domänen
- Enthalten in

Nächste Maßnahme

Um die Domänenhierarchie zu ändern, wechseln Sie zur zugehörigen Liste „Enthält Domänen“, und wählen Sie die Domänendatensätze aus, die die untergeordneten (enthaltenen) Domänen der Beziehung „Enthält“ sind.

Legen Sie eine Domäne als Standard fest

Eine Domäne wurde zur Standarddomäne gemacht, der das System automatisch Aufgaben- und Benutzerdatensätze zuweist, die noch keiner Domäne zugewiesen sind.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Wenn Sie keine Standarddomäne festlegen, werden neue Aufgaben und Benutzerdatensätze in der globalen Domäne platziert.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**.
2. Öffnen Sie die Domäne, die die Standarddomäne sein soll, z. B. Main.
3. Konfigurieren Sie das Formularlayout, um das Feld **Standard** hinzuzufügen.
4. Aktivieren Sie das Kontrollkästchen **Default (Standard)**.
5. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie die Domäne für bestimmte Datensätze manuell

Standardmäßig weist das System automatisch eine Domäne basierend auf dem Unternehmensdatensatz des Benutzers zu. In einigen Fällen möchten Domänenadministratoren jedoch manuell verwalten, zu welcher Domäne ein bestimmter Datensatz gehört.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Über das Feld **Verwaltete Domäne** können Domänenadministratoren manuell eine Domäne für den Benutzer-, Gruppen-, Abteilungs-, Standort- oder CI-Datensatz auswählen, anstatt die Domäne zu verwenden, die automatisch aus dem Unternehmensdatensatz zugewiesen wird. Das Feld **Verwaltete Domäne** ist für diese Datensatztypen verfügbar.

- Benutzerdatensätze
- Gruppendatensätze
- Abteilungsdatensätze
- Standortdatensätze
- CI-Datensätze

Prozedur

1. Navigieren Sie zu dem Datensatz, den Sie manuell verwalten möchten.
2. Aktivieren Sie das Kontrollkästchen **Verwaltete** Domäne.
3. **Wählen** Sie im Feld Domäne die Domäne für den Datensatz aus.
4. Klicken Sie auf **Aktualisieren**.

   Wenn Sie das Kontrollkästchen **Verwaltete Domäne** deaktivieren, wird das Feld **Domäne** ausgeblendet, und der Datensatz verwendet den Domänenwert des Unternehmens des Datensatzes.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Nach Domänen getrennte Tabellen

Mit der Funktion „Domain Separated Tables“ können Sie auf einen Blick sehen, welche Tabellen in Ihrer Instanz nach Domänen getrennt sind.

Übersicht

Verwenden Sie die Funktion Domänengetrennte Tabellen, um anzuzeigen, welche Tabellen domänengetrennt sind. Beginnen Sie mit der Eingabe von „Domäne“ in den Filter **Alle**, um im linken Navigationsbereich auf Domänengetrennte **Tabellen** zuzugreifen.

Sie können diese Ansicht filtern, um Spaltennamen anzuzeigen oder zu entfernen, um nach bestimmten Eigenschaften oder Attributen zu suchen, die in Ihren Tabellen enthalten sind. Es gibt zwei Tabellentypen, die in der Liste angezeigt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Tabellen, in denen eine explizite **Spalte***sys_domain* vorhanden ist, wobei der Spaltenname den Wert *sys_domain* in der Liste anzeigt.
- Tabellen, die das Attribut *domain_master* verwenden, um die Domänentrennung von einem referenzierten Datensatz abzuleiten, wobei die Spalte **Attribute** den Wert *domain_master=ref-field-value* enthält.

Wenn Sie im Menü „Spaltenname“ die Auswahl „Übereinstimmung anzeigen“ oder „Herausfiltern“ verwenden, können Sie diese beiden Tabellentypen anzeigen.

Domänenüberschreibungsbetrachter

Mit dem Domänenüberschreibungs-Viewer können Sie alle Prozessüberschreibungen in der gesamten Instanz gleichzeitig anzeigen und verwalten.

Übersicht

Anstatt eine aufwändige Suche nach Überschreibungen in Ihren Skripts zu erstellen, können Sie sie mit dem Domänenüberschreibungs-Viewer schnell finden. Beginnen Sie mit der Eingabe von „Domäne“ in den Filter **Alle**, um im linken Navigationsbereich auf den **Domänenüberschreibungs-Viewer** zuzugreifen.

Die Tabellenauswahl im Domänenüberschreibungs-Viewer zeigt eine Liste nur der Tabellen an, die Datensatzüberschreibungen enthalten, zusammen mit der Anzahl der Überschreibungen in dieser Tabelle. Nachdem Sie eine Tabelle ausgewählt haben, wird eine Liste aller übergeordneten Datensätze mit Überschreibungen zurückgegeben. Sie können schnell alle **übergeordneten Datensätze**, die **Domäne** des übergeordneten Datensatzes und die **Anzahl** der Überschreibungen für jeden Datensatz anzeigen.

Wenn Sie Überschreibungen anzeigen **auswählen**, wird eine neue Registerkarte geladen, auf der alle Überschreibungen, einschließlich des übergeordneten Datensatzes, in der Standardlistenansicht angezeigt werden. Wählen Sie eine Tabelle aus der Dropdown-Liste aus, um alle Datensätze und Überschreibungen anzuzeigen. Wählen Sie Überschreibungen anzeigen für einen Datensatz aus, um alle **datensatzspezifischen** Überschreibungen anzuzeigen.

Hinweis:
Nur Tabellen mit Überschreibungen werden aufgelistet.

Weitere Informationen finden Sie unter Domänengetrennte Eigenschaftsüberschreibungen erstellen .

Aktivieren oder deaktivieren Sie eine Domäne

Wenn Sie eine Domäne aktivieren oder deaktivieren, kaskadiert der Aktivierungsstatus auf Unternehmen innerhalb der Domäne.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie einen Unternehmensdatensatz aktivieren, wird durch die Domänentrennung automatisch die zugehörige Domäne des Unternehmens aktiviert. Wenn Sie beispielsweise das Unternehmen ACME aktivieren, aktivieren Sie auch die Domäne TOP/ACME.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zum Domänendatensatz.
2. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Aktiv**.
3. Klicken Sie auf **Aktualisieren**.

> **Warnung:**
> Löschen Sie keine Domänen. Deaktivieren Sie Domänen, die Sie nicht mehr benötigen, anstatt sie zu löschen.

Fügen Sie einer Tabelle ein Domänenfeld hinzu

Trennen Sie als Administrator eine benutzerdefinierte Tabelle nach Domänen, indem Sie ihr ein sys_domain-Feld hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

> **Hinweis:**
>
> Fügen Sie Basissystemtabellen keine Domänen hinzu.

Prozedur

1. Navigieren Sie zur Listenansicht der Tabelle.
   Beispiel: Typ <table name>.list im Navigationsfilter.
2. Klicken Sie mit der rechten Maustaste auf die Listenkopfzeile, und wählen Sie **Konfigurieren** > **Listenlayout**.
3. Geben Sie im Abschnitt **Neues Feld erstellen**sys_domain als **Name** und Domänen-ID als **Typ**ein.
4. Klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Speichern**.

> **Hinweis:**
>
> Jede andere Methode zum Erstellen eines Felds fügt dem Spaltennamen das Präfix **u_** hinzu. Beim Domänenfeld erstellt das System das Feld jedoch automatisch ohne das Präfix **u_**. Sie können die folgende Funktionalität als Kurzbefehl verwenden: Wenn Sie ein **sys_domain**-Feld erstellen, nennen Sie es **sys_domain**, und lassen Sie den Feldtyp unverändert. Das System legt den Feldtyp automatisch auf Domänen-**ID** und die Feldbezeichnung auf **Domäne**fest, wodurch Sie sich einige Klicks sparen.
>
> Das Hinzufügen von Domänen zu Basissystemtabellen erfordert übermäßig gründliche Tests, Aktualisierungen und das Hinzufügen neuer Logik. Darüber hinaus ist der Quellcode in vielen Fällen für den Kunden nicht zugänglich.

Zeigen Sie Domänenbeziehungen an

Die Domänenzuordnung bietet Domänenadministratoren eine schreibgeschützte Darstellung der aktiven Domänen in der Instanz und ihrer Beziehung zueinander.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Für alle Domänenzuordnungen muss eine Domäne als primäre Domäne festgelegt sein. Darüber hinaus muss jede Domäne in der Domänenzuordnung die folgenden Kriterien erfüllen:

- Das Feld „ **Übergeordnet** “ muss ausgefüllt werden (die einzige Ausnahme ist die primäre Domäne).
- Das Kontrollkästchen **Aktiv** muss aktiviert sein.

Die Domänenzuordnung zeichnet keine Domänenbeziehungen für Domänen, die die Zuordnungskriterien nicht erfüllen.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänenzuordnung**.
2. Klicken Sie auf die Plus- (**+**) oder Minus- (**-**) Symbole in den Domänenheadern, um Subdomänen ein- oder auszublenden.

Wählen Sie eine primäre Domäne aus

Die primäre Domäne gibt die Domäne der obersten Ebene in der Domänenzuordnung an.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

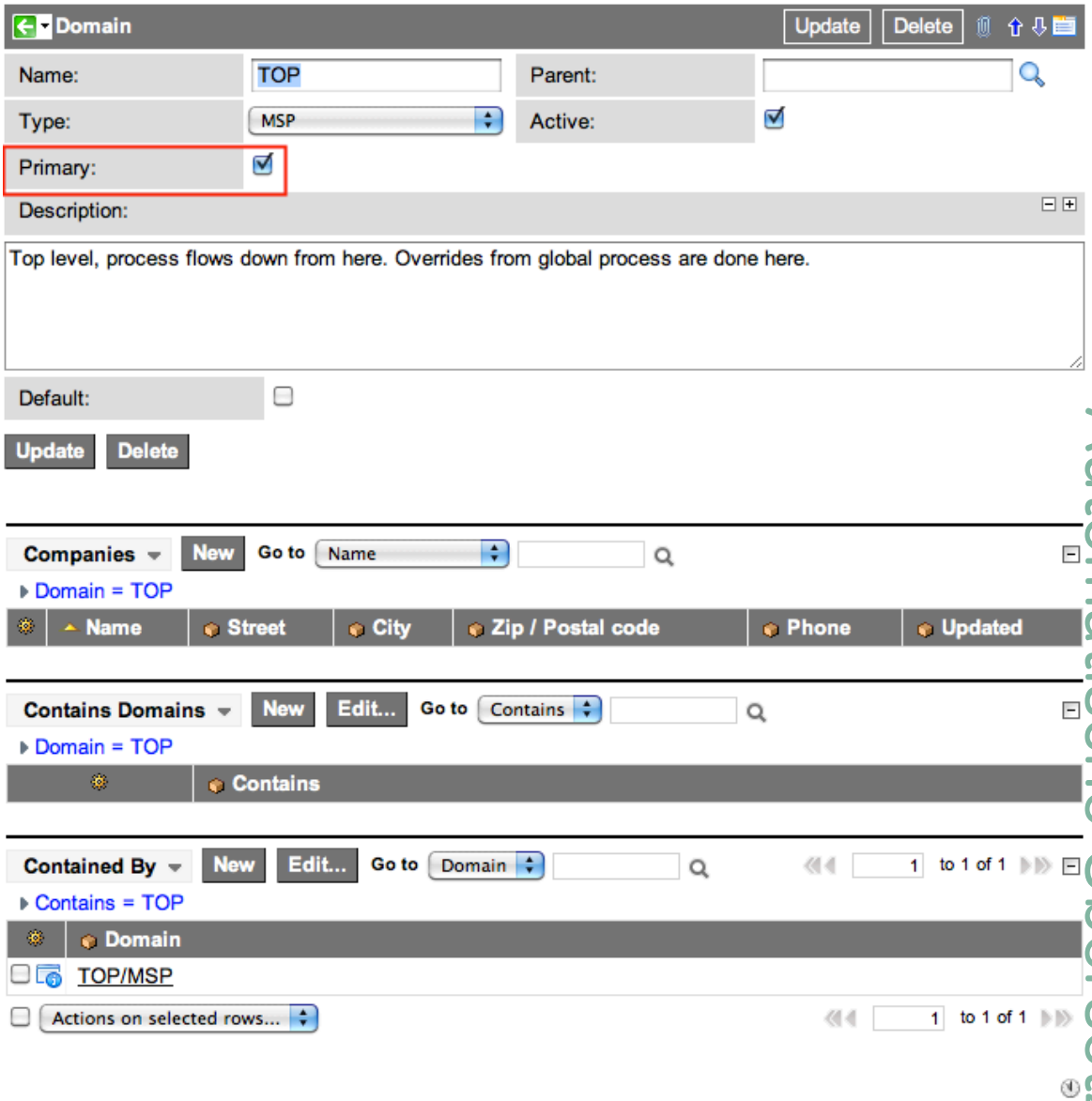
Die primäre Domäne darf keine übergeordnete Domäne haben und muss mindestens eine untergeordnete Domäne haben. Es kann jeweils nur eine primäre Domäne geben. Wenn Sie eine andere Domäne als primäre Domäne auswählen, wird die vorherige primäre Domäne überschrieben.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**.
2. Wählen Sie die Domäne aus, die die primäre Domäne sein soll, z. B. TOP.
3. Aktivieren Sie das Kontrollkästchen **Primär**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Aktualisieren**.



Automatische Übersetzung

Erstellt Enthält-Beziehungen zwischen Domänen

Erstellen Sie eine Beziehung vom Typ „Enthält“ zwischen Domänen, um die Domänenhierarchie zu ändern.

Vorbereitungen

Erforderliche Rolle: admin

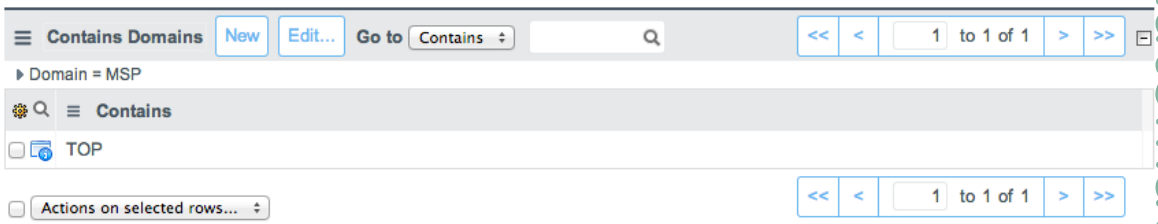
Warum und wann dieser Vorgang ausgeführt wird

Domänen in einer Beziehung vom Typ „Enthält“ erben die Einstellungen der enthaltenen Domäne. Die enthaltende Domäne ermöglicht es Benutzern, Daten in der enthaltenen Domäne sowie in ihren untergeordneten Domänen anzuzeigen. Prozesse sind von einer Beziehung vom Typ „Enthält“ nicht betroffen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Domänentabelle.
2. Wählen Sie den Domänendatensatz aus, der die übergeordnete Domäne (Container) der neuen enthält-Beziehung ist.
3. Schalten Sie den Domänenbereich um, um bei Bedarf zwischen dem Sitzungsbereich und dem Datensatzbereich zu wechseln.
4. Klicken Sie in der zugehörigen Liste „Enthält Domänen“ auf **Bearbeiten**.
5. Wählen Sie die Domänendatensätze aus, die die untergeordneten (enthaltenen) Domänen der Beziehung „Enthält“ sind.
   Standardmäßig werden nur untergeordnete Domänen angezeigt, wenn die Domänenauswahl auf Global festgelegt ist. Schalten Sie den Domänenbereich um, um alle Domänen anzuzeigen.
6. Klicken Sie auf **Speichern**und dann auf **Aktualisieren**.



Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenbereich erweitern

Wenn ein Benutzer in der globalen Domäne eine Tabelle mit einer **sys_overrides-** Spalte anzeigt, sieht er standardmäßig nur Datensätze aus der globalen Domäne. Wenn ein Administrator in der globalen Domäne eine Prozesstabelle anzeigt, sieht dieser Administrator nur Datensätze, die sich in dieser Prozesstabelle befinden.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Ändern Sie die Eigenschaft `glide.sys.restrict_global_domain_processes` in **true**.
2. Um Datensätze aus allen Domänen anzuzeigen, klicken Sie unter Zugehörige Links auf **Domänenbereich erweitern**.
3. Klicken Sie auf Domänenbereich reduzieren, um nur Datensätze aus der globalen Domäne **anzuzeigen**.

Fügen Sie Domänen einer Liste der Sichtbarkeitsdomänen hinzu

Durch das Hinzufügen einer Sichtbarkeitsdomäne kann ein Benutzer oder eine Gruppe Datensätze aus einer anderen Domäne anzeigen und möglicherweise bearbeiten, unabhängig von der normalen Domänenmitgliedschaft des Benutzers oder der Gruppe.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Das Zuweisen von Sichtbarkeitsdomänen an alle Mitglieder einer Gruppe wird bevorzugt, anstatt sie einzelnen Benutzern zu gewähren.

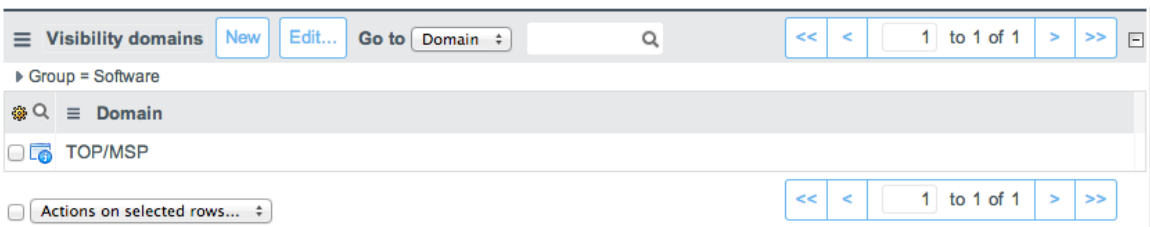
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Durch das Hinzufügen einer Sichtbarkeitsdomäne werden die Anforderungen der Zugriffskontrollregel einer Tabelle oder eines Datensatzes nicht geändert.

Prozedur

1. Navigieren Sie zur Gruppentabelle.
2. Wählen Sie die Gruppe aus, für die Sie Sichtbarkeitsdomänen bereitstellen möchten.
3. Fügen Sie dem Formular die zugehörige Liste **Sichtbarkeitsdomänen hinzu**.
4. Klicken Sie in der zugehörigen Liste **Sichtbarkeitsdomänen** auf **Bearbeiten**.
5. Wählen Sie die Domänendatensätze aus, die die Gruppe oder Domäne anzeigen soll.
6. Klicken Sie auf **Speichern**und dann auf **Aktualisieren**.



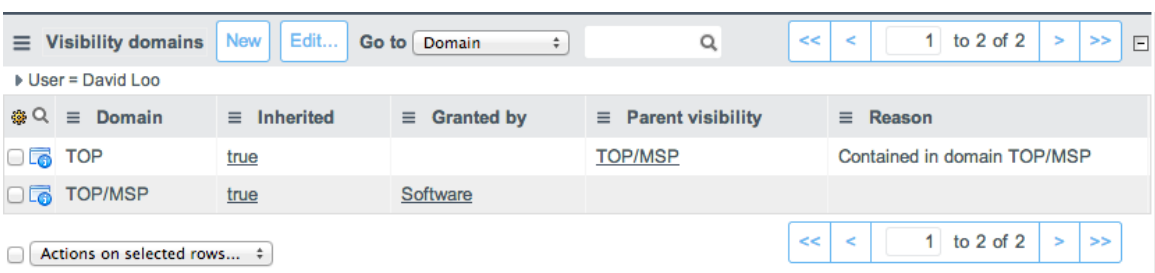
Gewähren Sie einem einzelnen Benutzer Sichtbarkeitsdomänen

Es ist zwar möglich, Sichtbarkeitsdomänen für bestimmte Benutzer im Benutzerformular hinzuzufügen, es ist jedoch am besten, sie nur über Gruppen hinzuzufügen. Dies steuert Berechtigungen und Zugriff, wenn Personen die Abteilung wechseln oder das Unternehmen verlassen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Benutzer**.
2. Wählen Sie den Benutzer aus, dem Sie Sichtbarkeitsdomänen bereitstellen möchten.
3. Fügen Sie dem Formular die zugehörige Liste **Sichtbarkeitsdomänen hinzu**.
4. Klicken Sie in der zugehörigen Liste „Sichtbarkeitsdomänen“ auf **Bearbeiten**.
5. Wählen Sie die Domänen aus, deren Datensätze der Benutzer sehen soll.
6. Klicken Sie auf **Speichern**und dann auf **Aktualisieren**.



Die eingebettete Liste der Sichtbarkeitsdomänen enthält die folgenden Felder.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Domäne	Domäne, die für die Gruppe oder den Benutzer sichtbar ist.
Geerbt	Die Domäne wird von der Domänentransparenz oder einer übergeordneten Domäne geerbt.
Gewährt von	Name der Gruppe, die die Domänensichtbarkeit gewährt hat.
Übergeordnete Sichtbarkeit	Name der übergeordneten Domäne, der zum Gruppieren von Datensätzen verwendet wird. Wenn der übergeordnete Datensatz gelöscht wird, werden auch alle Datensätze mit demselben übergeordneten Element gelöscht.

Erstellen Sie eine domänenspezifische Auswahlliste

Administratoren können Auswahllisten so konfigurieren, dass sie Einträge enthalten, die für eine bestimmte Domäne spezifisch sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Wählen Sie die Domäne aus der Domänenauswahl aus, der die Auswahl hinzugefügt werden soll.
2. Klicken Sie mit der rechten Maustaste auf das Auswahlfeld, das Sie anpassen möchten, und wählen Sie Auswahlmöglichkeiten **konfigurieren**aus.
3. Aktualisieren oder fügen Sie Auswahlmöglichkeiten hinzu.
4. Übertragen Sie Änderungen über den normalen Change-Prozess, z. B. Update Sets.

> **Hinweis:**
> Administratoren sollten sicherstellen, dass die Auswahlmöglichkeiten domänenübergreifend eindeutig sind, um administrative Verwirrung in der globalen Domäne zu vermeiden.

Wenn ein Administrator eine neue Auswahl aus der globalen Domäne hinzufügt, sehen Benutzer aus Domänen niedriger in der Hierarchie die neue Auswahl am Ende ihrer aktuellen Auswahllisten. Wenn die neue Auswahl auf globaler Ebene nicht aktiv ist, steht sie den Domänenbenutzern über Auswahlmöglichkeiten **konfigurieren** zur Verfügung, wird jedoch nicht als aktive Auswahl angezeigt.

Erweiterte Verwaltung der Domänentrennung

Administratoren können Informationen zur Domänentrennung anzeigen, potenzielle Probleme identifizieren und Konfigurationseinstellungen ändern.

Sie können die folgenden erweiterten administrativen Aufgaben für Domänen ausführen:

- Verwenden Sie Domänenauswahlmenüs
- Zeigen Sie Domänenbeziehungen an

Verwenden Sie Domänenauswahlmenüs

Die Instanz bietet die Domänenauswahl über zwei Menüformate.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Domänenauswahl: Bietet eine einfache Dropdown-Liste der verfügbaren Domänen.
- Domänenreferenzauswahl: Aktiviert ein Referenzfeld, das Filter und eine Type-ahead-Eintragsfunktion für die automatische Vervollständigung bietet. Verwenden Sie dieses Format für längere Listen.

Die Platzierung dieser Auswahlen und das Verfahren zum Ein- oder Ausblenden unterscheiden sich je nach Version der Benutzeroberfläche.

Aktivieren Sie Domänenauswahlmenüs in Core-UI

Wenn Sie die Domänenauswahl in Core-UI anzeigen, wird die Domänenauswahl standardmäßig aktiviert. Nach dem Aktivieren der Domänenauswahl können Sie eine Systemeigenschaft hinzufügen, um die Domänenreferenzauswahl zu aktivieren.

Vorbereitungen

Hinweis:
Die Domänentrennung (Plugin com.snc.pa.domain_support) ist erforderlich, um die Domänenreferenzauswahl zu aktivieren.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Klicken Sie im Header auf das Zahnradsymbol.
2. Klicken Sie auf der Registerkarte Allgemein auf den Schalter **Domänenauswahl in Header** anzeigen.
   Die Domänenauswahl wird im Header Core-UI angezeigt.
3. **Wahlweise:** Aktivieren Sie die Domänenreferenzauswahl.

   Hinweis:
   Durch Aktivieren der Domänenreferenzauswahl wird die globale Option aus der Liste entfernt. Um zu Ihrer Startdomäne zurückzukehren, klicken Sie auf den Zurück-Pfeil neben dem Referenzfeld. Administratorbenutzer können auf den Zurück-Pfeil klicken, um zur globalen Domäne zurückzukehren.

   a. Geben Sie `sys_properties.list` im Anwendungsnavigator ein.
   b. Wenn noch nicht vorhanden, fügen Sie die Eigenschaft `glide.ui.domain_reference_picker.enabled` hinzu, und legen Sie den Wert auf **true**fest.
   c. Aktualisieren Sie den Browser.
   Die Domänenreferenzauswahl wird im Header Core-UI angezeigt.

Beschränken Sie den Zugriff auf die Domänenauswahl

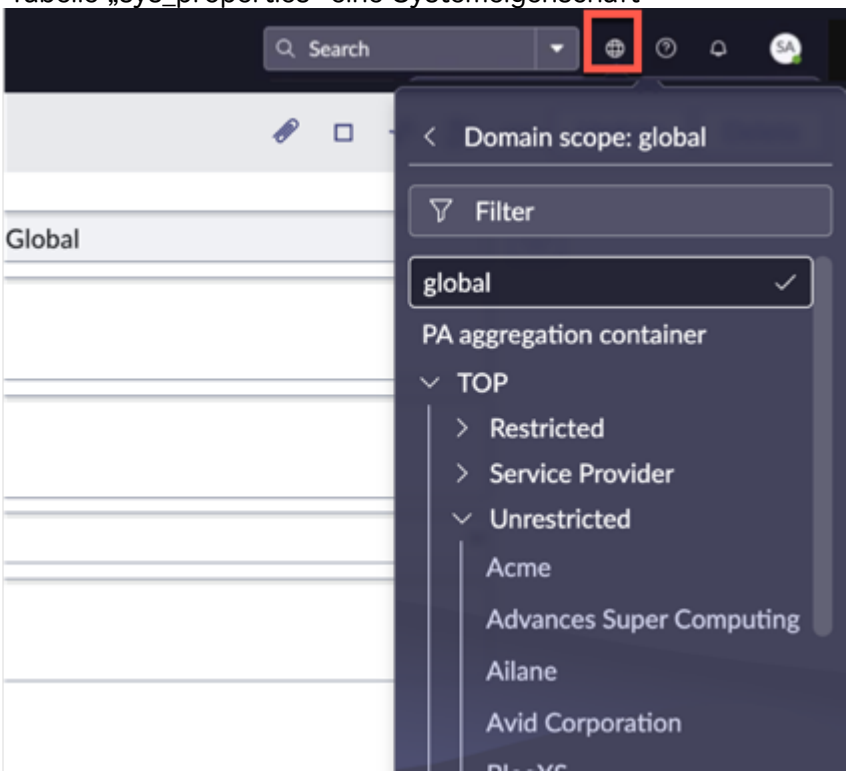
Verwenden Sie eine Systemeigenschaft, um den Zugriff auf die Domänenauswahl in Core-UI und Next Experienceeinzuschränken.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig können Benutzer mit der ITIL-Rolle und Rollen, die die ITIL-Rolle enthalten (z. B. Administratoren), in Next Experienceauf die Domänenauswahl zugreifen. Sie können anderen Rollen Zugriff gewähren, indem Sie sie der Eigenschaft hinzufügen, oder Rollen einschränken, indem Sie sie entfernen. Es wird empfohlen, die Rolle nur auf Administratoren zu beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratoren können Benutzern Zugriff gewähren, indem sie in der Tabelle „sys_properties“ eine Systemeigenschaft erstellen.



Prozedur

1. Öffnen Sie die Tabelle „Systemeigenschaften“ [sys_properties].
2. Fügen Sie diese Eigenschaft hinzu: `glide.ui.polaris.domain_picker.role`
3. Konfigurieren Sie den Eigenschaftswert als kommagetrennte Liste von Rollen: **admin, itil**.
   Weitere Informationen finden Sie unter Next Experience-Auswahlen konfigurieren

Eigenschaften der Anwendung zur Domänentrennung

Das Plugin „Domain Separation“ verfügt über zwei neue Tabellen, um Service Providern mehr Flexibilität bei der Anpassung ihrer Anwendungen zu geben, die Domänentrennung verwenden. Diese Tabellen sind die Tabelle „Systemanwendungseigenschaft“ [sys_application_property] und die Tabelle „Systemanwendungseigenschaftswert“ [sys_application_property_value].

Neue Tabellen bieten mehr Optionen

Bei Anwendungen von Service Providern (SP) können bestimmte Aktionen je nach Domäne variieren. Die Tabelle „ ServiceNow® Basissystem-Systemeigenschaften [sys_properties] ist jedoch nicht domänengetrennt, sodass sie die Anforderungen für Anwendungen, die Domänentrennung verwenden, nicht erfüllt.

Jeder SP-Kunde möchte seine Anwendungen möglicherweise anders anpassen. Zuvor wurden Funktionen, die angepasst werden konnten, nur als ein globaler Wert definiert. Anwendungsentwickler benötigen eine flexiblere Tabelle. Jetzt können Sie Ihre Anwendung ändern, ohne jedes Mal Code erstellen zu müssen, wenn Sie die Funktionalität hinzufügen oder ändern möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsweise von Überschreibungen in den neuen Tabellen

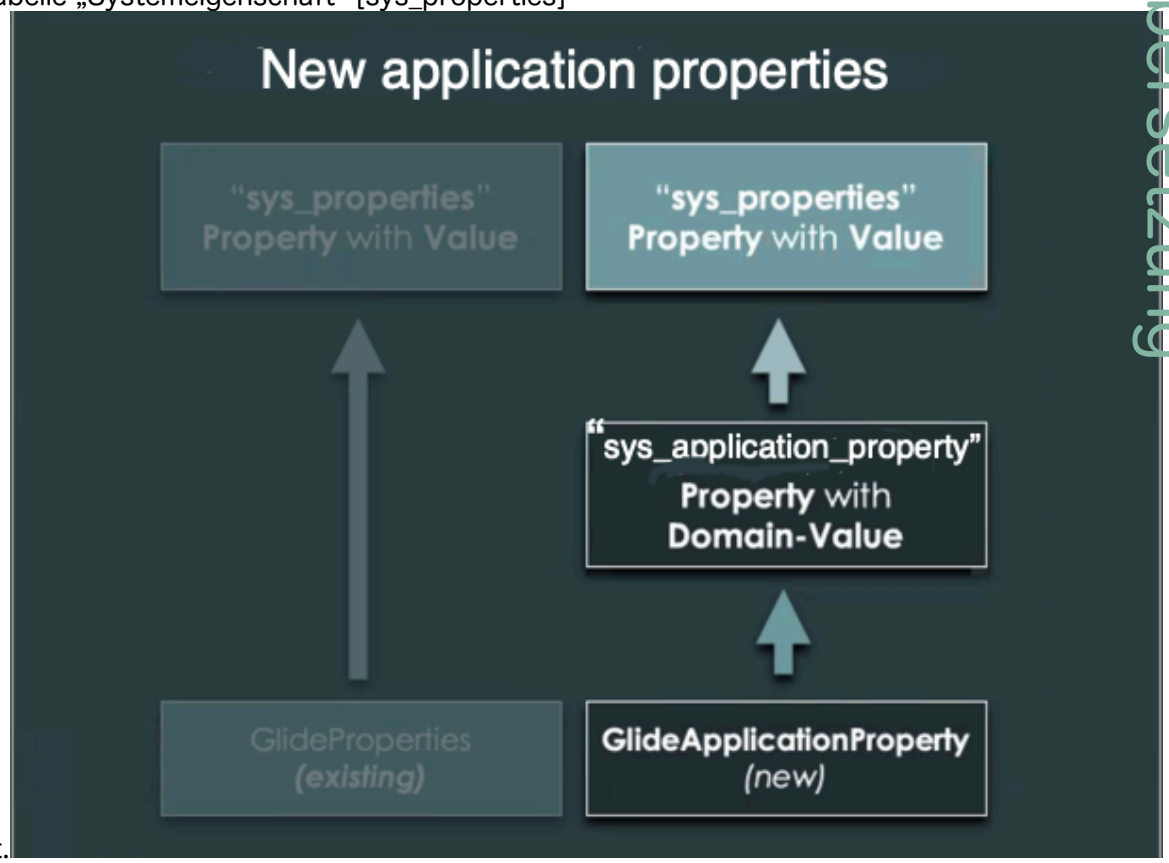
Entwickler verwenden normalerweise die Tabelle ServiceNow Systemeigenschaft [sys_properties], um verschiedene Funktionen in Anwendungen zu erstellen. Wenn Sie eine Anwendung entwickeln möchten, die sich in verschiedenen Domänen unterschiedlich verhält, müssen Sie sie selbst anpassen.

Im Paris-Release vereinfacht die neue Tabelle „Anwendungseigenschaft“ [sys_application_property] diese Anpassung. Anstatt für einen Wert direkt in die Systemeigenschaftentabelle zu wechseln, wird die Anwendungseigenschaftentabelle zuerst in die Systemanwendungstabelle verschoben. Diese neue Tabelle speichert jetzt die Logik, die Sie zum Konfigurieren Ihrer Anwendung benötigen. Wenn eine Eigenschaft in der neuen Tabelle gefunden wird, wird dieser Inhalt verwendet. Wenn in dieser Tabelle keine Informationen vorhanden sind, wird in die Basissystem-Eigenschaftentabelle gewechselt.

Wenn Sie die Unterstützung für Domänentrennung konfigurieren, können Sie dieser neuen Anwendungseigenschaftentabelle Domänenlogik hinzufügen. Diese Tabelle kann Eigenschaften enthalten, die in der Tabelle „Systemeigenschaften“ nicht vorhanden sind. Oder Sie können der Konfigurationstabelle Eigenschaften hinzufügen, die alle in der Tabelle „Systemeigenschaften“ ausgewählten Eigenschaften überschreiben können.

Angenommen, Sie möchten eine Anwendung mit einer Funktion für den ersten Tag der Woche konfigurieren. Manchmal möchten Sie vielleicht, dass der erste Tag der Woche Sonntag ist. In anderen Fällen möchten Sie vielleicht, dass der erste Tag der Woche Montag ist. In der Basissystemtabelle gibt es möglicherweise nur eine Option für Tag 1, und zwar Sonntag. Mit der neuen Tabelle können Sie eine weitere Eigenschaft speichern, indem Sie Tag 1 zu „Sonntag“ und eine untergeordnete Domäne zu „Montag“ machen.

Diese Abbildung zeigt, wie das System Eigenschaften aus der Tabelle „Anwendungseigenschaften“ bezieht, bevor es zur Tabelle „Systemeigenschaft“ [sys_properties] wechselt.

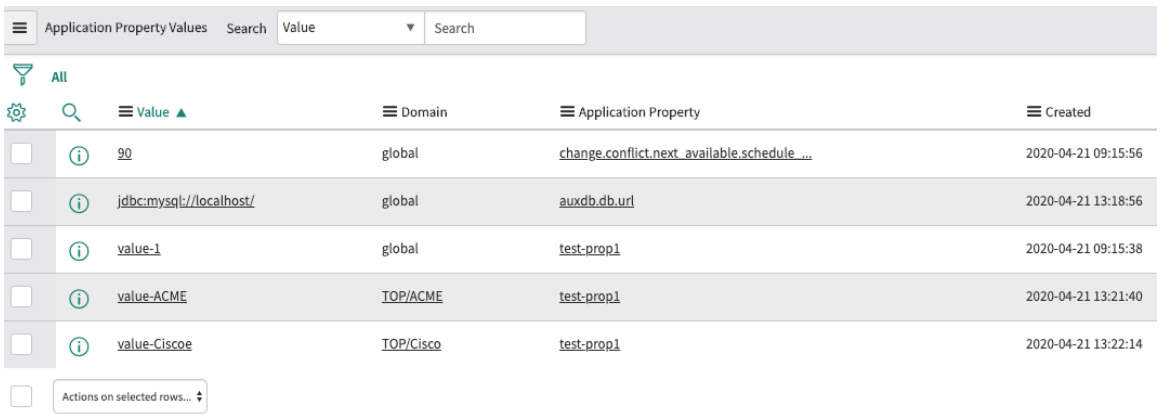


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie bereichsbezogene Apps in der neuen Tabelle funktionieren

Die neue Tabelle „Anwendungseigenschaften“ wird von bereichsbezogenen Anwendungen unterstützt. Der Anwendungseigenschaftsname ist ähnlich wie der Systemeigenschaftsname eindeutig. Dies bedeutet, dass ihm der Bereichsname vorangestellt wird, wenn er nicht global ist. Der Umfang einer Anwendung wirkt sich auf Ihre Konfiguration aus. Der Umfang kann bestimmen, welcher Tag 1 als Sonntag und welcher als Montag definiert ist. Sie können dieselbe Eigenschaft verwenden, sie jedoch so anpassen, dass „Tag 1, Sonntag“ die übergeordnete Domäne und Tag 1, Montag die untergeordnete Domäne ist. In der neuen Tabelle gibt es sowohl eine Domänenspalte als auch eine Bereichsspalte, sodass Sie diese Eigenschaften für beide festlegen können.

Sie können die Ansicht Domänenbereich erweitern in der Tabelle „sys_application_property_value“ verwenden, um alle Überschreibungen anzuzeigen, wie in der folgenden Abbildung dargestellt.



Hinweis:

Wenn diese Tabellen nicht verfügbar sind, stellen Sie sicher, dass Sie das Plugin „Domain Extension Installer“ (com.glide.domain.msp_extensions.installer) aktiviert haben.

Neue Anwendungseigenschaftstabellen

Die neue Tabelle „Systemanwendungseigenschaft“ [sys_application_property] enthält die folgenden Felder:

- Name
- Beschreibung
- Typ (Auswahl Zeichenfolge, Wahr|Falsch, Ganzzahl, Zeitzone, Farbe usw.)
- default_value
- Eigenschaft (Verweis auf sys_properties)
- „usage_notes“
- read_roles
- write_roles
- eindeutiger Schlüssel: (name)

Die neue Tabelle „Systemanwendungseigenschaftswert“ [sys_application_property_value] enthält die folgenden Felder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sys_application_property (Verweis auf sys_application_property)
- sys_domain
- sys_overrides
- Wert
- Eindeutiger Schlüssel: (sys_application_property, sys_domain)

Neue APIs

Die neuen APIs werden auch in bereichsbezogenen Apps unterstützt. Domänengetrennte Anwendungseigenschaften haben unterschiedliche APIs. Die GlideApplicationProperty-API verfügt über zwei neue skriptfähige Methoden, die sowohl in globalen als auch in bereichsbezogenen Anwendungen verfügbar sind. Weitere Informationen zu diesen neuen APIs finden Sie unter GlideApplicationProperty – Scoped, Global .

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenmigrationstool

Verwenden Sie das Domänenmigrationstool, um einen Kunden aus einer domänengetrennten Umgebung in eine eigene dedizierte Instanz zu verschieben.

Plugin „Domain Migration Tool“

Das Plugin „Domain Migration Tool“ (com.glide.domain.migration_tool) vereinfacht die Aufgabe, einen Kunden aus einer domänengetrennten Umgebung in eine flexiblere dedizierte Instanz zu verschieben. Kunden möchten möglicherweise zu einer separaten Instanz migrieren, um die Fähigkeiten von Now Platform besser nutzen zu können. Obwohl das Plugin „Domain Separation“ installiert ist, sind die Daten- und Prozesstrennungseigenschaften deaktiviert.

Hinweis:
Sie müssen eine geklonte Instanz anfordern und die Aktivierung des Plugins „Domain Migration Tool“ anfordern, bevor Sie es verwenden können.

Das Domänenmigrationstool wird nur ausgeführt, wenn Daten- und Prozesstrennung in der domänengetrennten Instanz aktiviert sind:

- Die Dateneigenschaft `glide.sys.domain.partitioning` muss auf **true**festgelegt werden.
- Die Prozesseigenschaft `glide.sys.domain.delegated_administration` muss auf **true**festgelegt werden.

Was das Migrationstool tut

- Automatisiert einen Großteil des Migrationsprozesses, insbesondere die Datenbereinigung.
- Migriert die domänengetrennte Instanz in eine neue dedizierte Instanz.
- Löscht Daten aus der dedizierten Instanz.

Hinweis:
Das Tool löscht keine globalen Daten in der Zieldomäne oder in zusätzlichen Datendomänen (falls angegeben).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Reduziert Prozessdaten oder löscht Prozessdaten, wenn dies nicht möglich ist
- Behält Prozessdatensätze bei, die für die Zieldomäne sichtbar sind
- Aktualisiert die Spezialtabellen sys_choice, sys_ui_list und sys_ui_related_list
- Bereinigt Datensätze, die von Plugins für Domänentrennung hinzugefügt wurden:
  - Business-Regeln
  - UI-Aktionen
  - Geplante Aufgaben
  - Die Installation wird beendet
  - Navigationsmodule
- Deaktiviert die Domänentrennung und entfernt Domänen aus der geklonten Instanz:
  - Legt diese Eigenschaften in der geklonten Instanz auf „ **false** “ fest:
    - *`glide.sys.domain.partitioning`*
    - *`glide.sys.domain.delegated_administration`*
    - *`glide.sys.domain.enabled`*
  - Löscht alle Domänen mit Ausnahme der Zieldomäne und zusätzlicher angegebener Datendomänen.
- Aktualisiert das Feld **Status** in der Tabelle „domain_migration_tool_status“.

Individueller Status der Tabellen

Status	Beschreibung
Ausstehend	Standardstatus von domänengetrennten Tabellen während der Migration. Die Migration der Tabellen ist geplant, die Migration wurde jedoch noch nicht gestartet.
Fehler	Fehler auf Tabellenebene. Wenn der Migrationsprozess mit Fehlern abgeschlossen wurde, gibt dieser Status an, welche Tabellen Fehler enthalten.
Wird ausgeführt	Der Status der Tabelle, die derzeit migriert wird. Nur eine Tabelle kann diesen Status haben und wird derzeit migriert.
Erfolgreich	Der Status der Tabellen, die erfolgreich migriert wurden.
Erfolgreich beendet	Der Migrationsprozess wurde ohne Fehler abgeschlossen.
Mit Fehlern abgeschlossen	Der Migrationsprozess wurde mit Fehlern abgeschlossen.

- Protokolliert Fortschritt und Status in syslog_domain

  Die Quelle ist **MigrationTool** für alle Protokolleinträge, die der Migration zugeordnet sind.

  - Protokolliert jede Datentabelle und wie viele Datentabellen verbleiben
  - Protokolliert jede Prozesstabelle und die Datensätze der Domäne, die derzeit deaktiviert oder gelöscht werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Was das Migrationstool nicht kann

- Klonen Sie die Instanz
- Erstellen Sie eine weitere domänengetrennte Instanz
- Migrieren Sie Datensätze (Daten oder Prozess), wenn Daten- oder Prozesstrennungseigenschaften deaktiviert sind, bevor Sie das Tool ausführen
- Ändern Sie alle Daten in der Quellinstanz
- Globale Daten in der Zieldomäne oder in zusätzlichen Datendomänen löschen (falls angegeben)

Was Sie nach der Ausführung des Tools tun müssen

Das Domänenmigrationstool automatisiert die Entfernung von Daten außerhalb der gewünschten Domänen (Zieldomäne, zusätzliche Datendomänen und globale Domäne). Sie müssen alle verbleibenden Konfigurationen bewerten, um sicherzustellen, dass sie für Ihre dedizierte Instanz geeignet sind und funktionieren. Wenn Sie beispielsweise eine Geschäftsregel hatten, die das Domänenfeld für Datensätze festlegte, möchten Sie diese Geschäftsregel möglicherweise deaktivieren, da sie keinen Zweck mehr erfüllt.

Migrieren Sie eine domänengetrennte Instanz zu einer dedizierten Instanz

Verschieben Sie einen Kunden aus einer domänengetrennten Umgebung in eine eigene dedizierte Instanzumgebung.

Vorbereitungen

Erforderliche Rolle: security_admin und admin

Prozedur

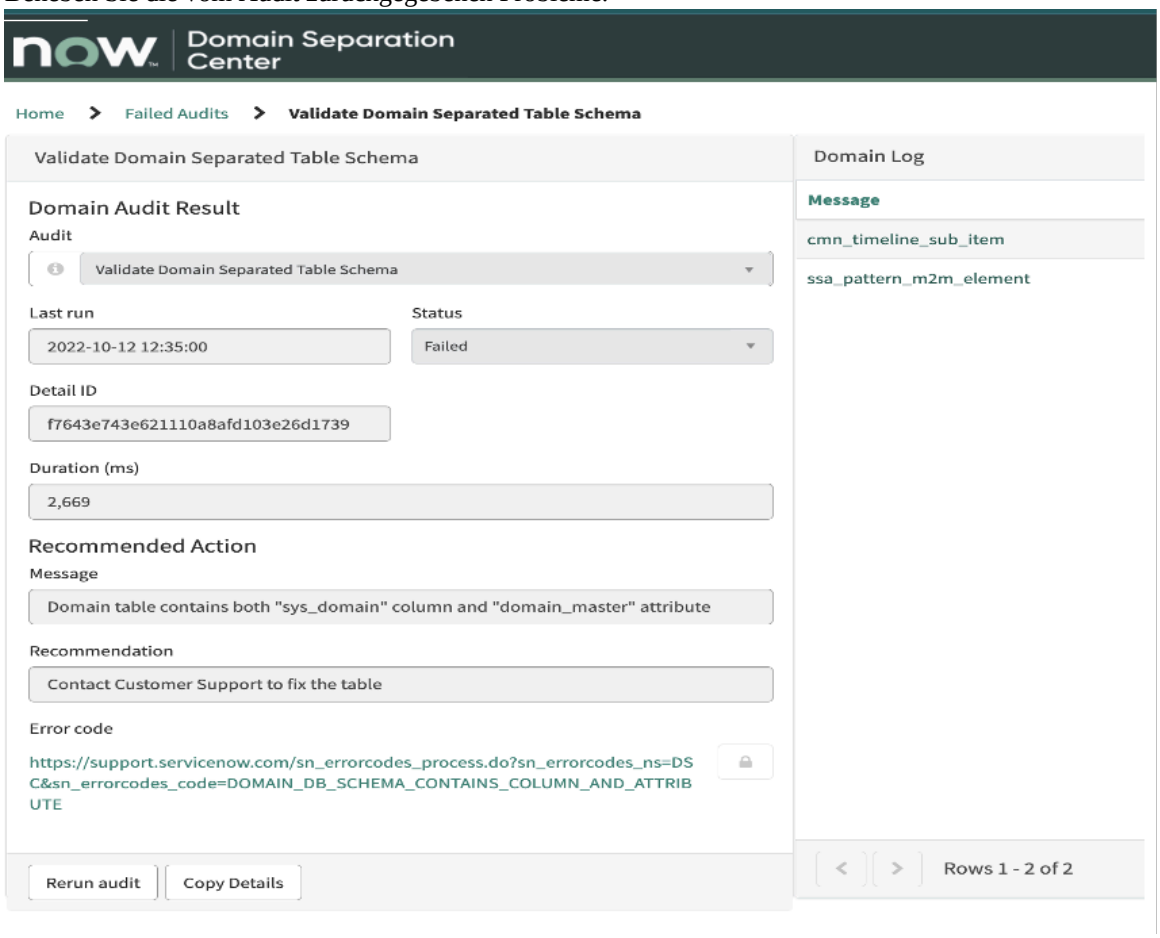
1. Erhöhen Sie die Berechtigungen auf die Rolle security_admin.
   Details siehe Führen Sie eine Erhöhung auf eine privilegierte Rolle durch.
2. Navigieren zu **Alle** > **Domänenadministrator** > **Domänenmigrationstool**.
   Greifen Sie auch mit **domain_migration_tool_status.list**zu.
3. Klicken Sie auf **Neu**.
4. Füllen Sie das Formular aus.

Feld	Beschreibung
Zieldomäne	Geben Sie die Domäne an, die sowohl für den Prozess als auch für die Daten verwendet wird, die Sie migrieren möchten. Nur die Zieldomäne wird beibehalten, keine ihrer untergeordneten Elemente, sofern dies nicht im Feld **Zusätzliche Datendomänen** angegeben ist.
Zusätzliche Datendomänen	Geben Sie optional zusätzliche Datendomänen an, die Sie migrieren möchten. Wenn Sie die Zieldomäne und alle ihre untergeordneten Elemente migrieren möchten, müssen Sie alle untergeordneten Elemente angeben.

5. Wählen Sie **Absenden**.
6. Öffnen Sie das Formular, das Sie gerade übermittelt haben.
7. Navigieren zu **Alle** > **Domain Separation Center** > **Audits konfigurieren** .
   Weitere Informationen finden Sie unter Domain Separation Center.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

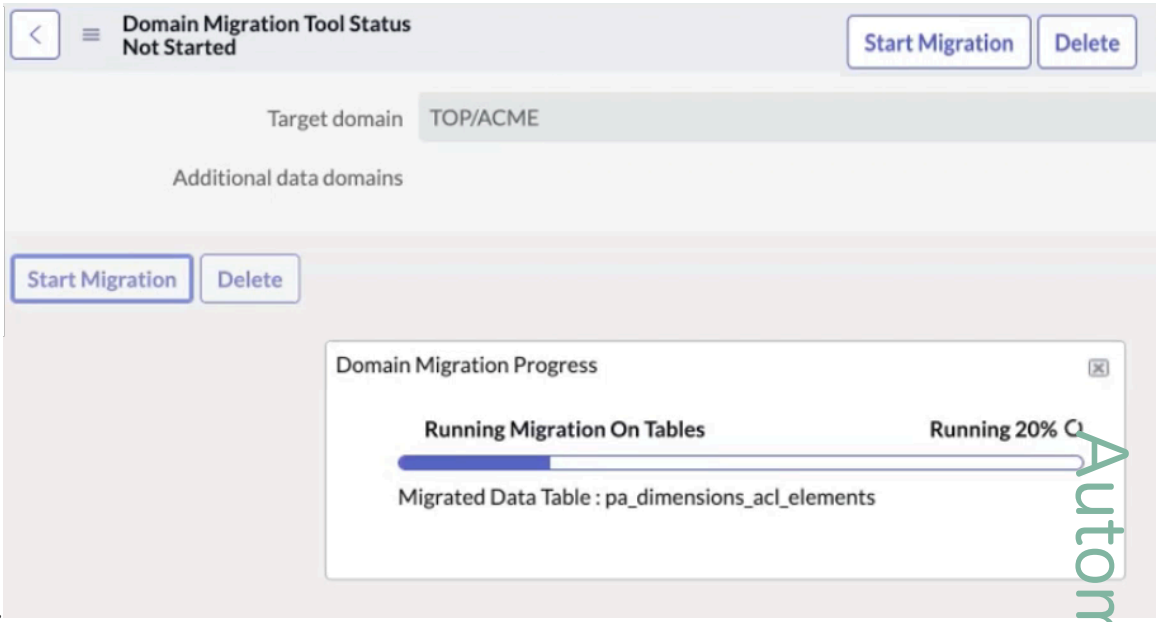
8. Legen Sie das Audit „Tabellenschema mit **Domänentrennung validieren“** auf „ **Aktiv** “ fest, und weisen Sie einen Zeitplan zu.
   Dies ist ein vorsorgliches Domänenaudit, um das Schema vorab auf die Integrität von domänengetrennten Tabellen zu überprüfen. Auf diese Weise können Sie Fehler beheben, bevor Sie die Migration ausführen.
9. Führen Sie den **Auditzeitplan aus**, der das Schema enthält.
   Details siehe Führen Sie Audits sofort aus.
10. Beheben Sie die vom Audit zurückgegebenen Probleme.



11. Wählen **Sie Migration starten aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Fortschrittsleiste der Ausführungsnachverfolgung und das Domänenmigrationstool werden



ausgelöst.

- Die aktuelle Migrationstabelle mit Fortschritt wird zusammen mit dem Gesamtprozentsatz der erfolgreich migrierten Tabellen angezeigt.
- Die Tabelle, in der alle domänengetrennten Tabellen mit dem Migrationsstatus, der Gesamtzahl der Datensätze in jeder Tabelle und der Anzahl der migrierten Datensätze aufgezeichnet werden.
- Die Anzahl der Tabellen, bei denen die Migration fehlgeschlagen ist, wird ebenfalls aufgezeichnet.
- Der **Status** wird aktualisiert, wenn das Tool seine Funktionen ausführt.
- Die Domänenmigration wird weiterhin im Hintergrund ausgeführt, wenn Sie die Fortschrittsleiste schließen. Greifen Sie auf die Tabelle `sys_execution_tracker` zu, und suchen Sie nach **Running Migration on Tables**, um den im Hintergrund ausgeführten Migrationsprozess zu überprüfen.

Der Status des Domänenmigrationstools zeigt die folgenden Felder an:

Statusfelder des Domänenmigrationstools

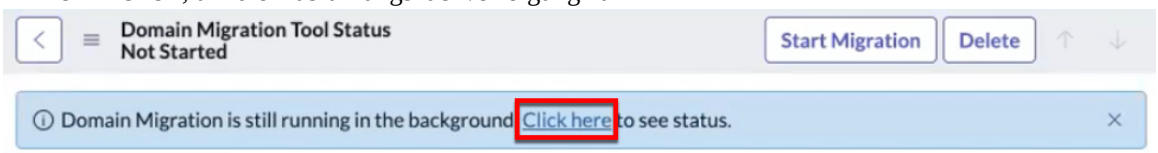
Feld	Beschreibung
Status	Zeigt den Migrationsstatus an. ○ **Datentabellen werden migriert...**: Status in Bearbeitung. ○ **Migration erfolgreich**: Der aktualisierte Status nach einer erfolgreichen Migration. ○ **In einer der domänengetrennten Tabellen wurde eine Fehlkonfiguration beobachtet**: Zeigt einen Fehler bei der Datenmigration an. Ein Schemafehler wurde gefunden, die Migration wird nicht gestartet. Führen Sie das Audit **Domänengetrenntes Tabellenschema validieren aus**. Das Audit schlägt fehl und zeigt die Tabellen an, die nicht dem Schemastandard entsprechen. ○ **Abgeschlossen mit Fehlern in Tabellen erneut aufrufen: Die Anzahl der Tabellen für die Schemamigration**ist aufgelistet. Suchen Sie die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Fehler in der Anzahl der Tabellen erneut aufrufen, und beheben Sie Schemaprobleme. ○ **Domänenmigration für Tabellen fehlgeschlagen...**: Nicht-Zieldatensätze müssen manuell aus fehlgeschlagenen Tabellen gelöscht werden. ○ **Erfolgreich abgeschlossen**: Wenn alle Tabellen migriert wurden.
Zieldomäne	Die ausgewählte Zieldomäne für die Migration.
Zusätzliche Datendomänen	Wird ausgefüllt, wenn mehrere Migrationsdomänen ausgewählt wurden.
Anzahl der erneut verarbeiteten Tabellen	Dieses Feld wird nur ausgefüllt, wenn eine Tabelle nicht migriert werden kann. Wenn es keine Fehler gibt, ist diese Anzahl null. In diesem Fall werden die Tabellen erneut aufgerufen, um die Migration erneut zu versuchen. Wenn keine Fehler auftreten, müssen die Tabellen nicht erneut aufgerufen oder die Migration erneut versucht werden.
Aktuell verarbeitete Tabelle	Zeigt den Namen der Tabelle an, die derzeit migriert wird. Nach einer erfolgreichen Migration ist dieses Feld leer.

12. Klicken Sie auf der Statusseite des Domänenmigrationstools auf den Link **Hier klicken**, um die Ausführungsnachverfolgung zu öffnen.

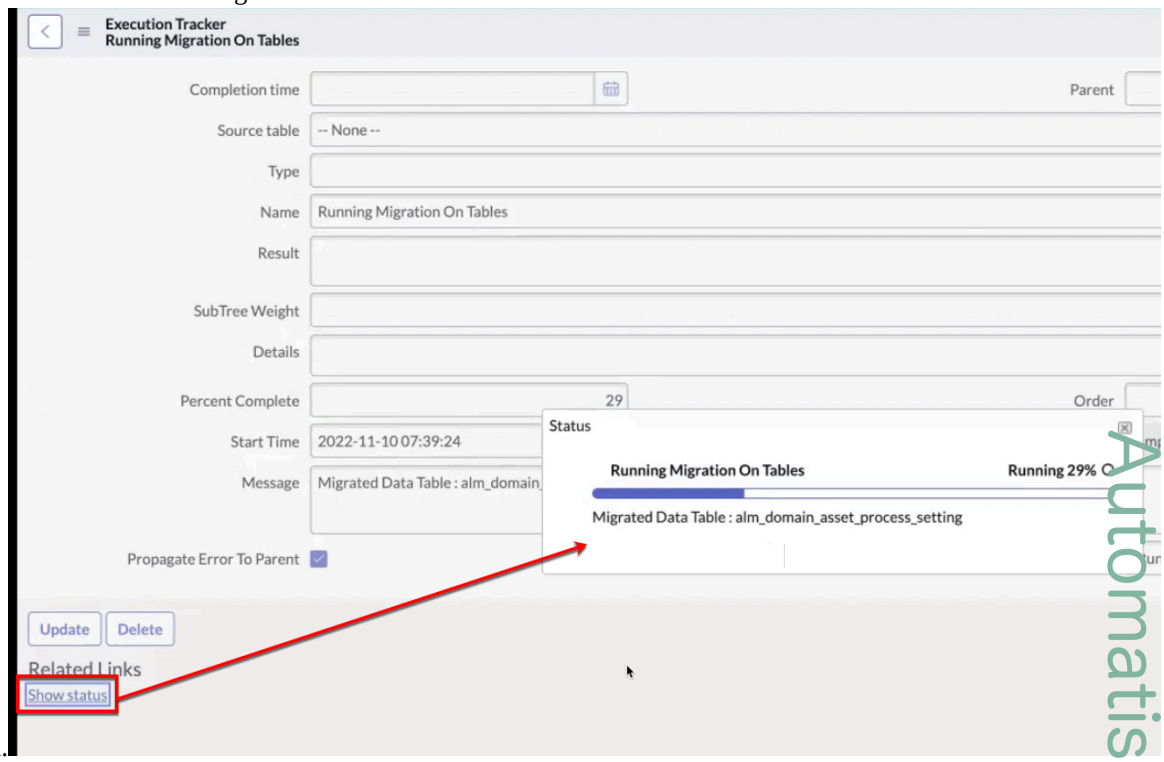


Sie können auch auf die Tabelle `sys_execution_tracker` zugreifen und nach **Running Migration on Tables** suchen, um den im Hintergrund ausgeführten Migrationsprozess zu überprüfen.

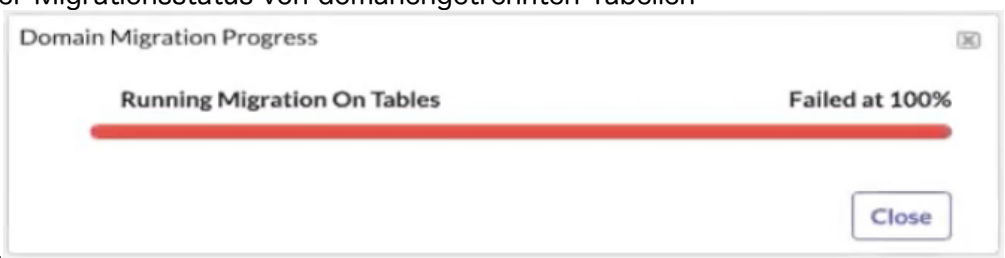
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

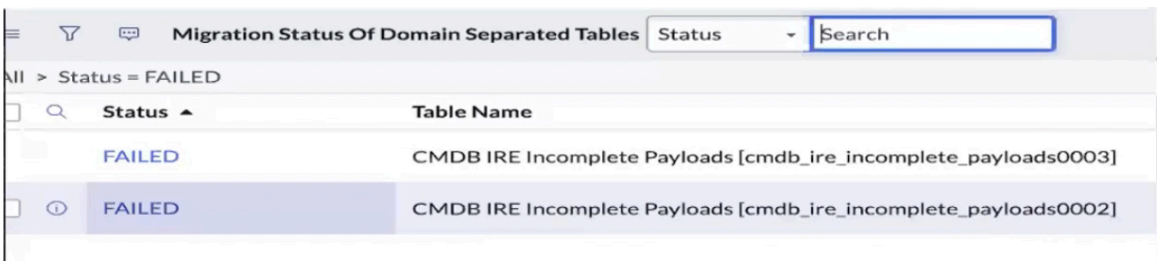
13. Wählen Sie **Status** anzeigen im Abschnitt „Zugehörige Links“ aus, um jederzeit während der Migration auf den Fortschrittsbalken zuzugreifen.



Wenn eine Tabelle die Schemaprüfung nicht bestanden hat, lautet der Gesamtstatus der Migrationsstatus von domänengetrennten Tabellen **Fehlgeschlagen**.



Für jede entsprechende Tabelle gibt es **Fehlgeschlagene** Einträge.

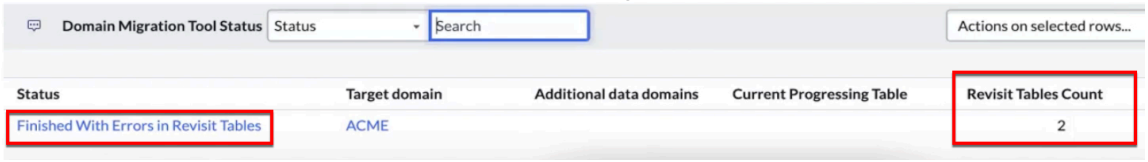


Der Rest der Migration wird fortgesetzt, und eine Zusammenfassung aller fehlgeschlagenen Tabellen und die Gesamtzahl der Anzahl der

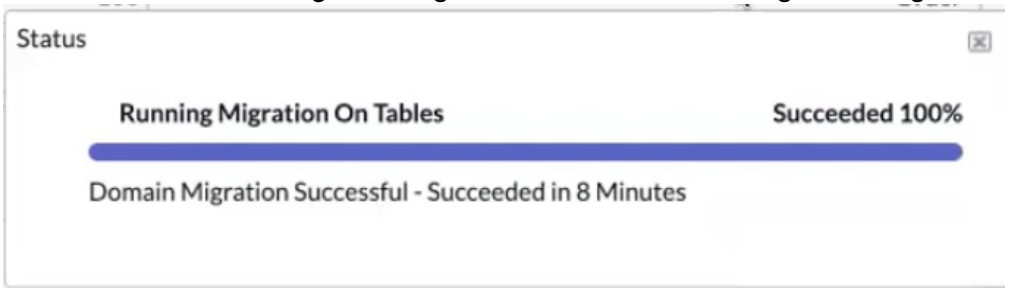
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erneuten Aufruftabellen werden im Status des Domänenmigrationstools ausgefüllt.



Der **Status** lautet **„Erfolgreich** abgeschlossen“, wenn die Migration abgeschlossen ist.



Prozessverwaltung

Mit der Prozessverwaltung können Administratoren domänenspezifische Richtlinien festlegen.

Die Richtlinien, die in der Domänenhierarchie weiter unten festgelegt sind, überschreiben Richtlinien, die in der Domänenhierarchie weiter oben festgelegt sind. Während sie sich in einer Domäne befinden, können Administratoren domänenspezifische Versionen dieser globalen Richtlinien und Einstellungen festlegen:

- Clientskripts
- Systemrichtlinien
- Anwendungs- und Modulnamen
- Anwendungsrollen
- Modulfilter

⚠ Warnung:
Alle Benutzer mit der Administratorrolle haben speziellen Zugriff auf alle Systemfeatures, -funktionen und -daten, da Administratoren ACL-Regeln überschreiben und alle Rollenprüfungen bestehen können. Gewähren Sie diese Berechtigung mit Bedacht.

Wenn Benutzer über die **Administratorrolle** verfügen, stehen ihnen alle Richtlinien in der Instanz unabhängig von der zugewiesenen Domäne zur Verfügung. Sie können eine bestimmte Domäne eingeben, und dann sind nur Richtlinien in dieser Domäne oder höher sichtbar und werden während einer relevanten Transaktion verarbeitet. Wenn ein Administrator eine Richtlinie ändert, die sich in einer höheren Domäne oder der globalen Domäne befindet, erstellt das System automatisch einen neuen Datensatz für die aktuelle Domäne dieses Administrators. Der ursprüngliche Richtlinien-, Anwendungs- oder Moduldatensatz wird nicht geändert. Dieser neue Datensatz überschreibt den ursprünglichen.

Um Änderungen an einer Richtlinie in einer untergeordneten Domäne vorzunehmen, wechseln Sie in diese Domäne, und ändern Sie die Richtlinie. Dieser Ansatz erstellt den Richtliniendatensatz in Ihrer Domäne, der den ursprünglichen, übergeordneten Richtliniendatensatz überschreibt.

Ändern Sie nicht die übergeordnete Richtlinie, und ändern Sie dann das Feld **Domäne** in dieser Richtlinie. Bei diesem Ansatz wird weder ein Richtliniendatensatz in Ihrer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

untergeordneten Domäne erstellt, noch wird der Richtliniendatensatz für die übergeordnete Domäne beibehalten.

Das Feld **sys_overrides** gibt an, dass eine Richtlinie, Anwendung oder ein Modul auf einer niedrigeren Ebene in der Hierarchie einen Datensatz auf einer höheren Ebene überschreibt. Das System legt dieses Feld automatisch fest, wenn ein Administrator versucht, eine Richtlinie, Anwendung oder ein Modul zu ändern, die zu einer anderen Domäne weiter oben in der Hierarchie gehört.

Anstatt den übergeordneten Datensatz zu ändern, wird die versuchte Aktualisierung in eine Einfügung geändert, und das Feld **sys_overrides** wird so festgelegt, dass es die überschriebene Richtlinie, Anwendung oder das übergeordnete Modul angibt. Später, wenn die Datensätze für eine relevante Transaktion geladen werden, wird die überschreibende domänenspezifische Richtlinie, Anwendung oder das überschreibende Modul anstelle der ursprünglichen verwendet.

Domänen für die Prozessverwaltung

Standardmäßig verwendet die Prozessverwaltung immer die Domäne des Datensatzes, um zu bestimmen, welche Richtlinien angewendet werden sollen.

Die Domäne des Datensatzes hat Vorrang vor der Domäne des Benutzers. Wenn in der Domäne des Datensatzes keine Richtlinien vorhanden sind, sucht die delegierte Administration nach Richtlinien in der nächsthöheren Ebene der Domänenhierarchie. Die Suche nach Domänenrichtlinien wird in der Domänenhierarchie fortgesetzt, bis die globale Domäne erreicht ist. Wenn in der Domänenhierarchie keine Domänenrichtlinien vorhanden sind, verwendet die Prozessverwaltung die Richtlinien für die globale Domäne.

Zum Beispiel ist Fred Luddy ein Benutzer in der Acme-Domäne, der Datensätze in den untergeordneten Domänen von Acme: Atlanta, Acme: San Diego und Acme: NY anzeigen kann. Wenn dieser Benutzer einen Datensatz in der Domäne Acme: San Diego öffnet, sucht die Prozessverwaltung zuerst nach Richtlinien in der Domäne Acme: San Diego. Wenn auf dieser Ebene der Domänenhierarchie keine Richtlinien vorhanden sind, sucht die Prozessverwaltung nach Richtlinien aus der Acme-Domäne. Wenn in der Acme-Domäne keine Richtlinien vorhanden sind, verwendet die Prozessverwaltung die globalen Domänenrichtlinien, da in der Domänenhierarchie keine anderen Domänen höher sind.

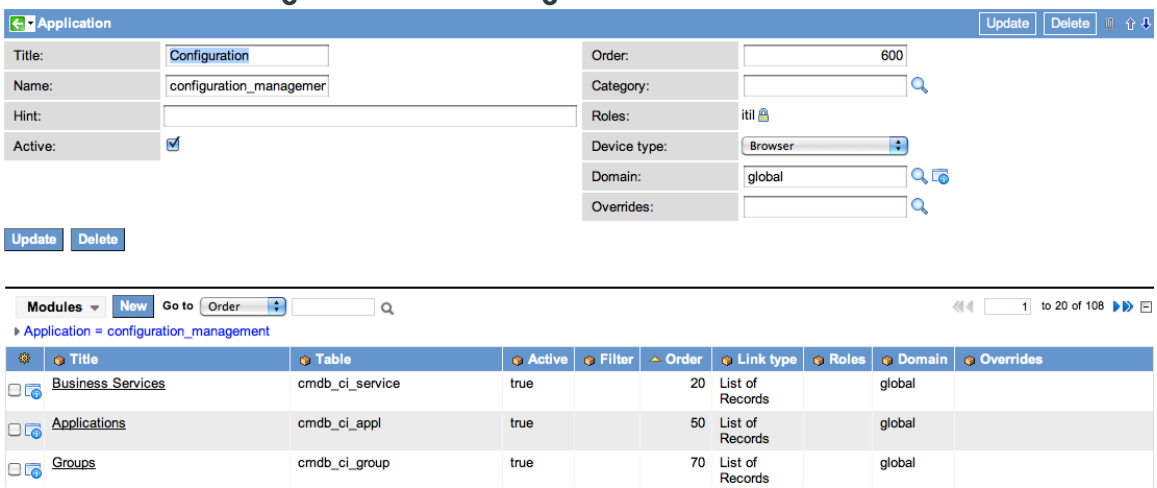
Beispielprozessverwaltung mit domänenspezifischen Anwendungen

Das folgende Beispiel veranschaulicht die Prozessverwaltung mit domänenspezifischen Anwendungen und Modulen.

Als Administrator der Domäne „Oceanic“ beschließt David Loo, die Konfigurationsanwendung anzupassen. Zunächst überprüft David die Module, die im Konfigurationsanwendungsmodul verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Startansicht der Konfigurationsanwendung



David beschließt, die Konfigurationsanwendung in CMDB umzubenennen und der Rolle „inventory_admin“ die Anwendung zu erlauben.

Beispiele für domänenspezifische Änderungen an der Konfigurationsanwendung

Applications | New | Go to Title | 1 to 20 of 46

All > Active = true > Device type != Mobile

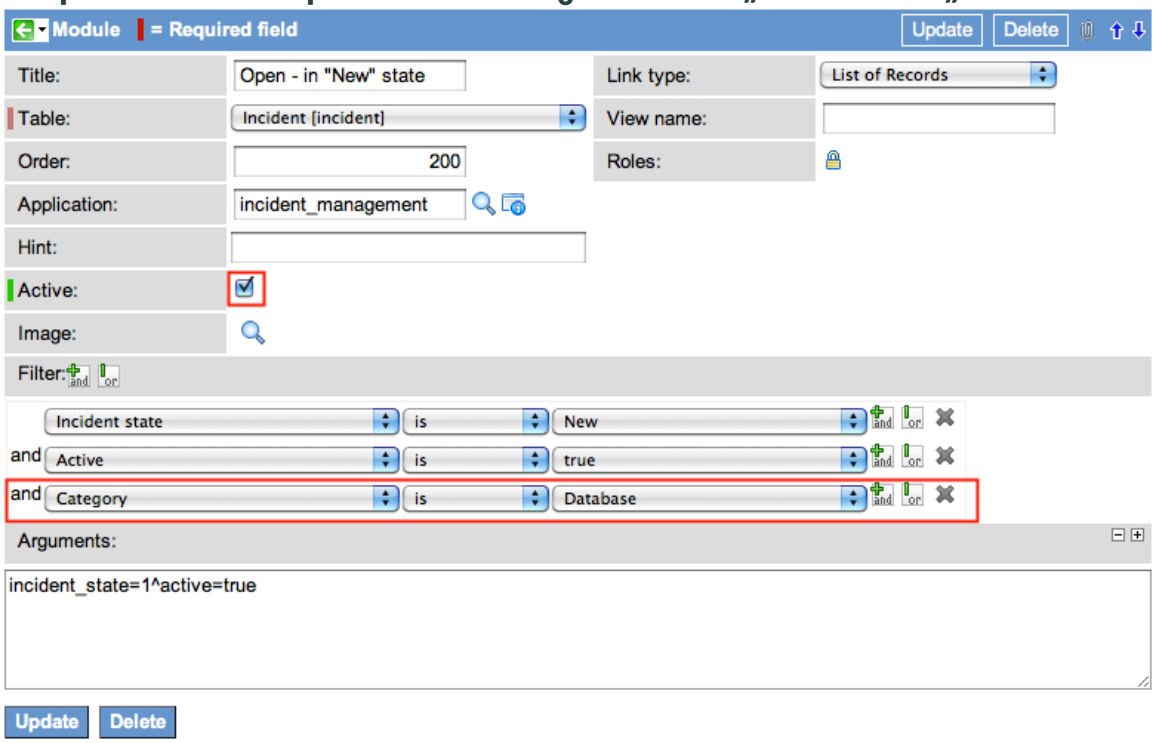
Title	Active	Order	Roles	Name	Domain	Overrides
Asset Management	true	900	asset	asset	global	
BSM Map	true		admin itil	bsm_map	global	
Change	true	400	itil	change_management	global	
CMDB	true	600	itil inventory_admin	configuration_management	Database	configuration_management
Content Management	true		content_admin	cms	global	
Contract Management	true	1,000	asset contract_manager	asset_contracts	global	
Domain Admin	true		domain_admin	domain_admin	global	
ECC	true		admin	ecc	global	
Homepage Admin	true		admin	home	global	
Incident	true	200	itil	incident_management	global	
Instance Clone	true		clone_admin	instance_clone	global	
Knowledge Base	true	800	knowledge	km	global	
Metrics	true		itil_admin metric_admin	metrics	global	
MID Server	true		admin	MID	global	
Organization Management	true	875	asset	organization_management	global	
Problem	true	300	itil	problem_management	global	
Reports	true	1,100	itil	reports	global	
SAML 2 Single Sign-on	true		admin	saml_2_single_sign_on	global	
SAML Single Sign-on	true		admin	SAML Single Sign-on	global	

Activate | Deactivate | Actions on selected rows... | 1 to 20 of 46

Als Nächstes beschließt David, die Incident-Anwendung zu ändern, indem er das Modul **„Offen – in Status „Neu““** aktiviert und ein neues Filterelement hinzufügt, um offene Incidents in der Kategorie „Ozean“ anzuzeigen.

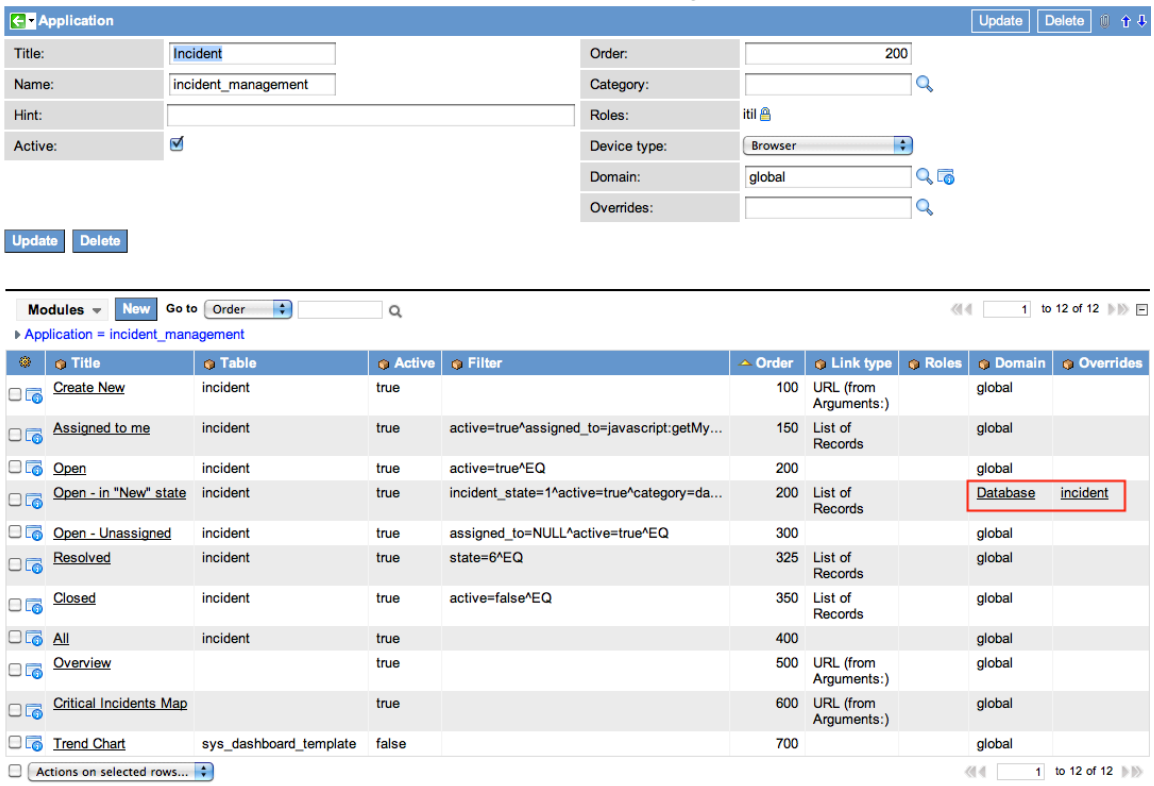
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für domänenspezifische Änderungen am Modul „Offen – Status „Neu"".



Dadurch wird ein neuer Moduleintrag in der Anwendung erstellt, anstatt das vorhandene Modul in der globalen Domäne zu überschreiben.

Domänenspezifische Ansicht der Incident-Anwendung

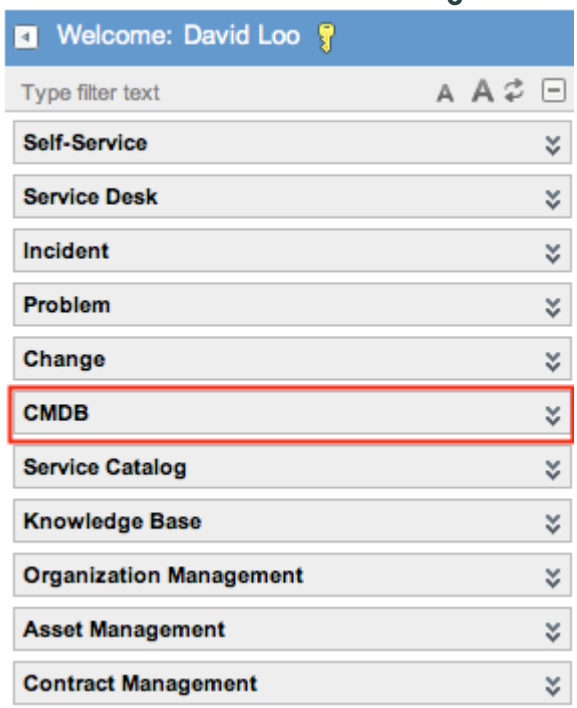


Wenn sich ein anderer Administrator aus einer anderen Domäne, z. B. Fred Luddy, anmeldet und die Konfigurationsanwendung betrachtet, werden die Einstellungen aus der globalen Domäne angezeigt.

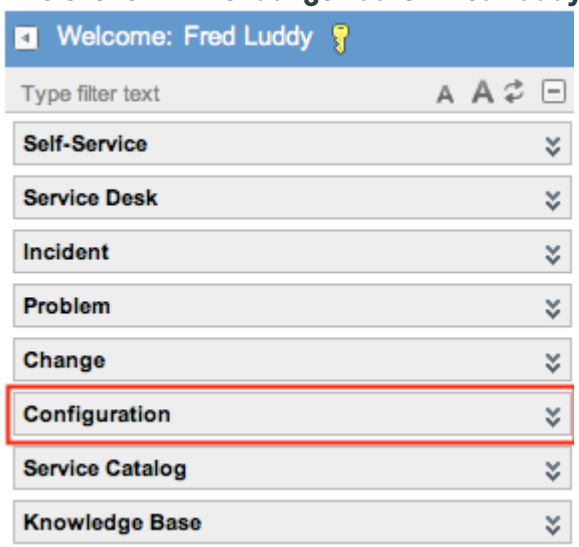
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

David Loos Ansicht der Anwendungen



Ansicht von Anwendungen durch Fred Luddy



Aktivieren Sie die ausführliche Domänenprotokollierung und Debug-Nachrichten

Domänenprotokoll- und Debug-Meldungen ermöglichen die Behebung von Domänenkonfigurationsfehlern.

Vorbereitungen

Erforderliche Rolle: admin

Stellen Sie sicher, dass Sie die neueste Instanz sind, um die beste Leistung zu erzielen.

Prozedur

1. Navigieren Sie im Domain Separation Center zu **Domänenadministrator**.
2. Klicken Sie **auf Domänencenter konfigurieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Aktivieren Sie für **Ausführliche Domänenprotokollierung aktivieren**das Kontrollkästchen **Ja**.
4. Klicken Sie auf **Aktualisieren**.

Zeigen Sie eine Echtzeit-Domänennachricht an

Sie können Echtzeit-Domänenmeldungen aus den Systemprotokollen anzeigen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Ausführliche Domänenprotokollierung aktivieren: Navigieren Sie zu **Alle** > **Domänenadministrator** > **Domain Separation Center** > **Domänencenter konfigurieren** > **Aktiviert die Protokollierung der Detaildomäne** > **Ja** (oder legen Sie die Eigenschaft glide.sys.domain.verbose auf **True**fest).
2. Navigieren zu **Systemdiagnostik** > **Sitzung debuggen** > **Alle aktivieren**.
   Da es sich um eine Echtzeitüberprüfung handelt, muss die Debug-Sitzung nicht ausgeführt werden, bevor die Protokolldateien überprüft werden.
3. Navigieren Sie zur Sitzungs-Debug-Konsole, um die detaillierten Systemdomänenprotokolle anzuzeigen.
4. Suchen Sie nach dem Text Abfrage für Tabelle.

   Diese Abfrage findet Protokollnachrichten in diesem Format:

```
08:36:43.974: [Domain Paths] Query against table incident restricted by domain values
 [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
Database[287ee6fea9fe198100ada7950d0b1b73],
Database San Diego[db53a9290a0a0a650091abebccf833c6], global, NY
 DB[5f74727dc0a8010e01efe33a251993f9]]
```

   In diesem Beispiel hat der Benutzer, der die Incident-Tabelle angezeigt hat, nur Datensätze gesehen, die den DB-Domänen „Database Atlanta“, „Database“, „Database San Diego“, „global“ und „NY“ entsprechen.

Zeigen Sie eine historische Domänennachricht an

Zeigen Sie historische Domänenmeldungen in der -Protokolldatei an, um Probleme bei der Domänentrennung zu beheben.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Ausführliche Domänenprotokollierung aktivieren: Navigieren Sie zu **Alle** > **Domänenadministrator** > **Domain Separation Center** > **Domänencenter konfigurieren** > **Aktiviert die Protokollierung der Detaildomäne** > **Ja** (oder legen Sie die Eigenschaft glide.sys.domain.verbose auf **True**fest).
2. Navigieren zu **Systemdiagnostik** > **Sitzung debuggen** > **Alle aktivieren**.
3. Lassen Sie die Debug-Sitzung für einen bestimmten Zeitraum laufen, z. B. einen Tag, bevor Sie die Protokolldateien überprüfen.
4. Navigieren zu **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**.
5. Öffnen Sie den Datensatz für den Tag, den Sie anzeigen möchten.
   Protokolldateien verwenden das Benennungsformat localhost_log.<yyyy-mm-dd> .txt .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf den zugehörigen Link Protokoll **herunterladen**.
7. Öffnen Sie die heruntergeladene Protokolldatei in einem Texteditor, und suchen Sie nach Protokollnachrichten mit dem folgenden Format:

   Durch Domänenwerte eingeschränkte Tabellen-Incidents abfragen [global, Software[8a4dde73c6112278017a6a4baf547aa7]]

   In diesem Beispiel hat ein Benutzer nur Datensätze aus der Incident-Tabelle gesehen, die den globalen Domänen und den Softwaredomänen entsprechen.

Beheben Sie Fehler bei der Domänentrennung

Wenn Probleme bei der Domänentrennung auftreten, überprüfen Sie diese Liste der Lösungen.

Fehler oder Symptom	Lösung
Eine Domänen-sys_id verweist auf eine nicht vorhandene Domäne	Dieser Fehler tritt auf, wenn ein Datensatz, z. B. ein Benutzer- oder Aufgabendatensatz, einen sys_domain- Spaltenwert hat, dessen sys_id in der aktuellen Domänentabelle nicht vorhanden ist. Die Domänen -sys_id wurde möglicherweise versehentlich gelöscht, oder sie verweist auf eine vorherige Domänentabelle, wenn Sie die Domänentabelle geändert haben. Um den Fehler zu beheben, öffnen Sie eine Liste für die Tabelle, die den Fehler enthält, und filtern Sie nach dem ungültigen sys_domain-Wert. Geben Sie dann entweder manuell den korrekten sys_domain-Wert ein, oder entfernen Sie ihn. **Hinweis:** Sie können ungültige Domänen -sys_ids in jeder Tabelle haben, die auf die Domänentabelle verweist. Beispielsweise können ungültige Domänen-IDs in den Tabellen „Benutzersichtbarkeitsdomäne “ [sys_user_visibility], „Gruppensichtbarkeitsdomäne “ [sys_user_group_visibility]und „Enthaltene Domäne “ [domain_contains] auftreten.
Ein Domänenpfad oder eine sys_id einer Domänennummer verweist auf die falsche Domäne	Dieser Fehler tritt auf, wenn eine Domänennummer oder eine Domänenpfadabfrage nicht mit dem tatsächlichen Domänennamen synchronisiert ist. Dieser Fehler kann bei Domänennummern auftreten, wenn das Hinzufügen von Domänen eine Neunummerierung erfordert oder während der Konvertierung von Domänennummern in Domänenpfade. Um den Fehler zu beheben, überprüfen Sie die Ergebnisse in Domain Separation Center. Wenn der Fehler weiterhin besteht, können Sie den Wert für die Spalten sys_domain_path oder sys_domain_number manuell so bearbeiten, dass er auf die richtige Domäne verweist.
Die Domänenstruktur ist beschädigt	Dieser Fehler tritt auf, wenn eine Reihe von Domänen enthält-Beziehungen eine Endlosschleife zwischen Domänen erstellt. Um den Fehler zu beheben, öffnen Sie eine Liste für die Domänentabelle, und bearbeiten Sie die Werte der Domäne manuell so, dass keine Schleife entsteht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

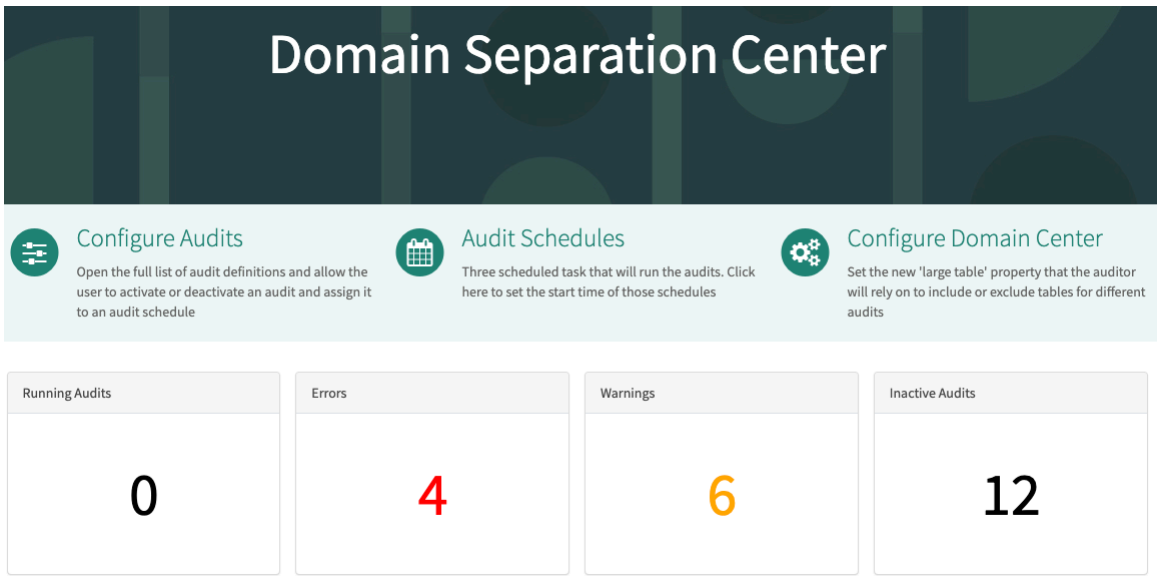
Domain Separation Center

Auditieren Sie Ihre Domänen regelmäßig, um Probleme aufzudecken.

Übersicht

Das Domain Separation Center ist ein Dashboard, in dem Sie Audits für alle in der Tabelle „domain_audit_definition“ gespeicherten Domänen planen und konfigurieren können. Mit dem Dashboard können Sie Audit-Ergebnisse überprüfen und sich eingehender mit Domänenfehlern und Warnungen befassen. Sie finden das Dashboard „Domain Separation Center“ unter<ServiceNow-instance-name> /domaincenter

Das Domain Separation Center bietet viele Audits. Sie können keine eigenen erstellen. Sie können jedoch konfigurieren, wie oft sie ausgeführt werden. Audits werden für alle in der Tabelle „domain_audit_definition“ gespeicherten Domänen ausgeführt.



Konfigurieren Sie Audits

Sie können konfigurieren, ob ein Audit aktiv ist und wie häufig es ausgeführt wird.

1. Wählen Sie im **Domänentrennungscenter Konfigurieren von Audits**aus.

   Die Seite „ **Audits konfigurieren** “ wird angezeigt.

2. Konfigurieren Sie jedes Audit, das aktiv sein soll. Audits sind standardmäßig inaktiv.
   a. Wählen Sie ein Audit aus.
   b. Aktivieren Sie das Kontrollkästchen **Aktiv**, um das Audit zu aktivieren.
   c. Geben Sie im Feld **Häufigkeit** an, wie oft das Audit ausgeführt wird.

      Das Domain Separation Center führt alle Audits, die mit derselben Häufigkeit markiert sind, gleichzeitig aus. Wählen Sie nicht **Täglich** für Audits aus, die für große Tabellen ausgeführt werden.

   d. Wiederholen Sie diese Schritte für jedes Audit, das Sie aktivieren möchten.
3. Wählen Sie **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditzeitpläne

Konfigurieren Sie ein oder mehrere Audits für die tägliche, wöchentliche oder monatliche Ausführung. Der Planer gibt an, an welchen Tagen und zu welchen Zeiten diese Audits ausgeführt werden sollen. Alle Audits mit derselben Planungshäufigkeit werden nacheinander ausgeführt, beginnend mit dem von Ihnen konfigurierten Zeitpunkt.

1. Wählen Sie im Domain Separation Center **Auditzeitpläne**aus.

   Die Seite „ **Auditzeitplan** “ wird angezeigt.

2. Konfigurieren Sie die Auditzeitpläne.
   a. Wählen Sie einen Zeitplannamen aus.
   b. Geben Sie die Uhrzeit an, zu der das Audit ausgeführt werden soll.

      Zeiteinheiten werden im 24-Stunden-Format gemessen, d. h. 14 Uhr ist 14:00 Uhr.

   c. Wählen Sie für wöchentliche Zeitpläne den Wochentag aus, an dem das Audit ausgeführt werden soll, wobei 1 Sonntag ist.
   d. Wählen Sie für monatliche Zeitpläne den Tag des Monats aus, an dem das Audit ausgeführt werden soll.
   e. Wiederholen Sie das Verfahren für die anderen Zeitpläne.
3. Wählen **Sie Speichern** aus, um die Konfigurationsänderungen zu speichern.
4. Wählen Sie **Jetzt** ausführen aus, um alle geplanten Audits in der Häufigkeit auszuführen, die oben im rechten Bereich angezeigt wird. Wenn der Titel des Bereichs beispielsweise **Domänenauditzeitplan – Täglich**lautet, werden alle täglich ausgeführten Audits ausgeführt.

Um den Status eines laufenden Audits anzuzeigen, wählen Sie im Domänentrennungscenter die Nummer im Feld **Laufende Audits** aus.

Führen Sie Audits sofort aus

Audits werden in der Regel wie geplant ausgeführt. Sie können jedoch alle Audits mit dem Befehl ausführen.

1. Wählen Sie im Domain Separation Center **Auditzeitpläne**aus.

   Die Seite „ **Auditzeitplan** “ wird angezeigt.

2. Wählen Sie den Namen des Auditzeitplans aus, den Sie ausführen möchten, z. B. täglich, wöchentlich oder monatlich.
3. Wählen Sie **Jetzt ausführen**.

Um den Status eines laufenden Audits anzuzeigen, wählen Sie im Domänentrennungscenter die Nummer im Feld **Laufende Audits** aus.

Konfigurieren Sie das Domänentrennungszentrum

1. Wählen Sie im Domänentrennungscenter **Konfigurieren Domänencenter**aus.
2. Wählen Sie auf der Seite **„Configure Domain Center** “ (Domänencenter konfigurieren) für **Aktiviert die detaillierte Domänenprotokollierung**die Option **Ja**, um detaillierte Protokolle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu speichern, die bei der Diagnose von domänenbezogenen Problemen helfen. Eine detaillierte Protokollierung kann zu Leistungsproblemen führen.

Diese Protokolle beziehen sich auf serverseitige Protokolle in der Tabelle „syslog_domain“. Weitere Informationen zum Anzeigen der Protokolle finden Sie unter Audits mit Warnungen und Fehlern anzeigen.

3. Wählen Sie im Slushbucket alle großen Tabellen aus, und verschieben Sie sie in die Spalte **Ausgewählt**.

   Tägliche Audits sollten nicht für große Tabellen ausgeführt werden. Ausgegraute Tabellennamen in der Spalte „ **Ausgewählt** “ sind groß und können nicht in die Spalte „ **Verfügbar** “ verschoben werden.

4. Wählen Sie **Aktualisieren**.

Audits mit Warnungen und Fehlern anzeigen

Im -Dashboard enthalten **Fehler** und **Warnungen** detaillierte Informationen zu Audits, bei denen Probleme aufgetreten sind. Protokolle im Zusammenhang mit der Domänentrennung befinden sich auf Ihrem Server in der Tabelle syslog_domain.

1. Wählen Sie im Domain Separation Center die Nummer im Feld **Fehler** oder **Warnungen** aus.

   Die Seite „ **Fehler** “ bzw. „ **Warnungen** “ wird angezeigt.

2. Wählen Sie eines der Audits in der Liste aus.

   Auf der Seite werden detaillierte Informationen zu Problemen mit dem von Ihnen ausgewählten Audit angezeigt. Die Nachrichten in **Audit-Ergebnisdetails** beziehen sich auf Werte in der Tabelle „syslog_domain“ für Tabellen-Audits, die Fehler oder Warnungen aufgedeckt haben.

3. So zeigen Sie die Protokolle auf dem Server an, die Informationen zu Warnungs- oder Fehleraudits enthalten:
   a. Kopieren Sie den Wert **Detail-ID** im linken Bereich einer Warnung oder eines Fehlers.
   b. Geben Sie im Filternavigator von HI *`syslog_domain.do`*ein.

      Die Seite Domänenprotokoll wird angezeigt.

   c. Geben Sie im Suchfeld **Quelle**= ein<Detail-ID> (kein Leerzeichen nach dem Gleichheitszeichen), z. B. =f6a00fd29a85b300a9503a81b9169678.

      Auf der Seite „Domänenprotokoll“ werden nur die Protokolle angezeigt, die sich auf das Audit mit der von Ihnen angegebenen Detail-ID beziehen. Jede Zeile in der Tabelle gibt einen anderen Datensatz an, in dem beim Audit Probleme gefunden wurden. Beachten Sie, dass das Feld **Nachricht** auf dieser Seite mit den Werten übereinstimmt, die in der Spalte **Nachricht** des Domain Service Center angezeigt werden. Das Format der Nachricht entspricht dem Audit-Typ.

4. Wählen Sie Folgendes aus:
   - **Audit**erneut ausführen: Führen Sie ein Audit erneut aus, um festzustellen, ob weiterhin eine Warnung oder ein Fehler auftritt.
   - **Audit deaktivieren**: Deaktiviert ein Audit.
   - **Details**kopieren: Audit-Details in die Zwischenablage kopieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie laufende und ausstehende Audits an

Aktive Audits werden regelmäßig ausgeführt oder in die Warteschlange gestellt, um sie wie geplant auszuführen. Sie können ihren Status anzeigen, während sie ausgeführt werden.

1. Wählen Sie die Zahl im Feld **Audits** aus, um Audits anzuzeigen, die derzeit ausgeführt werden oder deren Ausführung aussteht.

   Die Seite „ **Laufende Audits** “ wird angezeigt.

2. Wählen Sie ein Audit aus, um weitere Informationen dazu zu erhalten.

Zeigen Sie inaktive Audits an

1. Wählen Sie die Nummer im Feld **Inaktive Audits** aus.

   Auf der Seite „ **Inaktive Audits** “ werden alle derzeit deaktivierten Audits angezeigt.

2. Wählen Sie eines der Audits aus, um weitere Informationen dazu anzuzeigen.
3. Um ein Audit zu aktivieren, aktivieren Sie das **Kontrollkästchen Aktiv**, und geben Sie im Feld **Häufigkeit** an, wie oft das Audit ausgeführt wird.
4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie das Domänentrennungszentrum

Geben Sie an, welche Tabellen in Domänen groß sind und ob Sie eine detaillierte Protokollierung wünschen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Audits so planen, dass sie täglich, wöchentlich oder monatlich ausgeführt werden. Audits, die für große Tabellen ausgeführt werden, können sehr lange dauern. Vermeiden Sie es daher, Audits für große Tabellen täglich auszuführen. Das Starten eines neuen Audits für ein Audit, dessen Ausführung mehr als einen Tag dauert, kann negative Auswirkungen haben.

Eine detaillierte Protokollierung bietet bessere Einblicke in Probleme, die bei Audits gefunden wurden, kann jedoch zu Leistungsproblemen führen.

Prozedur

1. Wählen Sie im Domänentrennungscenter **Konfigurieren Domänencenter**aus.
   Die Seite Domänencenter konfigurieren wird angezeigt.
2. Wählen Sie **Ja** für **Aktiviert die detaillierte Domänenprotokollierung**aus, um detaillierte Protokolle zu speichern, die bei der Diagnose von domänenbezogenen Problemen helfen.
   Diese Protokolle beziehen sich auf serverseitige Protokolle in der Tabelle „Domänenprotokoll“ [syslog_domain]. Weitere Informationen zum Anzeigen der Protokolle finden Sie im Abschnitt Audits mit Warnungen und Fehlern anzeigen.
3. Verschieben Sie in der Liste alle großen Tabellen in die Spalte **Ausgewählt**.
   Tägliche Audits sollten nicht für große Tabellen ausgeführt werden. Ausgegraute Tabellennamen in der Spalte „ **Ausgewählt** “ sind groß und können nicht in die Spalte „ **Verfügbar** “ verschoben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Aktualisieren**.
5. Wenn Sie große Tabellen haben, die niemals geprüft werden sollten, legen Sie die Systemeigenschaft `com.glide.domain.audit.big_tables.additional` auf eine durch Kommas getrennte Liste dieser Tabellennamen fest.

Konfigurieren Sie Audits

Konfigurieren Sie, ob ein Audit aktiv ist und wie häufig es ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Klicken Sie im Domain Separation Center auf **Audits konfigurieren**.
   T wird angezeigt.
2. Konfigurieren Sie auf der Seite „Audits konfigurieren“ jedes Audit, das aktiv sein soll.
   Audits sind standardmäßig inaktiv.
   a. Klicken Sie auf ein Audit.
   b. Klicken Sie auf das Kontrollkästchen **Aktiv**, um das Audit zu aktivieren.
   c. Geben Sie im Feld **Häufigkeit** an, wie oft das Audit ausgeführt wird.
   Das Domain Separation Center führt alle Audits, die mit derselben Häufigkeit markiert sind, gleichzeitig aus. Wählen Sie nicht **Täglich** für Audits aus, die für große Tabellen ausgeführt werden.
   d. Wiederholen Sie die Schritte a bis c für jedes Audit, das Sie aktivieren möchten.
3. Klicken Sie auf **Speichern**.

Planen Sie Audits

Geben Sie die Uhrzeit und den Tag an, zu denen Audits ausgeführt werden.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Sie haben mindestens ein Audit so konfiguriert, dass es täglich, wöchentlich oder monatlich ausgeführt wird. Der Planer gibt an, an welchen Tagen und zu welchen Zeiten diese Audits ausgeführt werden sollen. Alle Audits mit derselben Planungshäufigkeit werden nacheinander ausgeführt, beginnend mit dem von Ihnen konfigurierten Zeitpunkt.

Prozedur

1. Klicken Sie im Domain Separation Center auf **Auditzeitpläne**.
   Die Seite „Auditzeitplan“ wird angezeigt.
2. Konfigurieren Sie die Auditzeitpläne.
   a. Klicken Sie auf einen Zeitplannamen.
   b. Geben Sie die Uhrzeit an, zu der das Audit ausgeführt werden soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeiteinheiten verwenden das 24-Stunden-Format (d. h. 14 ist 14 Uhr).

c. Wählen Sie für wöchentliche Zeitpläne den Wochentag aus, an dem das Audit ausgeführt werden soll, wobei 1 Sonntag ist.

d. Wählen Sie für monatliche Zeitpläne den Tag des Monats aus, an dem das Audit ausgeführt werden soll.

e. Wiederholen Sie das Verfahren für die anderen Zeitpläne.

3. Klicken Sie auf **Speichern**, um die Konfigurationsänderungen zu speichern.
4. **Wahlweise:** Klicken Sie auf **Jetzt** ausführen, um alle geplanten Audits in der oben im rechten Bereich angezeigten Häufigkeit auszuführen.
   Beispiel: Wenn der Titel des **Bereichs Domänenauditzeitplan – Täglich**lautet, werden mit **Jetzt** ausführen sofort alle Audits ausgeführt, deren tägliche Ausführung geplant ist.

Nächste Maßnahme
Um den Status eines laufenden Audits anzuzeigen, klicken Sie im Domain Separation Center auf die Zahl im Feld **Laufende Audits**.

Führen Sie Audits sofort aus

Audits werden in der Regel wie geplant ausgeführt. Sie können jedoch alle Audits mit dem Befehl ausführen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können einzelne Audits nicht manuell ausführen. Sie können jedoch alle Audits ausführen, die mit derselben Planungshäufigkeit konfiguriert sind. Sie können beispielsweise alle Audits ausführen, die für die tägliche Ausführung konfiguriert sind.

Prozedur

1. Klicken Sie im Domain Separation Center auf **Auditzeitpläne**.
2. Klicken Sie auf den Namen des Auditzeitplans, den Sie ausführen möchten (z. B. täglich, wöchentlich oder monatlich).
3. Klicken Sie auf **Jetzt ausführen**.

Nächste Maßnahme
Um den Status eines laufenden Audits anzuzeigen, klicken Sie im Domain Separation Center auf die Zahl im Feld **Laufende Audits**.

Audits mit Warnungen und Fehlern anzeigen

Das Domain Separation Center enthält Details zu Audit-Fehlern und -Warnungen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Im Dashboard „Domain Separation Center“ bieten **Fehler** und **Warnungen** detaillierte Informationen zu Audits, bei denen Probleme aufgetreten sind. Protokolle im Zusammenhang mit der Domänentrennung befinden sich auf Ihrem Server in der Tabelle syslog_domain. Fehler sind Probleme, die sofortige Aufmerksamkeit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erfordern. Warnungen führen nicht zu Fehlern, sondern stellen Best Practices dar, z. B. den Domänennamen nicht zu lang zu machen.

Prozedur

1. Klicken Sie im Domain Separation Center auf die Zahl im Feld **Fehler** oder **Warnungen**.
   Die Seite „ **Fehler** oder **Warnungen** “ wird angezeigt.
2. Klicken Sie auf eines der Audits in der Liste.
   Auf der Seite werden detaillierte Informationen zu Problemen mit dem von Ihnen ausgewählten Audit angezeigt. Die Nachrichten in **Audit-Ergebnisdetails** beziehen sich auf Werte in der Tabelle „syslog_domain“ auf dem Server für Tabellen-Audits, die Fehler oder Warnungen aufgedeckt haben.
3. So zeigen Sie die Protokolle auf dem Server an, die Informationen zu Warnungs- oder Fehleraudits enthalten:

   a. Kopieren Sie den Wert **Detail-ID** im linken Bereich einer Warnung oder eines Fehlers.

   b. Geben Sie in der Instanz, auf der das Domain Separation Center ausgeführt wird, im **Filternavigator**`syslog_domain.list`ein.
   Die Seite Domänenprotokoll wird angezeigt.

   c. Geben Sie im Suchfeld der Spalte **Quelle**= ein<Detail-ID> (kein Leerzeichen nach dem Gleichheitszeichen), z. B. `=f6a00fd29a85b300a9503a81b9169678`.
   Auf der Seite „Domänenprotokoll“ werden nur die Protokolle angezeigt, die sich auf das Audit mit der von Ihnen angegebenen Detail-ID beziehen. Jede Zeile in der Tabelle gibt einen anderen Datensatz an, in dem beim Audit Probleme gefunden wurden. Beachten Sie, dass das Feld **Nachricht** auf dieser Seite mit den Werten übereinstimmt, die in der Spalte **Nachricht** des Domain Service Center angezeigt werden. Die in der Nachricht enthaltenen Informationen stimmen mit dem Audit-Typ überein.

4. **Wahlweise:** Wählen Sie eine der folgenden Optionen aus:
   - **Audit** erneut ausführen – Führen Sie ein Audit erneut aus, um festzustellen, ob weiterhin eine Warnung oder ein Fehler auftritt.
   - **Audit deaktivieren – Deaktiviert** ein Audit.
   - **Details** kopieren: Kopiert Audit-Details in die Zwischenablage.

Laufende und ausstehende Ergebnisse anzeigen

Sie können laufende und ausstehende Audits anzeigen, um deren Status anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Aktive Audits werden regelmäßig ausgeführt oder in die Warteschlange gestellt, um sie wie geplant auszuführen. Sie können ihren Status anzeigen, während sie ausgeführt werden.

Prozedur

1. Klicken Sie auf die Zahl im Feld **Audits** wird ausgeführt, um Audits anzuzeigen, die derzeit ausgeführt werden oder deren Ausführung aussteht.
   Die Seite „Ausgeführte Audits“ wird angezeigt.
2. Klicken Sie auf ein laufendes oder ausstehendes Audit, um Informationen dazu anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie inaktive Audits an

Sie können alle inaktiven Audits an einem Ort anzeigen und optional aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Klicken Sie auf die Zahl im Feld **Inaktive Audits**.
   Auf der Seite „Inaktive Audits“ werden alle derzeit deaktivierten Audits angezeigt.
2. Klicken Sie auf eines der Audits, um weitere Informationen dazu anzuzeigen.
3. **Wahlweise:** Aktivieren Sie ein Audit, indem Sie auf das Kontrollkästchen **Aktiv** klicken und im Feld **Häufigkeit** angeben, wie oft das Audit ausgeführt werden soll.
4. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identität

Erfahren Sie mehr über die Identitäten in der Instanz.

Zugriffsanalyse

Die Zugriffsanalyse ist eine ServiceNow® Store-App, die ein Zugriffsdiagnoseservice ist. Es hilft zu bestimmen, wer Zugriff auf eine Ressource hat.

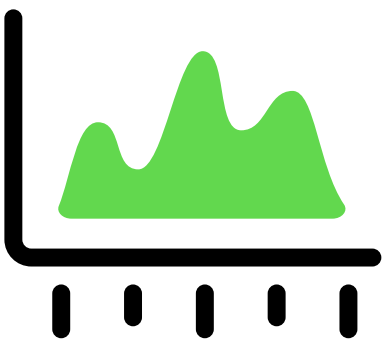
Globale Identität

Global Identity ist eine ServiceNow® Store-App, mit der Benutzerattribute von Instanz zu Instanz (mehrere Instanzen) aktualisiert werden können.

Identity Center

Mit Identity Center können Sie identitätsbasierte Risiken und Sicherheitslücken überwachen, verwalten und minimieren.

System für domänenübergreifendes Identitätsmanagement (SCIM)



Identitäts- und Zugriffsaudit

Verwenden Sie das Identitäts- und Zugriffsaudit, um die Änderungen an einem Benutzer, einer Gruppe, einer Rolle und einer ACL zu verstehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die SCIM-API (System for Cross-Domain Identity Management) bietet Endpunkte zum Erstellen, Lesen, Aktualisieren und Löschen von Vorgängen für Benutzer und Gruppen mithilfe des SCIM-Protokolls.		

Zugriffsanalyse

Die Zugriffsanalyse ist eine ServiceNow® Store-App, die ein Zugriffsdiagnosetool ist. Es hilft zu bestimmen, wer Zugriff auf eine Ressource hat.

Globale Identität

Global Identity ist eine ServiceNow® Store-App, mit der Benutzerattribute von Instanz zu Instanz (mehrere Instanzen) aktualisiert und synchronisiert werden können.

Identitäts- und Zugriffsaudit

Verwenden Sie das Identitäts- und Zugriffsaudit, um die Änderungen an einem Benutzer, einer Gruppe, einer Rolle und einer ACL zu verstehen.

Identity Center

Mit Identity Center können Sie identitätsbasierte Risiken und Sicherheitslücken überwachen, verwalten und minimieren.

System für domänenübergreifendes Identitätsmanagement (SCIM)

Die SCIM-API (System for Cross-Domain Identity Management) bietet Endpunkte zum Erstellen, Lesen, Aktualisieren und Löschen von Vorgängen für Benutzer und Gruppen mithilfe des SCIM-Protokolls.

Zugriffsanalyse

ServiceNow® Zugriffsanalyse ist ein Zugriffsdiagnosetool, das beim Anzeigen der Berechtigungen einer Identität für eine Ressource hilft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Lernen Sie die Funktionen und den Geschäftsnutzen der Zugriffsanalyse kennen.

Verwenden

Machen Sie sich mit der Verwendung der Zugriffsanalyse vertraut.

Berechtigungsauswertung

Wissen, wie die Berechtigungen ausgewertet werden.

Häufige Fragen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsanalyse erkunden

Analysieren Sie Identitäten in der Instanz ServiceNow®.

ServiceNow Die Zugriffsanalyse ist eine Anwendung, die Administratoren und Entwicklern hilft, Berechtigungen für den ausgewählten Benutzer, die ausgewählte Rolle oder die ausgewählte Gruppe anzuzeigen.

Hinweis:

- Die Zugriffsanalyse ist ein Produkt aus dem ServiceNow Store. Besuchen Sie die Website ServiceNow Store , um sich alle verfügbaren Apps anzusehen und Informationen zum Senden von Anforderungen an den Store zu erhalten.
- Die Zugriffsanalyse nimmt die Identität des Identitätsdatensatzes an, um Details zu den Berechtigungen abzurufen, und liest oder speichert keine persönlichen oder vertraulichen Daten der Identität.
- Die Auswertungsergebnisse der Zugriffsanalyse sind unabhängig von den für die Benutzer definierten Zugriffsrichtlinien identisch, z. B. Zero Trust Access (ZTA). Die Richtlinien werden nur während der tatsächlichen Benutzeranmeldung und nicht während des Zugriffsanalyse-Flows ausgewertet.
- Die Zugriffsanalyse hat Einschränkungen bei der genauen Auswertung des Zugriffs auf die Ressourcen im Zusammenhang mit Ressourcen im verwalteten Bereich und delegierten Entwicklern.

Evaluiert den Zugriff

„Zugriff evaluieren“ ist eine Fähigkeit der ServiceNow Zugriffsanalyse, die Administratoren und Entwicklern hilft, Berechtigungen für den ausgewählten Benutzer, die ausgewählte Rolle oder die ausgewählte Gruppe anzuzeigen.

Sie können damit die Berechtigungen von Benutzern, Gruppen, Rollen für eine Tabelle, vom Client aufrufbare Skripteinbindungen, UI-Seiten und REST-Endpunkte analysieren und anzeigen.

Mit der Zugriffsanalyse können Unternehmen ihre Sicherheitslage, Identitäts-Governance und Risikomanagement verbessern, ihre Compliance-Ziele erreichen und nachvollziehen, wer (Identität) Zugriff auf was (Ressourcen) hat.

Zugriff vergleichen

„Zugriff vergleichen“ ist eine Funktion der ServiceNow Zugriffsanalyse V2, mit der Administratoren, Entwickler und Support-Mitarbeiter den Benutzerzugriff vergleichen und die richtige Zugriffsebene für die Benutzer in Ihrer ServiceNow -Instanz bestimmen können.

Der Zugriffsvergleich kann zwischen den Benutzern für die Benutzerdatensätze und die Zugriffssteuerung durchgeführt werden.

Mit dem Vergleichszugriff können Sie die folgenden Analysen durchführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ebene 1: Benutzerdatensätze vergleichen, um die Attribute, Rollen und Gruppen zu verstehen.
- Ebene 2: Zugriffskontrollen vergleichen, um die Ursachenanalyse auszuführen, indem Zugriffsprobleme ermittelt werden.

Vorteile

Im Folgenden sind einige der Vorteile der Verwendung der Zugriffsanalyse aufgeführt:

- Analysieren Sie den Zugriff auf Ressourcen (Tabellen).
- Vergleichen Sie den Zugriff von 2 Anwendern.
- Vergleichen Sie die Rollen und Gruppen von 2 Benutzern.
- Verhindern Sie die übermäßige Bereitstellung von Berechtigungen.
- Generieren Sie einen Bericht, der zeigt, ob eine Identität Zugriff auf eine Ressource (Tabelle) hat.
- Verstehen, wer Zugriff auf kritische Sicherheitsmaßnahmen hat.
- Helfen Sie, eine übermäßige Bereitstellung von Berechtigungen zu verhindern.
- Bei der Implementierung von Zugriffskontrollen die Prinzipale mit den geringsten Berechtigungen erreichen.
- Beschränken Sie den Zugriff auf bestimmte Daten, einschließlich Anwendungen, Tabellen, Zeilen oder Spalten und andere Ressourcen.
- Stellen Sie Berichterstellungsfunktionen für die Analyseergebnisse bereit.
- Vergleichen Sie den Zugriff zwischen Benutzerdatensätzen und Zugriffssteuerungen.
- Bestimmen Sie die richtige Zugriffsebene für Benutzer in Ihrer Instanz ServiceNow.

Zugriffsanalyse verwenden

Analysieren Sie Identitäten und ihren Zugriff auf die Instanz ServiceNow®.

Vorbereitungen
Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Schritte für den Zugriff auf die Zugriffsanalyse und die Verwendung verschiedener Funktionen in der Zugriffsanalyse.

Hinweis:
Die Zugriffsanalyse ist ein Produkt aus dem ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.

   Die Zugriffsanalyse verfügt über die folgenden Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Evaluiert den Zugriff
- Benutzerdatensätze vergleichen
- Zugriffskontrollen vergleichen

2. Wählen Sie die entsprechende Registerkarte aus, um die Zugriffsanalyse basierend auf Ihren Anforderungen zu verwenden.

Verwenden des Evaluierungszugriffs

Analysieren Sie Identitäten in der Instanz ServiceNow®.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Schritte für den Zugriff auf Evaluate Access in der Zugriffsanalyse und die Verwendung der verschiedenen Funktionen.

Hinweis:
Die Zugriffsanalyse ist ein Produkt von ServiceNow Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie die Registerkarte **Zugriff** evaluieren aus.
3. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Analysieren Sie den Zugriff für einen Benutzer, eine Rolle oder eine Gruppe
Benutzer auswählen *	Geben Sie einen Benutzernamen an, den Sie aus der Liste auswählen können.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, den Sie aus der Liste auswählen können.
Datensatz auswählen	Geben Sie einen Datensatznamen an, den Sie aus der Liste auswählen möchten.
Feld auswählen	Geben Sie einen Feldnamen an, den Sie aus der Liste auswählen können.

4. Geben Sie die Beschreibung im Feld **Beschreibung** an.
5. Wählen Sie **Berechtigungen analysieren aus**.

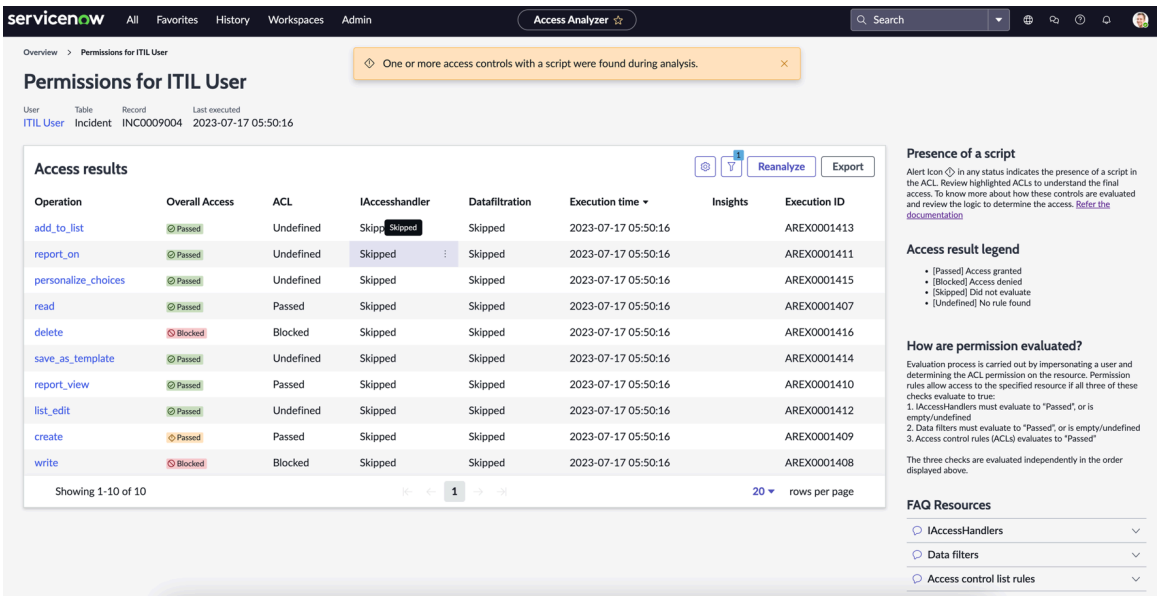
Die Zugriffsergebnisse für den Benutzer werden angezeigt. Ebenso können Sie die Berechtigungen einer Gruppe oder Rolle für die folgenden Regeltypen analysieren:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Tabelle (Datensatz)
- Vom Client aufrufbare Skripteinbindung
- REST-Endpunkte

Die Zugriffsergebnisse werden angezeigt.



Die Tabelle „Rhe-Zugriffsergebnisse“ enthält die folgenden Felder:

Auf Ergebnisse zugreifen

Felder	Beschreibung
Vorgang	Die Art des Vorgangs, den der Benutzer, die Gruppe oder die Rolle für die ausgewählte Tabelle, den Datensatz oder das Feld ausführen kann.
Allgemeiner Zugriff	Ergebnis des Gesamtzugriffs. Die Ergebnisse lauten wie folgt: ○ [Bestanden] Zugriff gewährt ○ [Blockiert] Zugriff verweigert ○ [Übersprungen] Wurde nicht ausgewertet ○ [Nicht definiert] Keine Regel gefunden
Sys-Sicherheits-ACL	Ob eine ACL für den ausgewählten Vorgang definiert ist.
IAccesshandler	Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet.
Datenfilterung	Ein Datenfilter ist eine Form der Zugriffskontrolle, die auf die vorhandenen Zugriffskontrollregeln (ACLs) in Ihrer Instanz abgestimmt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
Ausführungszeit	Der Zeitpunkt, zu dem die Zugriffsergebnisse ausgeführt wurden.
Einblicke	Weitere Informationen zum ausgewählten Vorgang.
Ausführungs-ID	Eine eindeutige ID für jede Ausführung des Zugriffsergebnisses.

Zeigen Sie Berechtigungen für einen Benutzer an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für einen ausgewählten Benutzer anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für einen ausgewählten Benutzer (**ITIL-Benutzer**), um die Berechtigungen der **Incident** -Tabelle mithilfe des Auswertungszugriffs in der Zugriffsanalyse anzuzeigen.

Hinweis:
Die Zugriffsanalyse ist ein Produkt aus dem ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

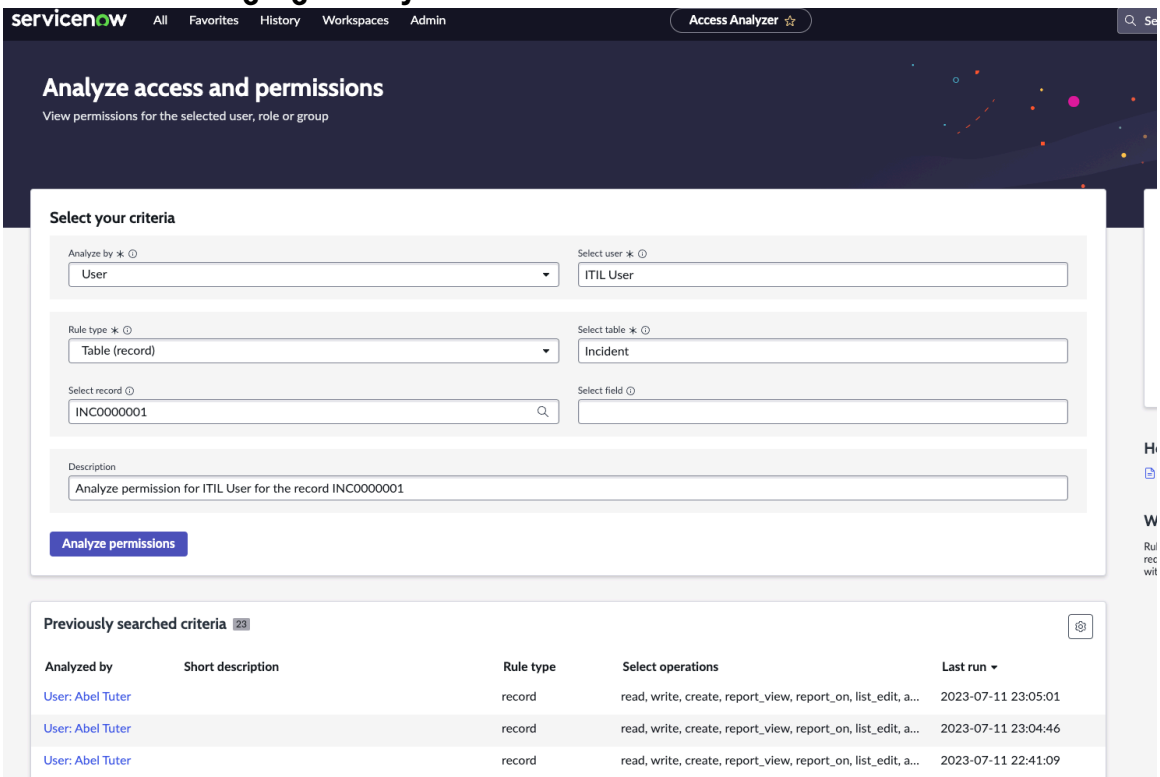
Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Wählen Sie **Benutzer** aus.
Benutzer auswählen *	Geben Sie einen Benutzernamen an, den Sie aus der Liste auswählen können. In diesem Beispiel **ITIL-Benutzer**.
Regeltyp *	Analysieren Sie den Zugriff für eine **Tabelle**, eine **UI-Seite**, einen **REST-Endpunkt**oder eine vom **Client aufrufbare Skripteinbindung**. In diesem Beispiel Tabelle.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, den Sie aus der Liste auswählen können. In diesem Beispiel **Incident**.
Datensatz auswählen	Geben Sie einen Datensatznamen an, den Sie aus der Liste auswählen möchten. In diesem Beispiel **INC0000001**.
Feld auswählen	Geben Sie einen Feldnamen an, den Sie aus der Liste auswählen können. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Beispiele: Aktiv, Erstellt von usw.

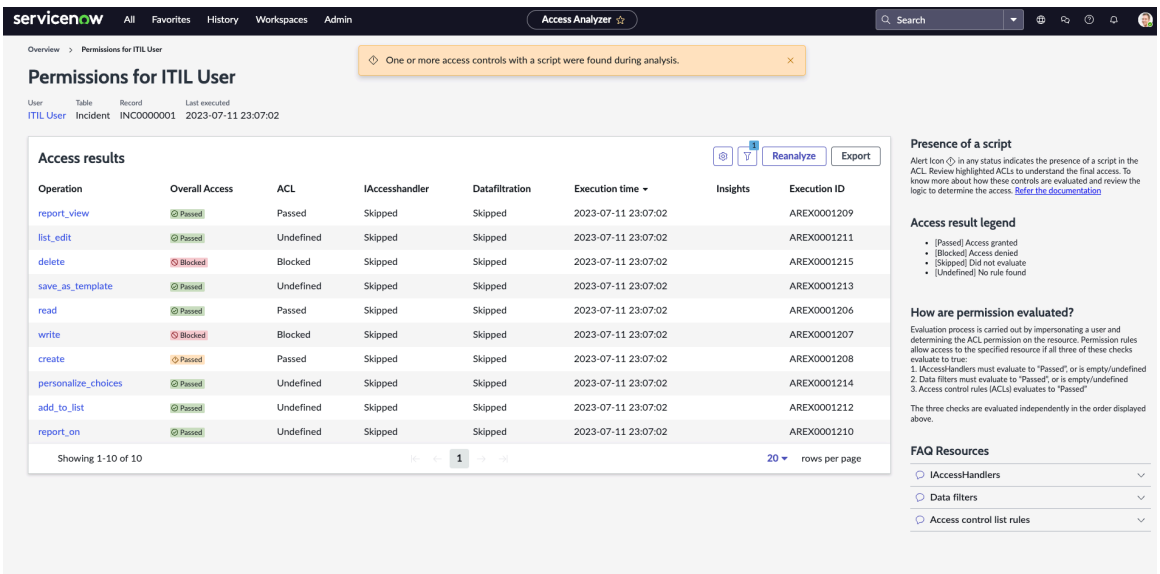
3. Geben Sie die Beschreibung im Feld **Beschreibung** an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Berechtigungen analysieren aus**.



Die **Zugriffsergebnisse** für den **ITIL-Benutzer** werden angezeigt.



Die Ergebnisse können anhand der Filter Legends, Access Control List (ACL), IAccesshandler und Data gelesen werden.

Nehmen wir das Beispiel des **Lesevorgangs**. Für den **ITIL-Benutzer** lautet der Gesamtzugriff Passed, was bedeutet, dass der Benutzer den Datensatz mit den richtigen Berechtigungen (ACL) lesen kann.

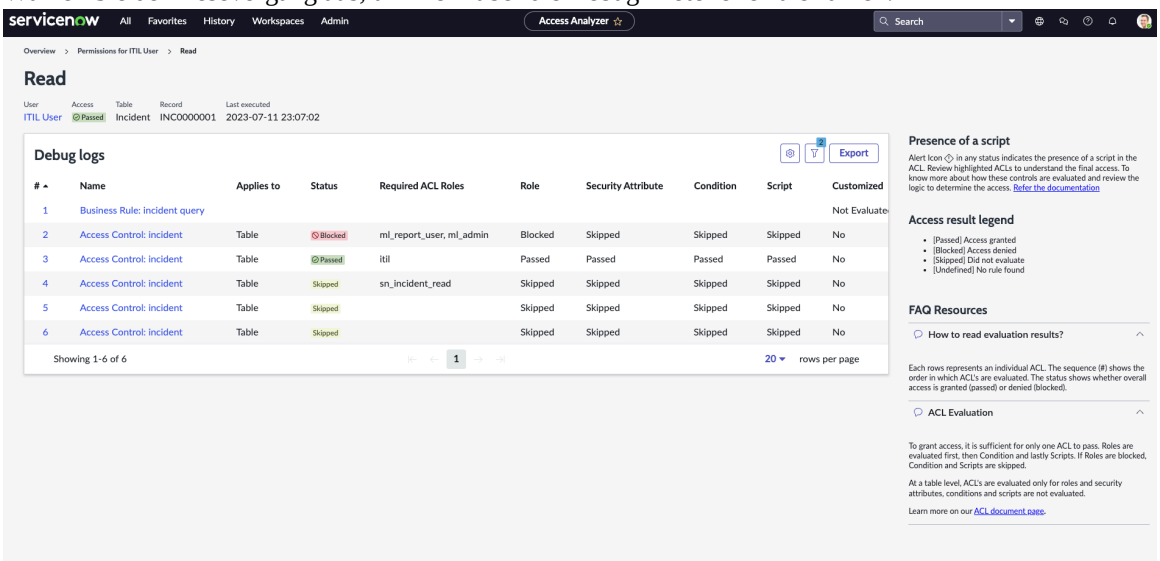
In ähnlicher Weise wird für den **Erstellungsvorgang** der Gesamtzugriff mit einem Warnungssymbol übergeben, was bedeutet, dass möglicherweise ein Skript für die ACL-Auswertung vorhanden ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In diesem Beispiel sind **Schreib-** und **Löschvorgänge** für den ausgewählten Benutzer blockiert, und der Benutzer kann den ausgewählten Datensatz nicht bearbeiten oder löschen (INC0000001).

5. Wählen Sie den Lesevorgang aus, um mehr über die Debug-Protokolle zu erfahren.

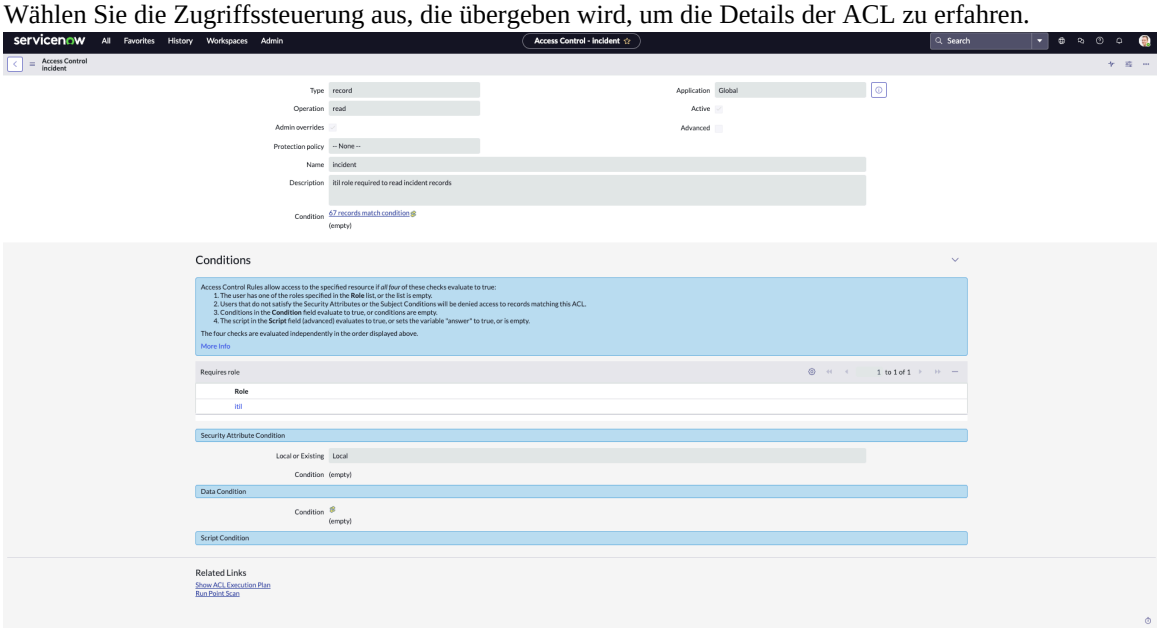


Auf der Seite „Debug-Protokolle“ werden die Business Rule und die zugehörigen ACLs angezeigt, die zum Ausführen des **Lesevorgangs** für den Datensatz erforderlich sind.

Die Debug-Protokolle zeigen, dass eine Geschäftsregel und 4 ACLs für den Lesevorgang zugeordnet sind.

Für eine der ACLs gibt es den Status **Bestanden**. Dies bedeutet, dass zum Lesen des ausgewählten Datensatzes der Benutzer über die erforderliche ACL verfügt und den Datensatz lesen kann. Da eine der ACLs **Bestanden**ist, werden die anderen ACL-Auswertungen **übersprungen**.

6. Wählen Sie die Zugriffssteuerung aus, die übergeben wird, um die Details der ACL zu erfahren.

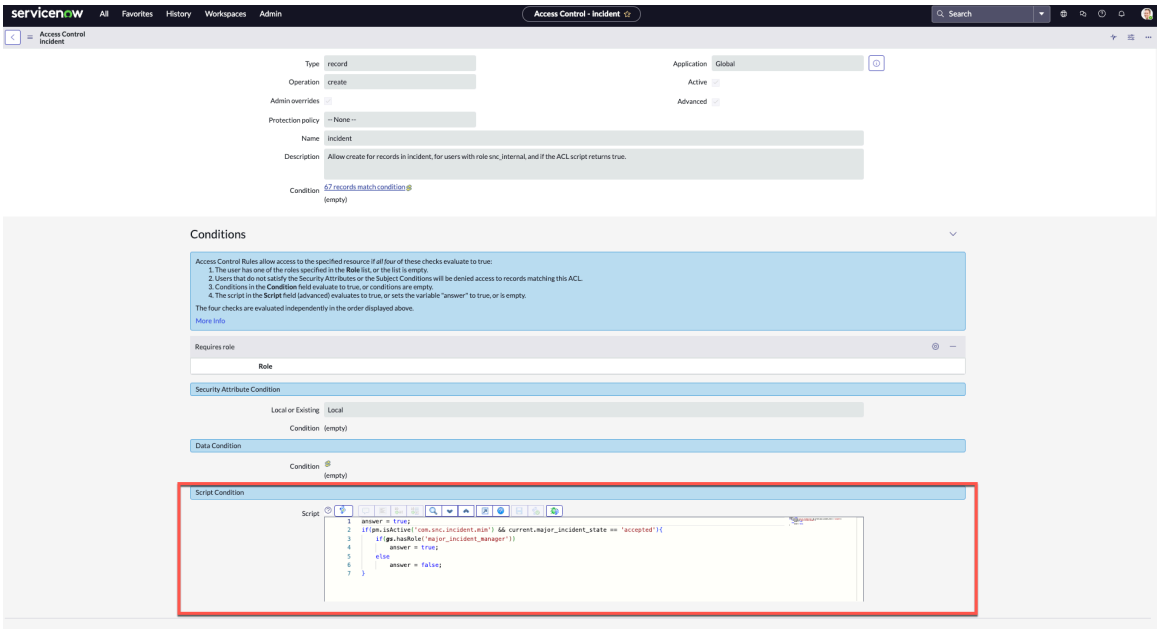


Die Details der Zugriffssteuerung für die ausgewählte ACL werden angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für einen ausgewählten Vorgang mit **Bestanden** und Vorhandensein eines Skripts. Auf der Seite „Zugriffssteuerung“ wird das zugehörige Skript für den Datensatz angezeigt.



Zeigen Sie Berechtigungen für eine Rolle an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für eine ausgewählte Rolle anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für eine ausgewählte Rolle (**user_admin**), um die Berechtigung für einen REST-API-Endpunkt mithilfe des Auswertungszugriffs in der Zugriffsanalyse anzuzeigen.

Hinweis:
Die Zugriffsanalyse ist ein Produkt aus dem ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

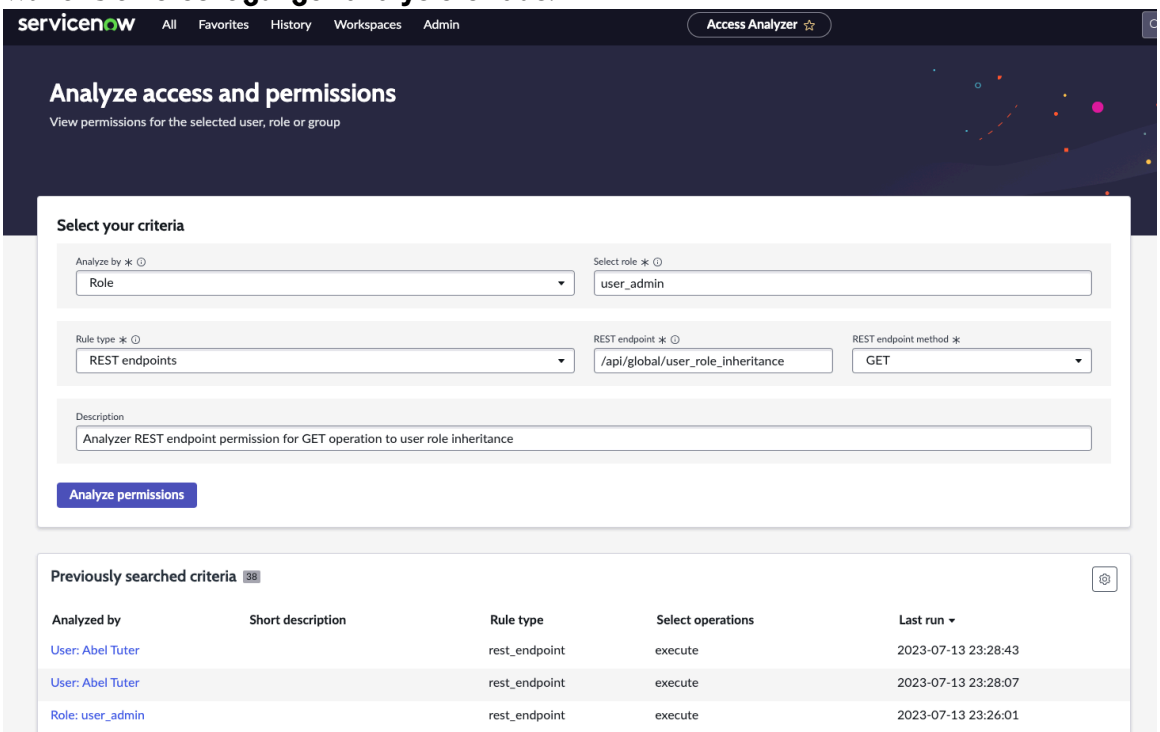
Feld	Beschreibung
Analysieren nach *	Wählen Sie **Rolle aus**.
Benutzer auswählen *	Geben Sie eine Rolle an, die aus der Liste ausgewählt werden soll. Beispiel: **user_admin**.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung. Beispiel: **REST-Endpunkt**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
REST-Endpunkt*	Geben Sie einen REST-Endpunkt an. Beispiel: `/api/global/user_role_inheritance`. **Hinweis:** Bei Verwendung des ausgewählten Felds muss der vollständige REST-Endpunkt verwendet werden.
REST-Endpunktmethode *	Geben Sie eine REST-Endpunktmethode an. Beispiel: GET.

3. Geben Sie die Beschreibung im Feld **Beschreibung** an.
4. Wählen Sie **Berechtigungen analysieren aus**.



Die **Zugriffsergebnisse** für die Rolle **user_admin** werden angezeigt.

Die Ergebnisse können anhand der Filter Legends, Access Control List (ACL), IAccesshandler und Data gelesen werden.

Der Gesamtzugriff für die Rolle wird übergeben, was bedeutet, dass die Rolle (**user_admin**) auf den **REST-Endpunkt** für die ausgewählte **GET** -Methode zugreifen kann.

Zeigen Sie Berechtigungen für eine Gruppe an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für eine ausgewählte Gruppe anzuzeigen.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für eine ausgewählte Gruppe (**Incident Management**), um die Berechtigungen einer **Incident-UI** -Seite mit dem Bewertungszugriff in der Zugriffsanalyse anzuzeigen.

Hinweis:
Die Zugriffsanalyse ist ein Produkt aus dem ServiceNow® Store.

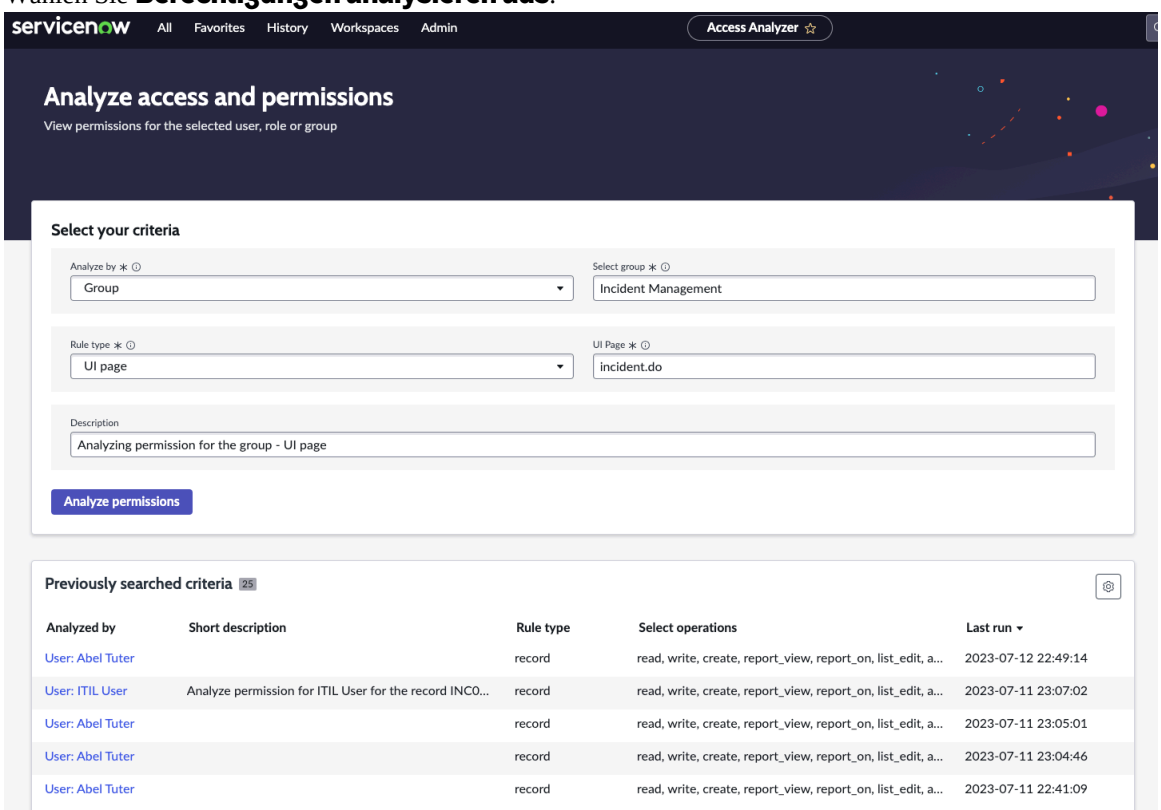
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Wählen Sie **Gruppe**aus.
Benutzer auswählen *	Geben Sie einen Benutzernamen an, den Sie aus der Liste auswählen können. Beispiel: **Incident Management**.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung. Beispiel: **UI-Seite**.
UI-Seite *	Geben Sie die UI-Seite an. Beispiel: **incident.do**.

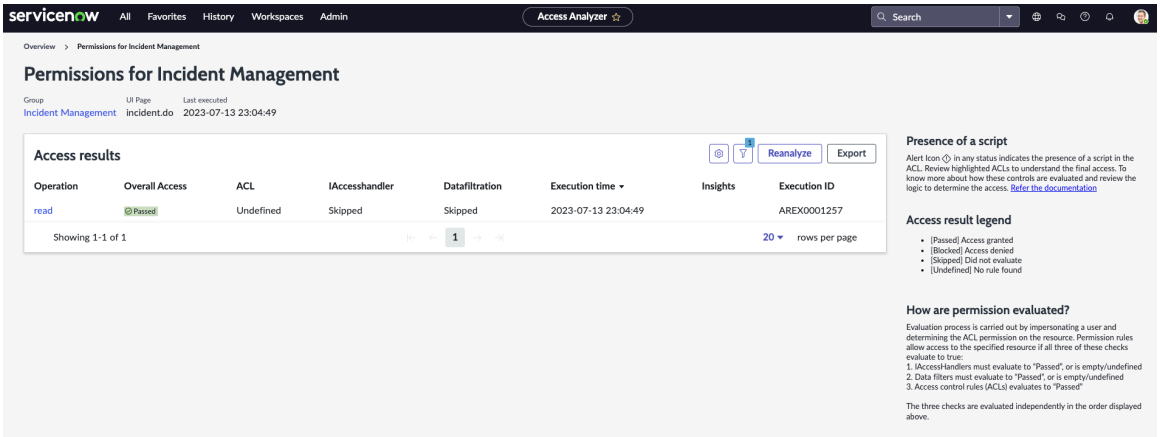
3. Geben Sie die Beschreibung im Feld **Beschreibung** an.
4. Wählen Sie **Berechtigungen analysieren aus**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Zugriffsergebnisse** für die **Incident Management** -Gruppe werden angezeigt.



Die Ergebnisse können anhand der Filter Legends, Access Control List (ACL), IAccesshandler und Data gelesen werden.

Der Gesamtzugriff für die Gruppe wird übergeben, was bedeutet, dass die Benutzer innerhalb der Gruppe (**Incident Management**) auf den Incident-Datensatz zugreifen können.

Exportieren Sie Abfragen der Zugriffsanalyse

Exportieren Sie die mit der Zugriffsanalyse analysierten Abfragen.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Schritte für den Zugriff auf die Zugriffsanalyse und die Verwendung verschiedener Funktionen in der Zugriffsanalyse.

Hinweis:
Die Zugriffsanalyse ist ein Produkt aus dem ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

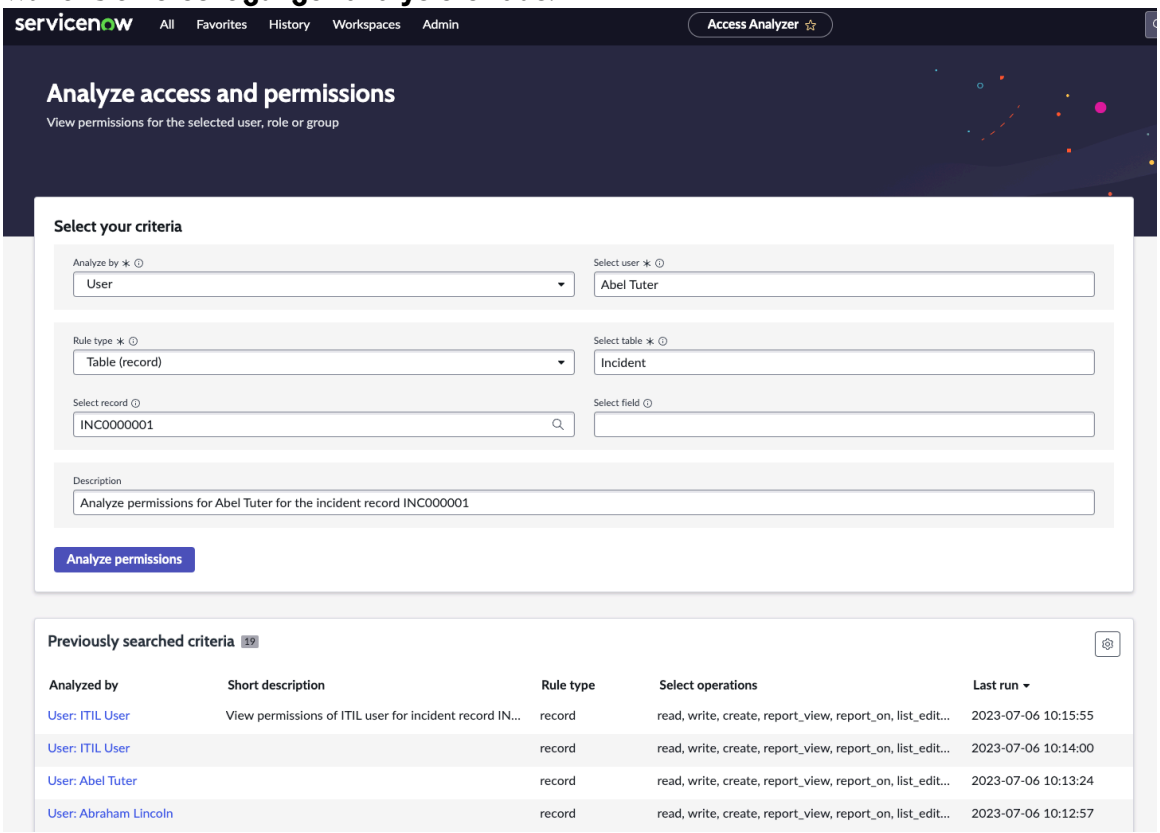
Feld	Beschreibung
Analysieren nach *	Analysieren Sie den Zugriff für einen Benutzer, eine Rolle oder eine Gruppe
Benutzer auswählen *	Geben Sie einen Benutzernamen an, den Sie aus der Liste auswählen können.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, den Sie aus der Liste auswählen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Datensatz auswählen	Geben Sie einen Datensatznamen an, den Sie aus der Liste auswählen möchten.
Feld auswählen	Geben Sie einen Feldnamen an, den Sie aus der Liste auswählen können.

3. Geben Sie die Beschreibung im Feld **Beschreibung** an.
4. Wählen Sie **Berechtigungen analysieren aus**.



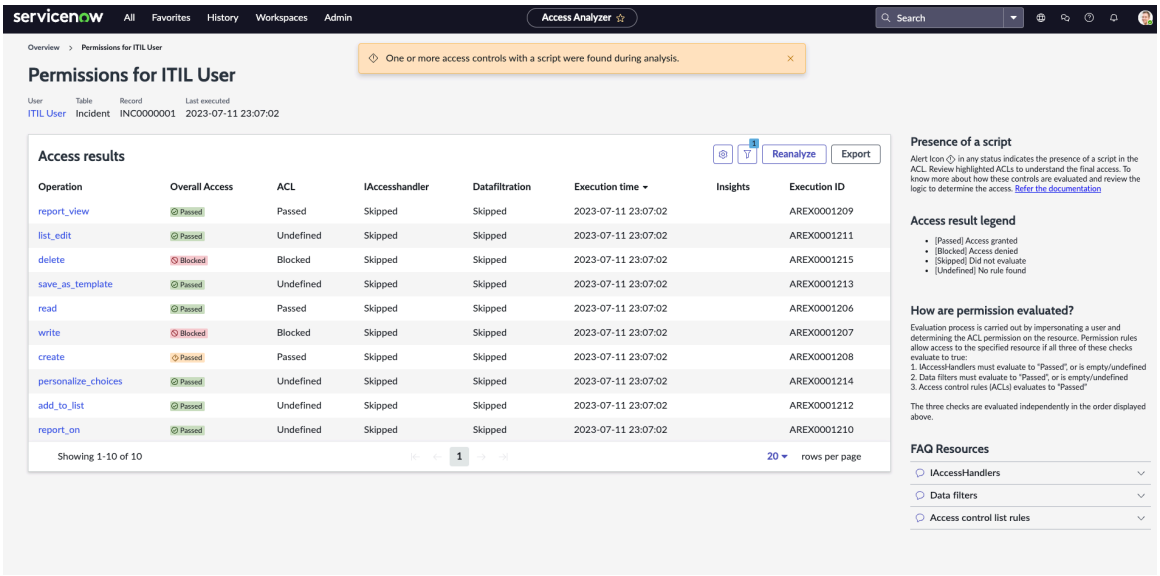
Die Zugriffsergebnisse für den Benutzer werden angezeigt. Ebenso können Sie die Berechtigungen einer Gruppe oder Rolle für die folgenden Regeltypen analysieren:

- Tabelle (Datensatz)
- Vom Client aufrufbare Skripteinbindung
- REST-Endpunkte

Die **Zugriffsergebnisse** für den ausgewählten Regeltyp werden angezeigt.

Automatische Übersetzung

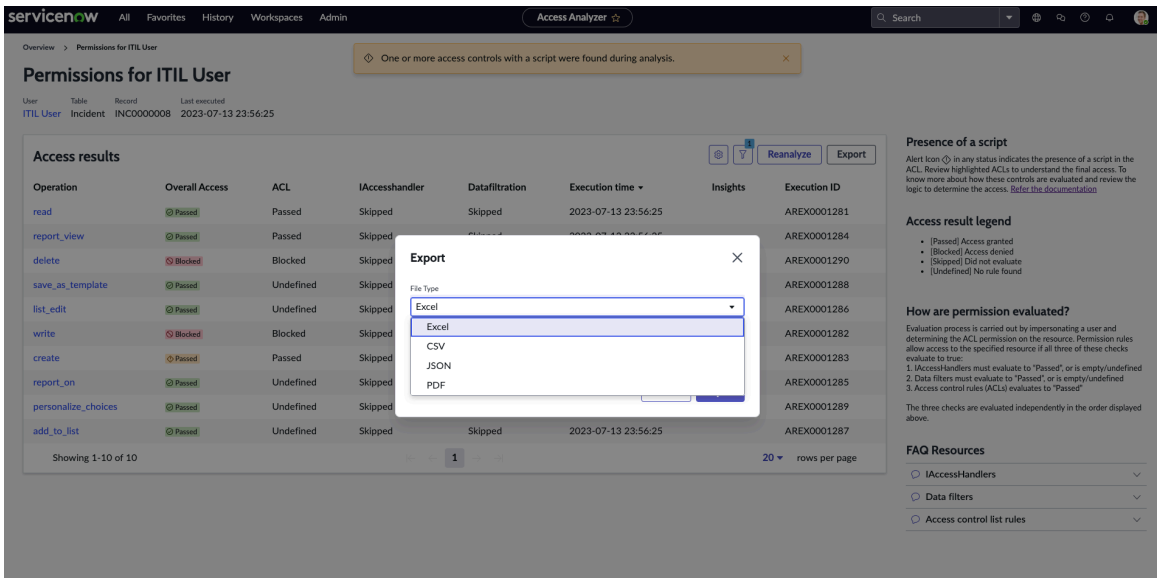
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Exportieren**.

a. Wählen Sie den Dateityp aus.

Verfügbare Dateitypen sind Excel, CSV, JSON, PDF.

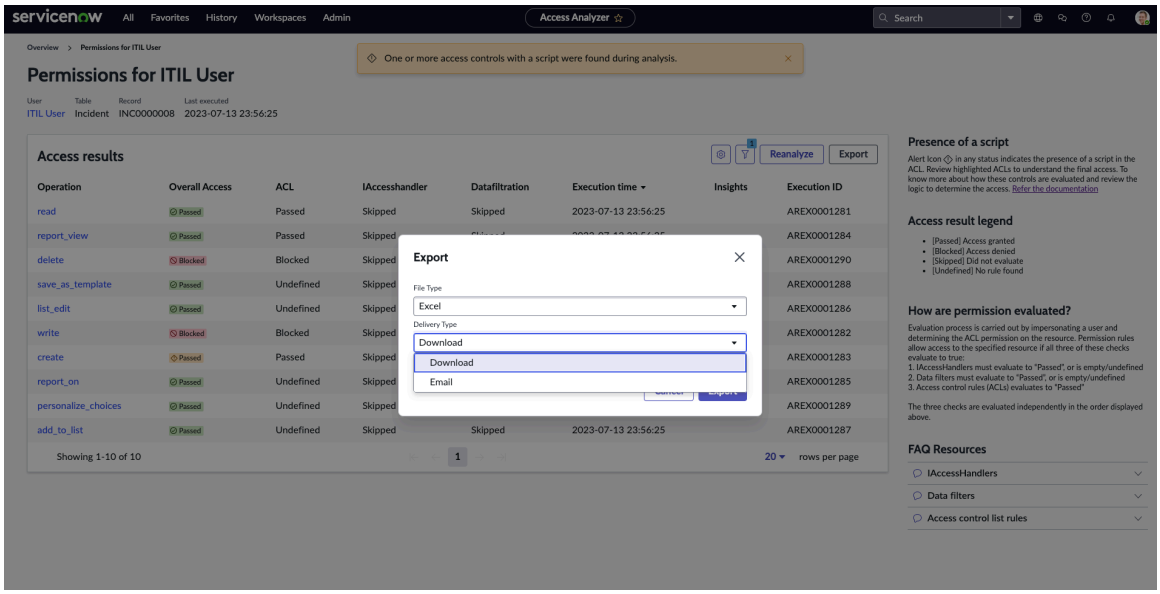


b. Wählen Sie den Bereitstellungstyp aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Bereitstellungstypen: Download und E-Mail.



Benutzerdatensätze werden verglichen

Vergleichen Sie Benutzerdatensätze, um den Zugriff zwischen zwei Benutzern zu verstehen.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Schritte zum Vergleichen von Benutzerdatensätzen mit der Zugriffsanalyse.

Hinweis:
Die Zugriffsanalyse ist ein Produkt von ServiceNow® Store.

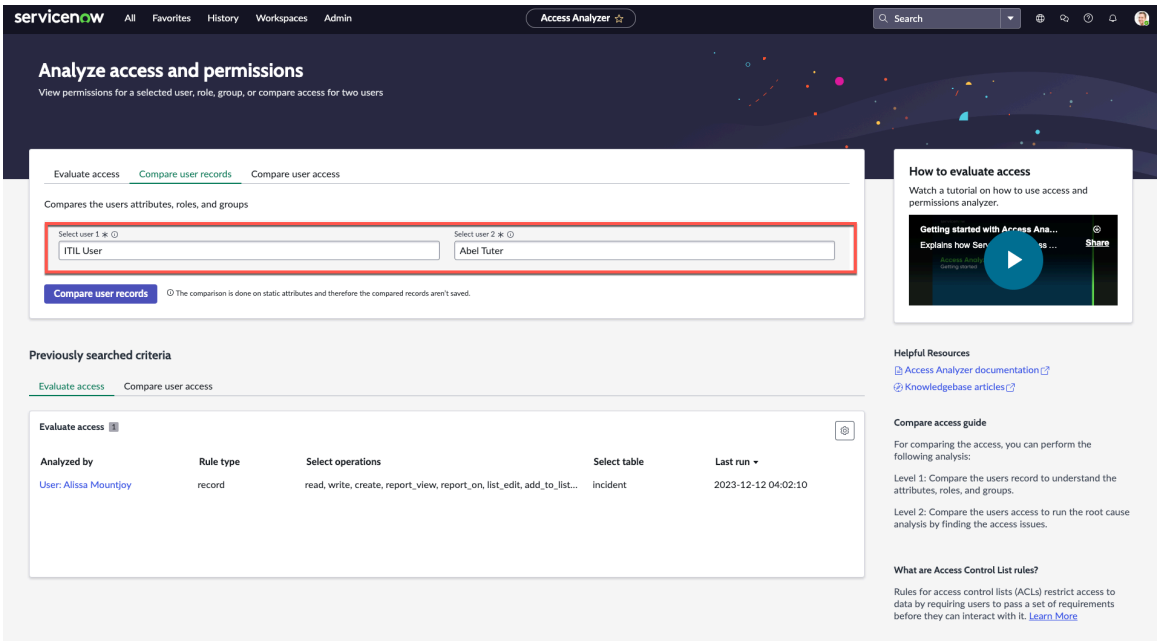
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie die Registerkarte **Benutzerdatensätze vergleichen** aus.
3. Wählen Sie **Benutzer 1** und **Benutzer 2** zum Vergleich aus.

   Beispiel: ITIL-Benutzer als **Benutzer 1** und Abel Tuter als **Benutzer 2**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



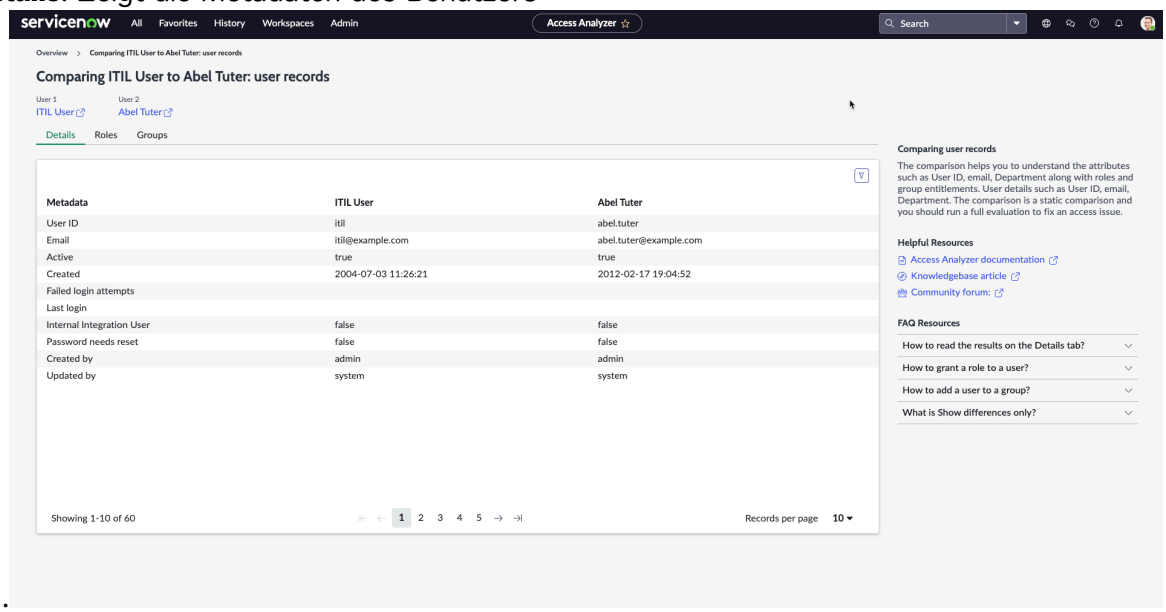
4. Wählen **Sie Benutzerdatensätze vergleichen aus**.

   Die Ergebnisse werden auf den folgenden Registerkarten angezeigt:

Automatische Übersetzung

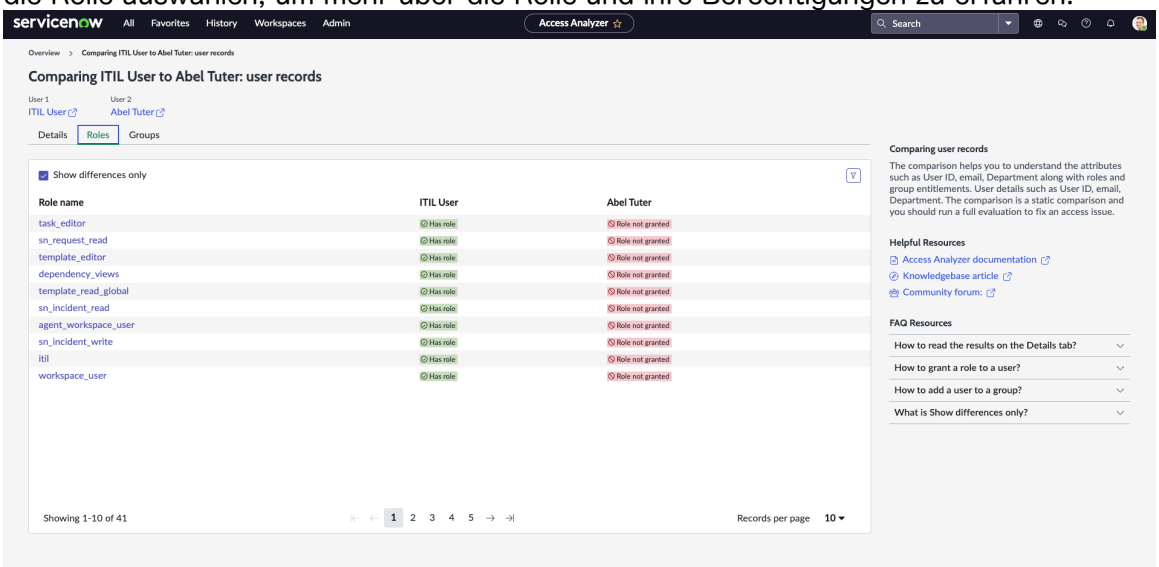
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Details**: Zeigt die Metadaten des Benutzers



an.

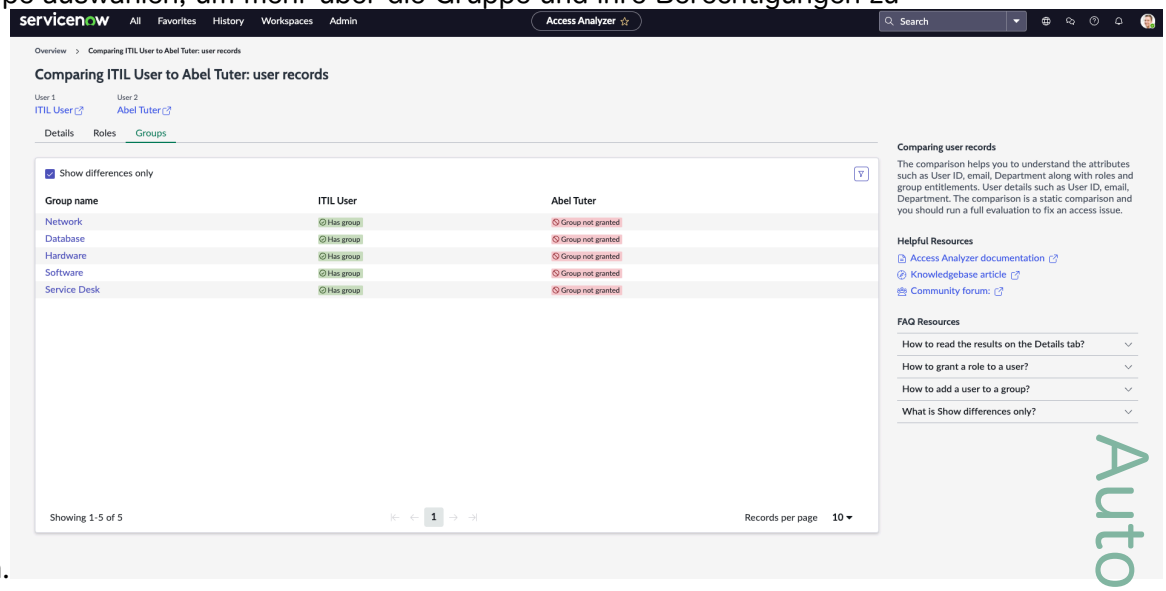
- **Rollen**: Zeigen Sie die Rollen an, die dem Benutzer zugewiesen sind. Sie können die Rolle auswählen, um mehr über die Rolle und ihre Berechtigungen zu erfahren.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Gruppen**: Zeigen Sie die Gruppen an, die dem Benutzer zugewiesen sind. Sie können die Gruppe auswählen, um mehr über die Gruppe und ihre Berechtigungen zu erfahren.



Ebenso können Sie verschiedene Benutzer in der Instanz ServiceNow vergleichen, um den Zugriff zu verstehen, der den Benutzern zugewiesen ist.

Vergleich des Benutzerzugriffs

Vergleichen Sie die Zugriffssteuerung des Benutzers mit der Zugriffsanalyse.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Schritte zum Vergleichen der Zugriffskontrolle zwischen den Benutzern mithilfe der Zugriffsanalyse.

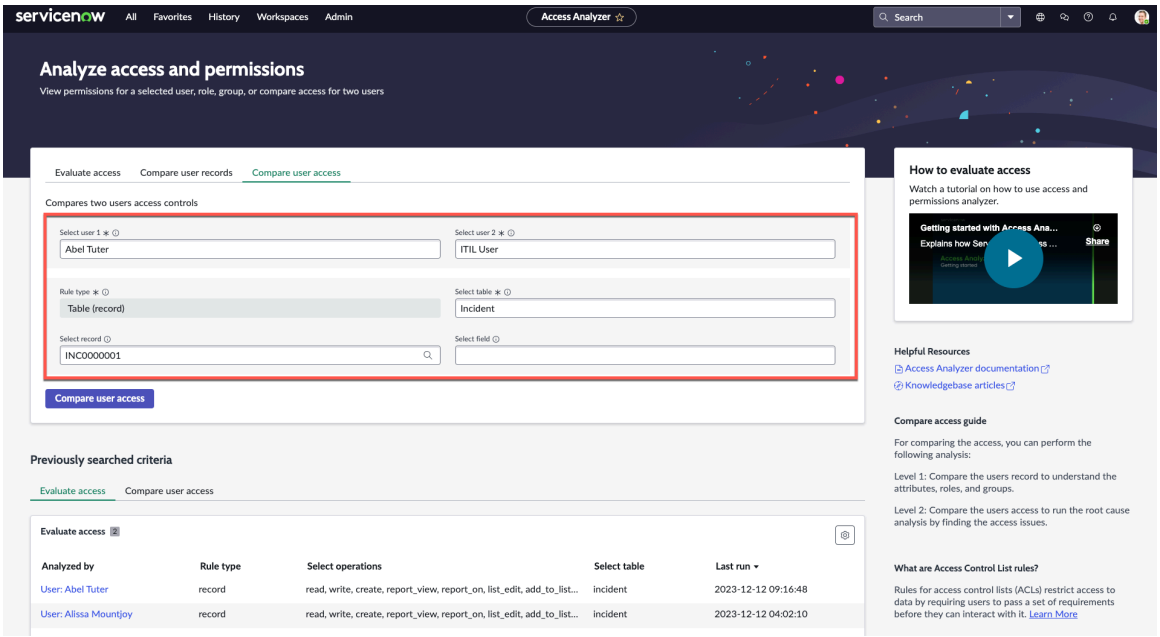
Hinweis:
Die Zugriffsanalyse ist ein Produkt von ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie die Registerkarte **Benutzerzugriff vergleichen** aus.
3. Füllen Sie folgende Felder aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Vergleichen Sie den Benutzerzugriff

Feld	Beschreibung
Anwender 1* auswählen	Geben Sie einen Benutzernamen an, den Sie aus der Liste für den Vergleich auswählen können.
Anwender 2* auswählen	Geben Sie einen Benutzernamen an, den Sie aus der Liste auswählen und mit dem Benutzer 1 vergleichen möchten.
Regeltyp*	Analysieren Sie Zugriffsberechtigungen für eine Tabelle. **Hinweis:** Beim **Vergleich des Benutzerzugriffs**können nur Zugriffsberechtigungen für eine Tabelle verwendet werden.
Tabelle auswählen*	Geben Sie einen Tabellennamen an, den Sie aus der Liste auswählen können.
Datensatz auswählen	Geben Sie einen Datensatznamen an, den Sie aus der Liste auswählen möchten.
Feld auswählen	Geben Sie einen Feldnamen an, den Sie aus der Liste auswählen können.

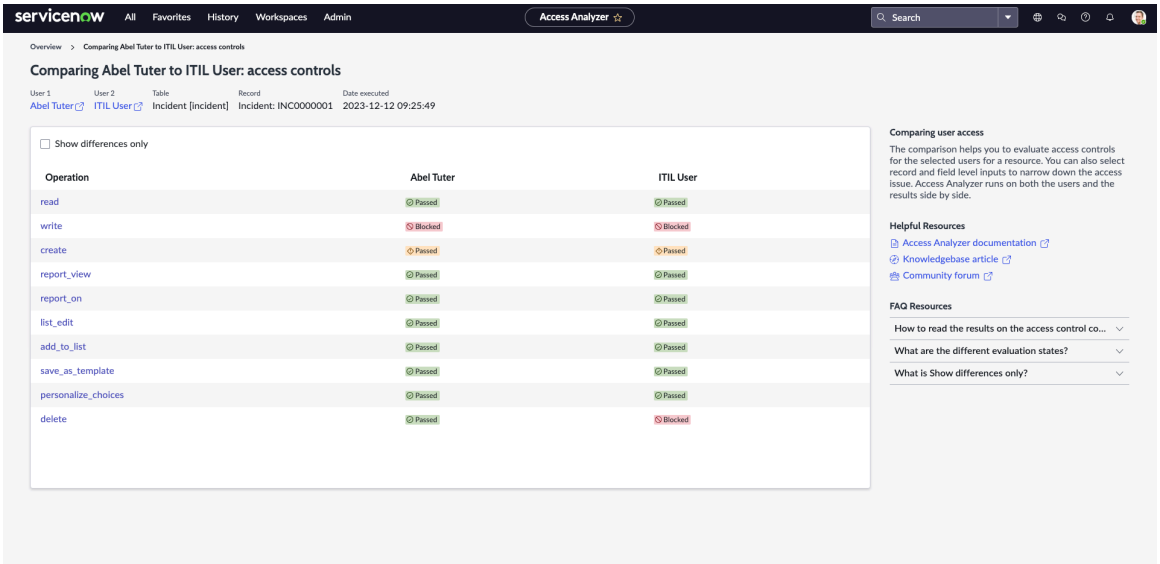
4. Wählen **Sie Benutzerzugriff vergleichen aus**.

   Die Ergebnisse des **Benutzerzugriffsvergleichs** für die ausgewählten Benutzer werden angezeigt.

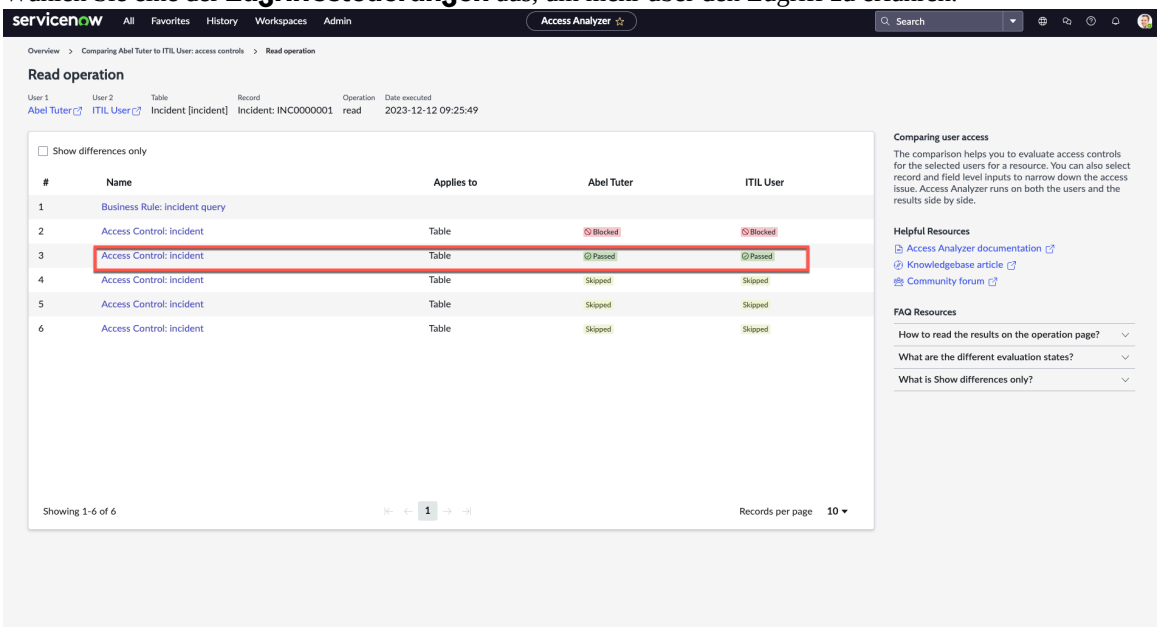
   Die Ergebnisse des Benutzerzugriffsvergleichs zeigen den Vorgang und den Zugriffsauswertungsstatus für die Benutzer an. Zum Beispiel Abel Tuter und ITIL-Benutzer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



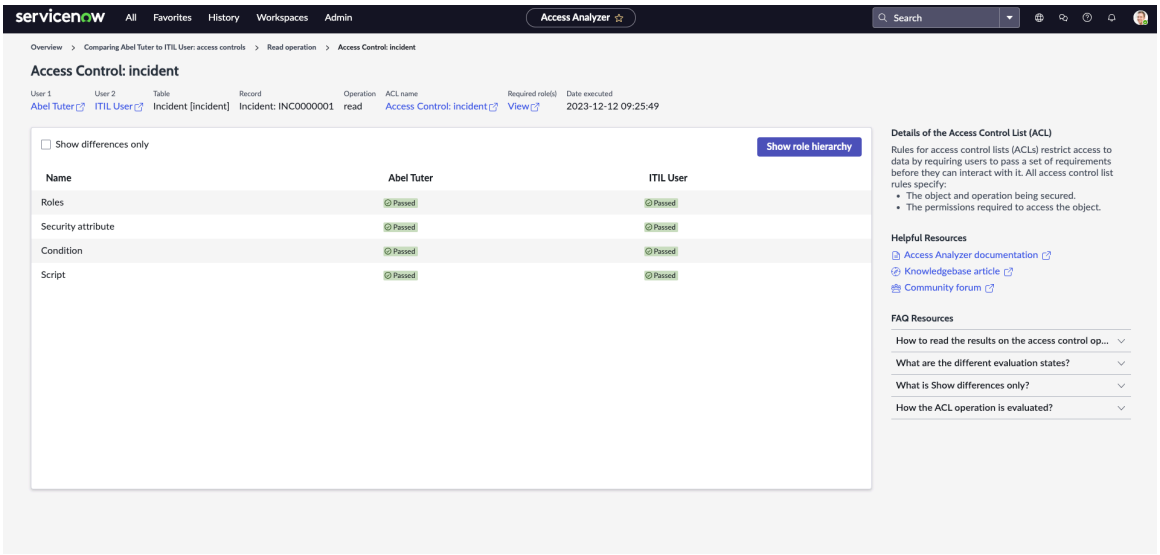
5. Wählen Sie den Vorgang aus, um mehr über die Berechtigungsbewertung und die Rollen zu erfahren, denen die Benutzer zugewiesen sind.
   Beispiel: **Lesevorgang**.
6. Wählen Sie eine der **Zugriffssteuerungen** aus, um mehr über den Zugriff zu erfahren.



Die Zugriffssteuerungsdetails wie Rollen, Sicherheitsattribut, Bedingung und Skriptauswertungsstatus werden angezeigt.

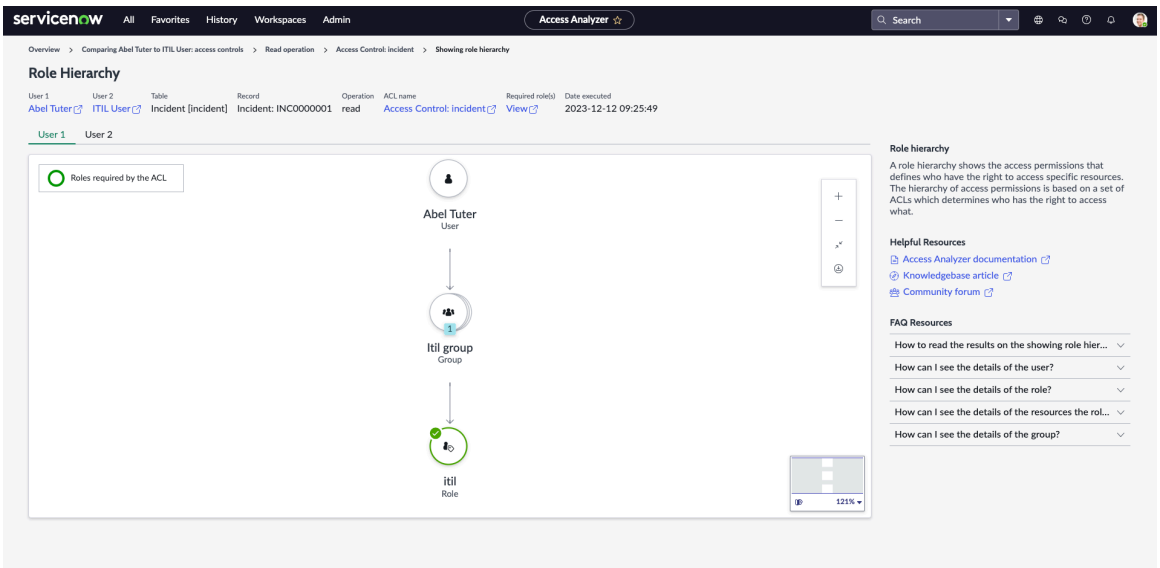
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wählen Sie **Rollenhierarchie anzeigen** aus, um mehr über die Rollen und Gruppen zu erfahren, die dem Benutzer zugewiesen sind, und beide Benutzer zu vergleichen.

Basierend auf der Rollenhierarchie können Sie dem Benutzer die erforderlichen Rollen- und Gruppenzuweisungen zuweisen, um Zugriff auf die Ressourcen (Tabelle) zu erhalten.

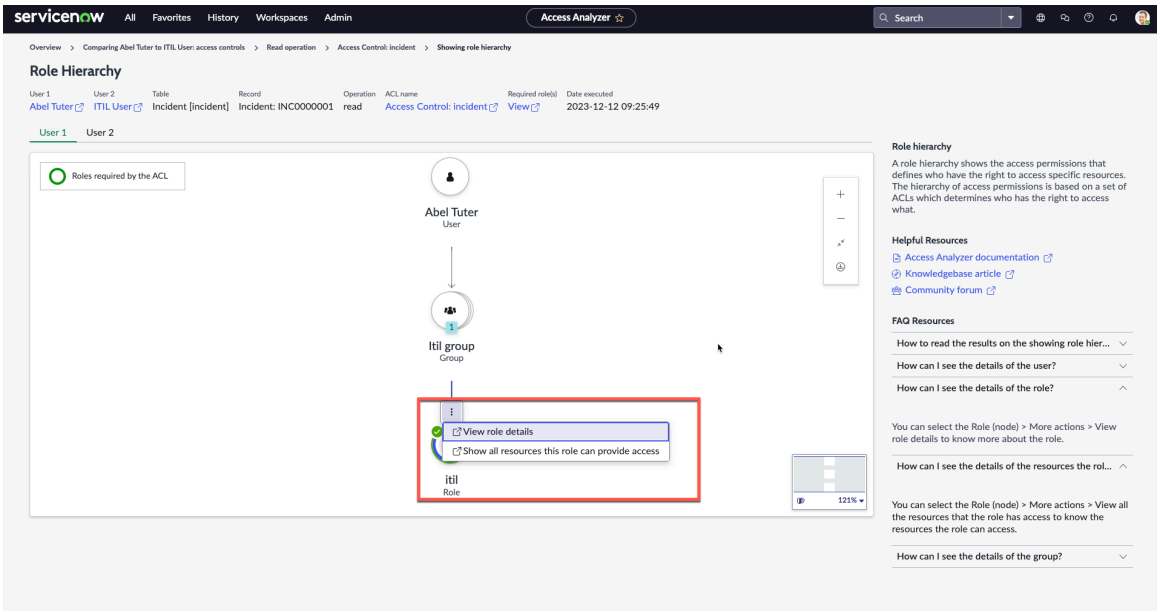


Im Beispiel ist sowohl **Abel Tuter** als auch dem **ITIL** -Benutzer der itil- Benutzer zugewiesen. Daher wurden beide Zugriffskontrollen bestanden. Sie können die erforderlichen Rollen- und Gruppenzuweisungen für den Benutzer ermitteln, indem Sie sich die Rollenhierarchie ansehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können den Knoten auswählen, um mehr über die Rolle, die Ressourcen, auf die die Rolle zugreifen kann, oder die Gruppe zu erfahren.



Abfragen der Zugriffsanalyse anzeigen – Zuvor durchsuchte Kriterien

Zeigen Sie zuvor durchsuchte Zugriffsanalysekriterien an.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis:
Die Zugriffsanalyse ist ein Produkt von ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Abfragen der Zugriffsanalyse**.

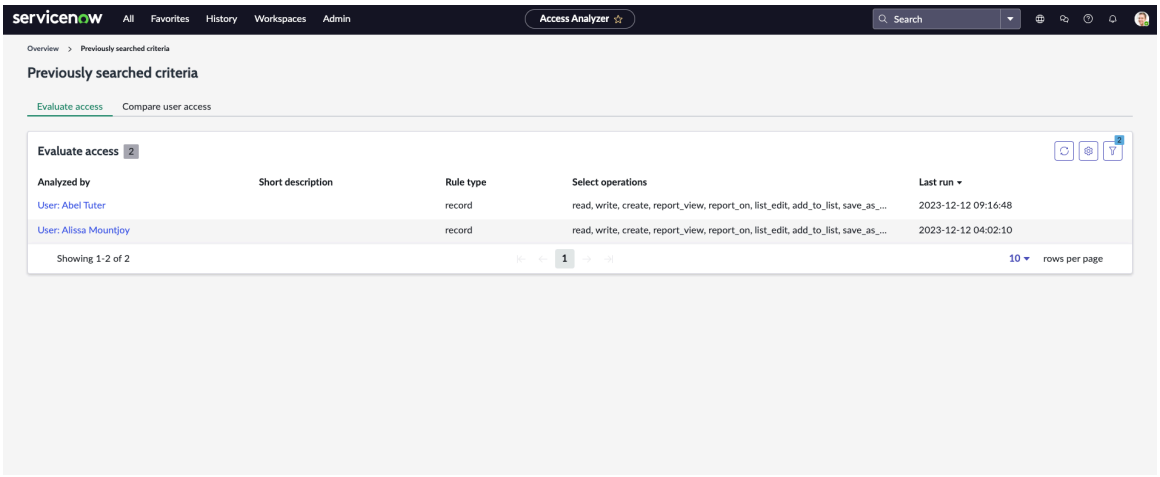
   Zuvor durchsuchte Kriterien weisen die folgenden Abschnitte auf:

   - **Zugriff evaluieren**: Zeigt Ergebnisse basierend auf Abfragen an, die über die Funktionen **„Zugriff** evaluieren“ gestellt wurden.
   - **Benutzerzugriff vergleichen**: Zeigt Ergebnisse basierend auf Abfragen an, die über die Funktionen zum **Vergleichen von Benutzerzugriffen** gestellt wurden.

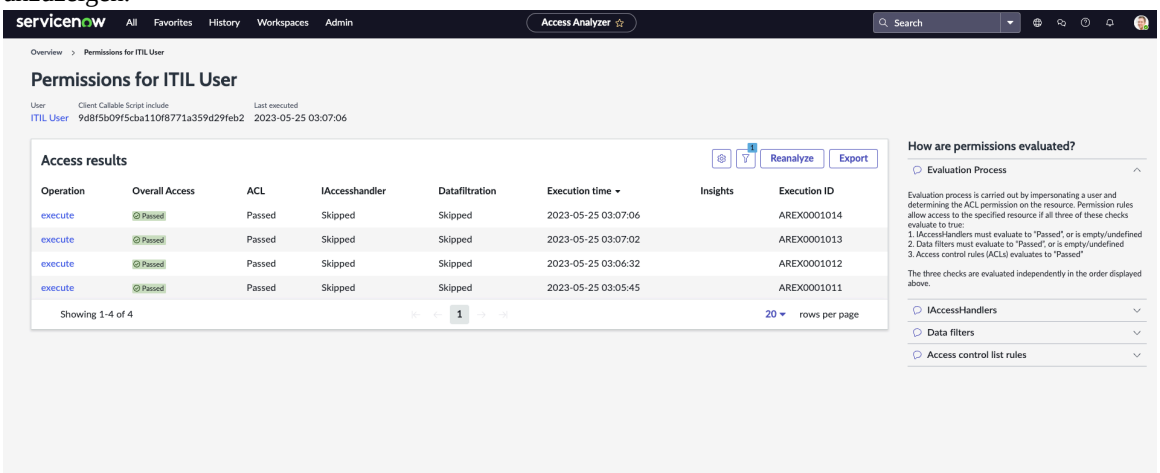
   Hinweis:
   Die zuvor durchsuchten Kriterien werden bei Verwendung der Funktion zum Vergleichen von Benutzerdatensätzen nicht gespeichert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

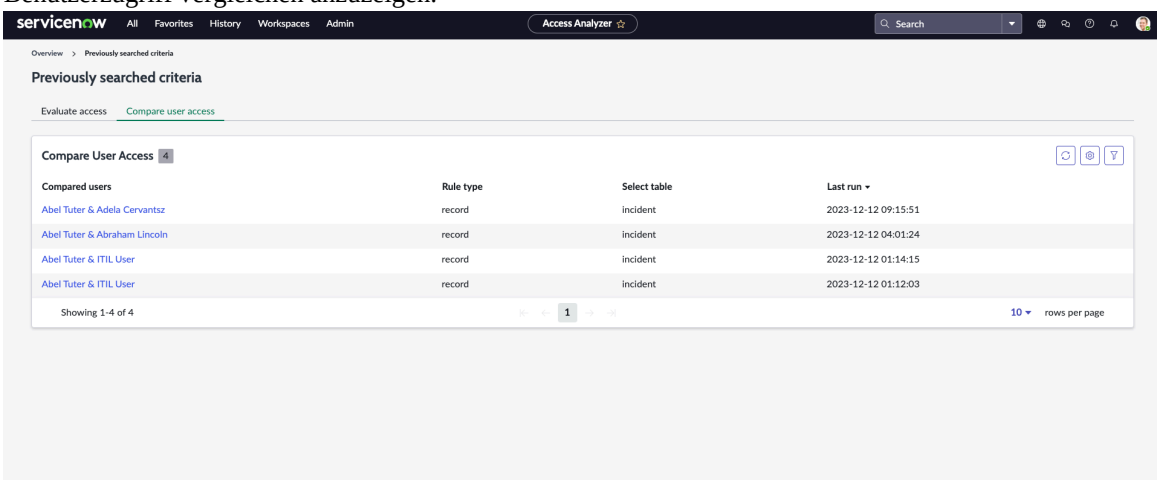


2. Klicken Sie auf die Links **Analysiert nach**, um zuvor gesuchte Kriterien im Abschnitt „Zugriff evaluieren“ anzuzeigen.



Sie können Zugriff für den Benutzer **erneut analysieren** auswählen. Exportieren Sie die Details mit der Option **Exportieren**.

3. Wählen Sie die Links **Benutzer verglichen** aus, um die zuvor durchsuchten Kriterien im Abschnitt Benutzerzugriff vergleichen anzuzeigen.



Berechtigungsauswertung

Berechtigungsauswertungskriterien bei Verwendung der Zugriffsanalyse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswertungshierarchie

Die Berechtigung für den ausgewählten Benutzer, die Gruppe oder die Rolle wird in der folgenden Hierarchie ausgewertet:

- Geschäftsregel: Eine Geschäftsregel ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder wenn eine Tabelle abgefragt wird.
- Zugriffs-Handler: Eine interne Systemprüfung mit verstecktem Quellcode auf der Plattform.
- Datenfilterung: Datenfilter sind eine Form der Zugriffskontrolle, die auf die vorhandenen Zugriffskontrollregeln (ACLs) in Ihrer Instanz abgestimmt ist. Datenfilter unterstützen nur Lesevorgänge.
- Zugriffskontrollliste (ACL): Regeln für Zugriffskontrolllisten (ACLs) schränken den Zugriff auf Daten ein, indem Benutzer eine Reihe von Anforderungen erfüllen müssen, bevor sie mit ihnen interagieren können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet:
  - Rolle
  - Sicherheitsattribut
  - Bedingung
  - Skript

Sie können den Zugriff und die Berechtigungen für den ausgewählten Benutzer, die ausgewählte Rolle oder die ausgewählte Gruppe mit der Zugriffsanalyse analysieren. Die Berechtigungen werden basierend auf den folgenden Regeltypen ausgewertet:

- **Auswertung auf Tabellenebene**: Rollen- und Sicherheitsattribut-ACLs werden für die Auswertung auf Tabellenebene verwendet.
- **Auswertung auf Datensatz- oder Feldebene**: ACLs auf Rollen-, Sicherheitsattribut-, Bedingungs- und Skriptebene werden für die Auswertung auf Datensatz- oder Feldebene verwendet.
- **UI-Seite**: Nur bereite Vorgänge werden unterstützt. Nur ACLs auf Leseebene werden ausgewertet.
- **REST-Endpunkt**: Unterstützt nur Ausführungsvorgänge. Nur ACLs auf Ausführungsebene werden ausgewertet.

Details zu den wichtigen Feldern in den Zugriffsergebnissen:

- Vorhandensein eines Skripts
- Auf die Ergebnislegende zugreifen
- Auswertungsvorgang
- IAccessHandlers
- Datenfilter
- Regeln der Zugriffssteuerungsliste

Vorhandensein eines Skripts

Das Warnsymbol weist in jedem Status auf das Vorhandensein eines Skripts in der ACL hin. Überprüfen Sie die hervorgehobenen ACLs, um den endgültigen Zugriff zu verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zur Auswertung dieser Steuerungen und zur Überprüfung der Logik zur Bestimmung des Zugriffs finden Sie unter Zugriffsanalyse-Debug-Protokolle.

Legende in der Zugriffsanalyse

Bei der Analyse des Zugriffs und der Berechtigungen werden Legenden als Teil des Bewertungsprozesses angezeigt. Im Folgenden finden Sie die Legenden:

- [Bestanden] Zugriff gewährt
- [Blockiert] Zugriff verweigert
- [Übersprungen] Wurde nicht ausgewertet
- [Nicht definiert] Keine Regel gefunden

Auswertungsvorgang

Der Evaluierungsprozess wird durchgeführt, indem die Identität eines Benutzers angenommen und die Berechtigung der Zugriffssteuerungsliste (ACL) für die Ressource bestimmt wird. Berechtigungsregeln ermöglichen den Zugriff auf die angegebene Ressource, wenn die folgenden Prüfungen als „wahr“ ausgewertet werden:

- IAccessHandlers müssen als „Bestanden“ ausgewertet werden oder sind leer oder undefiniert
- Datenfilter müssen als „Bestanden“ ausgewertet werden oder sind leer oder nicht definiert
- Zugriffskontrollregeln (ACLs) werden als „Bestanden“ ausgewertet.

IAccessHandlers

Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet.

Sie können die IAccessHandler-Prüfungen nicht ändern. Beispielsweise wird eine IAccessHandler-Implementierung für Zugriffsprüfungen für Anwendungsressourcen wie Lesezugriff verwendet.

Datenfilter

Der Datenfilter ist eine Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist.

Regeln der Zugriffssteuerungsliste

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Benutzern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Häufige Fragen

Häufig gestellte Fragen bei der Verwendung der Zugriffsanalyse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Evaluiert den Zugriff

Im Folgenden sind einige der häufig gestellten Fragen aufgeführt, die bei der Verwendung der Funktion „Zugriff evaluieren“ in der Zugriffsanalyse häufig gestellt werden:

Häufige Fragen

Fragen	Erklärung
Wie werden die von der Zugriffsanalyse angezeigten Bewertungsergebnisse gelesen?	Jede Zeile stellt eine einzelne Zugriffssteuerungsliste (ACL) dar. Die Sequenz (#) in der Reihenfolge, in der ACLs ausgewertet werden, ergibt. Der Status gibt an, ob der Gesamtzugriff gewährt (bestanden) oder verweigert (blockiert) wird.
Wie werden ACLs ausgewertet?	Auf Tabellenebene werden ACLs nur für Rollen und Sicherheitsattribute ausgewertet. Bedingungen und Skripts werden nicht ausgewertet. Rollen werden zuerst ausgewertet. Wenn Rollen blockiert sind, werden Bedingungen und Skripts übersprungen. Weitere Informationen finden Sie unter Konfigurieren einer ACL-Regel.
Wie lauten die Legenden in der Zugriffsanalyse?	Bei der Analyse des Zugriffs und der Berechtigungen werden Legenden als Teil des Bewertungsprozesses angezeigt. Im Folgenden sind die Legenden aufgeführt: • [Bestanden] Zugriff gewährt • [Blockiert] Zugriff verweigert • [Übersprungen] Wurde nicht ausgewertet • [Nicht definiert] Keine Regel gefunden
Was bedeutet das Warnungssymbol in den Access-Ergebnissen?	Das Warnsymbol weist in jedem Status auf das Vorhandensein eines Skripts in der ACL hin. Überprüfen Sie die hervorgehobenen ACLs, um den endgültigen Zugriff zu verstehen. Weitere Informationen zur Auswertung dieser Steuerungen und zur Überprüfung der Logik zur Bestimmung des Zugriffs finden Sie unter Zugriffsanalyse-Debug-Protokolle.
Was ist **IAccesshandler**?	Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. Es handelt sich um eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen (Fortsetzung)

Fragen	Erklärung
	Systemsicherheitsprüfung, die Sie nicht ändern können. **IAccessHandler** kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn dieser **IAccessHandler** ignoriert wird, werden die ACLs ausgewertet. Sie können die **IAccessHandler-**Prüfungen in keiner Weise ändern. Beispielsweise wird eine **IAccessHandler** -Implementierung für Zugriffsprüfungen auf Anwendungsressourcen wie schreibgeschützten Zugriff verwendet.
Was sind Datenfilter?	Datenfilter sind eine Form der Zugriffskontrolle, die auf die vorhandenen Zugriffskontrollregeln (ACLs) in Ihrer Instanz abgestimmt ist.
Was ist eine ACL-Regel?	Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Benutzern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Zeitlich begrenzte Rollenzuweisungen für den Benutzer gefunden, aufgrund derer die Ergebnisse beeinflusst werden können. Sie können die dem Benutzer zugewiesenen zeitlich begrenzten Rollen hier überprüfen.

Benutzerdatensätze vergleichen

Im Folgenden sind einige der häufig gestellten Fragen aufgeführt, die bei der Verwendung der Funktion „Benutzerdatensatz vergleichen“ in der Zugriffsanalyse häufig gestellt werden:

Häufige Fragen

Fragen	Erklärung
Wie werden die Ergebnisse auf der Registerkarte „Details“ gelesen?	Auf der Registerkarte Details werden die Metadaten angezeigt, die Benutzer 1 und Benutzer 2 zugeordnet sind
Wie erteile ich einem Benutzer eine Rolle?	Auf der Registerkarte Benutzer können Sie die Rolle überprüfen, die dem Benutzer gewährt werden muss, und diese Rolle zuweisen.
Wie füge ich einen Benutzer zu einer Gruppe hinzu?	Auf der Registerkarte Gruppen können Sie die Gruppe überprüfen, der der Benutzer hinzugefügt werden muss, und den Benutzer der Gruppe hinzufügen.
Was ist „Nur Unterschiede anzeigen“?	Wenn Sie das Kontrollkästchen Nur Unterschiede anzeigen aktivieren, werden nur die Rollen oder Gruppen angezeigt, die sich zwischen Benutzer 1 und Benutzer 2 unterscheiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleichen Sie den Benutzerzugriff

Im Folgenden sind einige der häufig gestellten Fragen aufgeführt, die bei der Verwendung der Funktion „Benutzerzugriff vergleichen“ in der Zugriffsanalyse häufig gestellt werden:

Häufige Fragen

Fragen	Erklärung
Wie werden die Ergebnisse auf der Vergleichsseite der Zugriffskontrolle gelesen?	Auf der Vergleichsseite der Zugriffssteuerung werden die Bewertungsstatus für verschiedene ACL-Vorgänge angezeigt.
Was sind die verschiedenen Evaluierungsstatus?	Beim Vergleich der Zugriffskontrollen zwischen den Benutzern sind die verschiedenen Auswertungsstatus: • Bestanden • Blockiert
Was bedeutet „Nur Unterschiede anzeigen“?	Wenn Sie das Kontrollkästchen Nur Unterschiede anzeigen aktivieren, wird nur der Auswertungsstatus des Vorgangs angezeigt, der sich zwischen Benutzer 1 und Benutzer 2 unterscheidet.
Wie wird der ACL-Vorgang ausgewertet?	Die Zugriffssteuerungsliste (ACL) ist die Regel für Zugriffssteuerungslisten (ACLs), die den Zugriff auf Daten einschränken, indem Benutzer eine Reihe von Anforderungen erfüllen müssen, bevor sie mit ihnen interagieren können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet: • Rolle • Sicherheitsattribut • Bedingung • Skript
Wie werden die Ergebnisse auf der Seite mit der angezeigten Rollenhierarchie gelesen?	Auf der Seite mit der Rollenhierarchie wird die Rolle angezeigt, die Benutzer 1 und Benutzer 2 zugewiesen ist. Sie können die Rolle verstehen, die für den Benutzer für einen bestimmten ACL-Vorgang erforderlich ist.
Wie kann ich die Details des Anwenders anzeigen?	Sie können auswählen **Benutzer (Knoten)** > **Weitere Aktionen** > **Benutzer anzeigen** Details, um mehr über den Benutzer zu erfahren.
Wie kann ich die Details der Rolle anzeigen?	Sie können auswählen **Rolle (Knoten)** > **Weitere Aktionen** > **Rolle anzeigen** Details, um mehr über die Rolle zu erfahren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen (Fortsetzung)

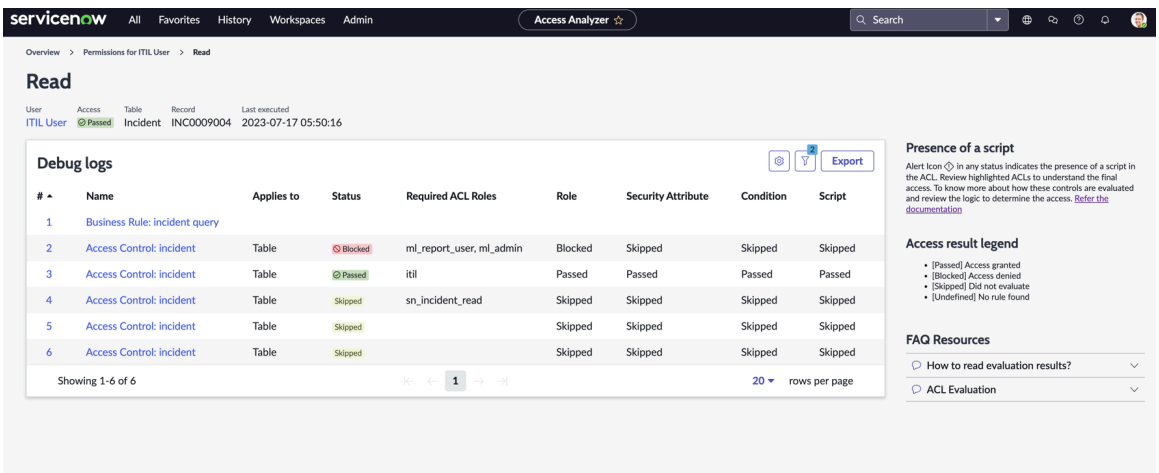
Fragen	Erklärung
Wie kann ich die Details der Ressourcen anzeigen, auf die die Rolle zugreifen kann?	Sie können auswählen **Rolle (Knoten)** > **Weitere Aktionen** > **Zeigen Sie alle Ressourcen an, auf die die Rolle Zugriff hat** , um zu erfahren, auf welche Ressourcen die Rolle zugreifen kann.
Wie kann ich die Details der Gruppe anzeigen?	Sie können auswählen **Gruppe (Knoten)** > **Weitere Aktionen** > **Gruppe anzeigen** Details, um mehr über die Gruppe zu erfahren.

Zugriffsanalyse-Debug-Protokolle

Debug-Protokolle zeigen die Details des Vorgangs zum Auswählen des Zugriffsergebnisses an.

Felder in Debug-Protokollen

Die Debug-Protokolle in der Zugriffsanalyse zeigen Informationen zum ausgewählten Vorgang an, um die mit dem Vorgang verknüpften Berechtigungen, Geschäftsregeln und ACLs zu verstehen.



Im Folgenden finden Sie die Felder und ihre Beschreibung in den Debug-Protokollen:

Protokolle debuggen

Felder	Beschreibung
Name	Die Details zur Business Rule oder ACL. Sie können die Geschäftsregel der ACL auswählen, um weitere Informationen zu erhalten.
Betrifft	Die Details zur Anwendung der ACL auf Feld-, Datensatz- oder Tabellenebene.
Status	Status der ACL für die zugeordnete Rolle und Berechtigung.
Erfordert ACL	Die Rolle, die für den Zugriff auf das Feld, den Datensatz oder die Tabelle erforderlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolle debuggen (Fortsetzung)

Felder	Beschreibung
Rolle	Die Details zur Rolle „Blockiert“, „Bestanden“, „Übersprungen“ für die Zugriffssteuerung.
Sicherheitsattribut	Die Details zum Sicherheitsattribut „Blockiert“, „Bestanden“, „Übersprungen“ für die Zugriffssteuerung.
Bedingung	Die Details zur Bedingung „Blockiert“, „Bestanden“, „Übersprungen“ für die Zugriffssteuerung.
Skript	Die Details zum Skript, das für die Zugriffskontrolle blockiert, bestanden und übersprungen ist.
Angepasst	Die Details zur benutzerdefinierten ACL, falls vorhanden, für die Zugriffssteuerung.
Anwendung	Status der Anwendung. Global oder Store.

Auswertungshierarchie

Die Berechtigung für den ausgewählten Benutzer, die Gruppe oder die Rolle wird in der folgenden Hierarchie ausgewertet:

- Geschäftsregel: Eine Geschäftsregel ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder wenn eine Tabelle abgefragt wird.
- Zugriffs-Handler: Eine interne Systemprüfung mit verstecktem Quellcode auf der Plattform.
- Datenfilterung: Ein Datenfilter ist eine Form der Zugriffskontrolle, die auf die vorhandenen Zugriffskontrollregeln (ACLs) in Ihrer Instanz abgestimmt ist. Datenfilter unterstützen nur Lesevorgänge.
- Zugriffskontrollliste (ACL): Regeln für Zugriffskontrolllisten (ACLs) schränken den Zugriff auf Daten ein, indem Benutzer eine Reihe von Anforderungen erfüllen müssen, bevor sie mit ihnen interagieren können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet:
  - Rolle
  - Sicherheitsattribut
  - Bedingung
  - Skript

Auswertung der Zugriffskontrollliste

ACLs für die Vorgänge werden in der folgenden Reihenfolge ausgewertet:

- Rolle
- Sicherheitsattribut
- Bedingung
- Skript

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorhandensein eines Skripts

Das Warnsymbol weist in jedem Status auf das Vorhandensein eines Skripts in der ACL hin. Überprüfen Sie die hervorgehobenen ACLs, um den endgültigen Zugriff zu verstehen.

Hinweis:
Während einer Zugriffsanalyse-Abfrage werden zuerst Business Rules und dann die Zugriffssteuerungsliste ausgeführt.

Reihenfolge der Ausführung

Die Reihenfolge der Ausführung von Zugriffsergebnissen in verschiedenen Szenarien lautet wie folgt:

- **Vorhandensein einer geerbten ACL oder Platzhalter-ACL**: Während der Ausführungssequenz werden zuerst die geerbten ACLs und dann die Platzhalter-ACL ausgewertet.
- **Eine ACL wird übergeben, die anderen werden übersprungen**: Wenn während der Ausführung und Auswertung der Berechtigung eine ACL übergeben wird, wird die Ausführung und Auswertung der anderen ACL übersprungen. Weil die allgemeine Berechtigung für den ausgewählten Vorgang erfordert, dass eine ACL auf ein Feld, einen Datensatz oder eine Tabelle für eine Identität zugreift.
- Ausführung von ACLs auf Feld-**und Tabellenebene**: Während der Ausführung werden zuerst ACLs auf Feldebene ausgeführt, gefolgt von der ACL auf Tabellenebene, um bei der Analyse des Zugriffs für eine Identität detailliertere Ergebnisse zu liefern.
- **Auswertung in Anwesenheit einer geskripteten ACL**: Wenn ein Skript vorhanden ist, wird der Gesamtzugriff für den Vorgang mit einem Warnsymbol übergeben, um das Skript in der ACL anzuzeigen.

Globale Identität

Global Identity ist ein Produkt von ServiceNow®, mit dem eindeutige Benutzer über mehrere Instanzen hinweg identifiziert werden können.

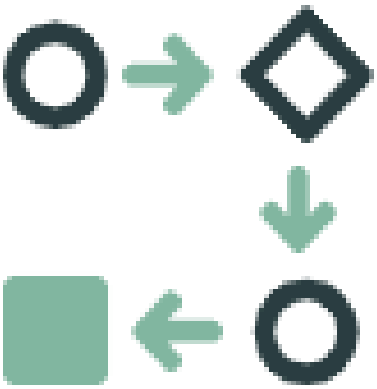
Globale Identität hilft bei mehreren ServiceNow® -Instanzen, um Benutzer, ihre Attribute und andere grundlegende Daten über mehrere ServiceNow® -Instanzen hinweg zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen Sie die Verbund-ID

Machen Sie sich mit den wichtigsten Funktionen und dem Geschäftsnutzen von Verbund-IDs vertraut.

Zugriff auf Verbund-ID



Greifen Sie auf die Verbund-ID zu.

ID-Felder werden aktualisiert

Aktualisieren und richten Sie die Verbund-ID ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbund-ID wird untersucht

Bestimmen Sie die Benutzer in mehreren Instanzen basierend auf Benutzername und E-Mail-Adresse, und stellen Sie dem Benutzer in allen Instanzen eine eindeutige ID (Verbund-ID) bereit.

Die föderierte ID wird verwendet, um Benutzer in mehreren Instanzen von ServiceNow® zu identifizieren. Anhand der Verbund-ID kann der Benutzer identifiziert und die genaue Anzahl der Benutzer in mehreren Instanzen bestimmt werden. Weitere Informationen finden Sie unter Verbund-ID.

Hinweis:
Benutzername ist zum Generieren von Verbund-IDs erforderlich.

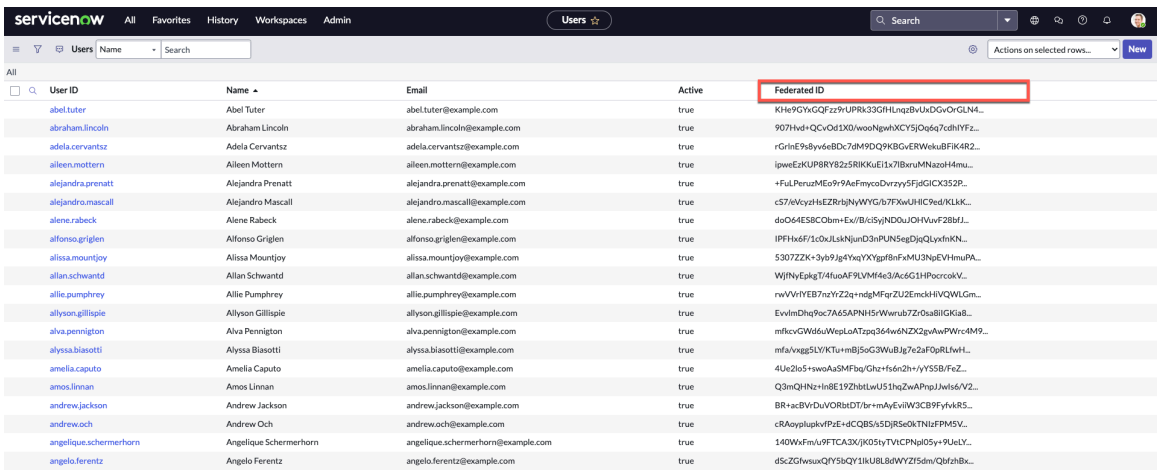
Die Föderierte ID ist ein eindeutiger Bezeichner für eine Identität, der eine Hashing-Funktion für die ServiceNow® Instanzen verwendet.

Durch die Verwendung der **Benutzer-ID** und der E- **Mail** -Adresse des Benutzers in allen Instanzen wird die Verbund-ID erstellt und in der Tabelle „sys_user“ angezeigt.

Nach dem Upgrade auf das Release Washington DC wird das Plugin „Federated ID Generation“ (com.glide.identity.globalid) automatisch auf allen Instanzen installiert.

Hinweis:

- Benutzername ist zum Generieren von Verbund-IDs erforderlich.
- Benutzername und E-Mail-Adresse werden standardmäßig zum Generieren von Verbund-IDs verwendet. Informationen zum Aktualisieren der Felder zum Generieren von Verbund-IDs basierend auf Ihren Anforderungen finden Sie unter ID-Felder werden aktualisiert.
- Die Rolle**Iamsync_admin** ist erforderlich, um die Konfiguration zu aktualisieren.
- Wenn Benutzer mit doppelten Benutzernamen und E-Mail-Adressen vorhanden sind, wird die Verbund-ID nur für einen Benutzer generiert. Wenn der Benutzername NULL oder leer ist, ist die Verbund-ID NULL.



Schemaänderungen nach der Installation des Plugins:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Neue Spalte federated_id in der Tabelle „sys_user“ wird erstellt.
- Neue Tabelle – „iamsync_type“ wird automatisch mit der Standardkonfiguration für die Tabelle „sys_user“ ausgefüllt.

Die föderierte ID wird nur für die Tabelle „sys_user“ und alle Tabellen unterstützt, die die Tabelle „sys_user“ erweitern.

Nach dem Upgrade auf das Release Washington DC wird das Plugin „Federated ID Generation“ (com.glide.identity.globalid) automatisch auf allen Instanzen installiert.

Zugriff auf Kriterien für föderierte IDs

Greifen Sie auf die Kriterien der föderierten ID zu, um mehr über die ID-Felder zu erfahren, die zum Generieren der föderierten ID verwendet werden.

Vorbereitungen

Erforderliche Rolle: iamsync_admin

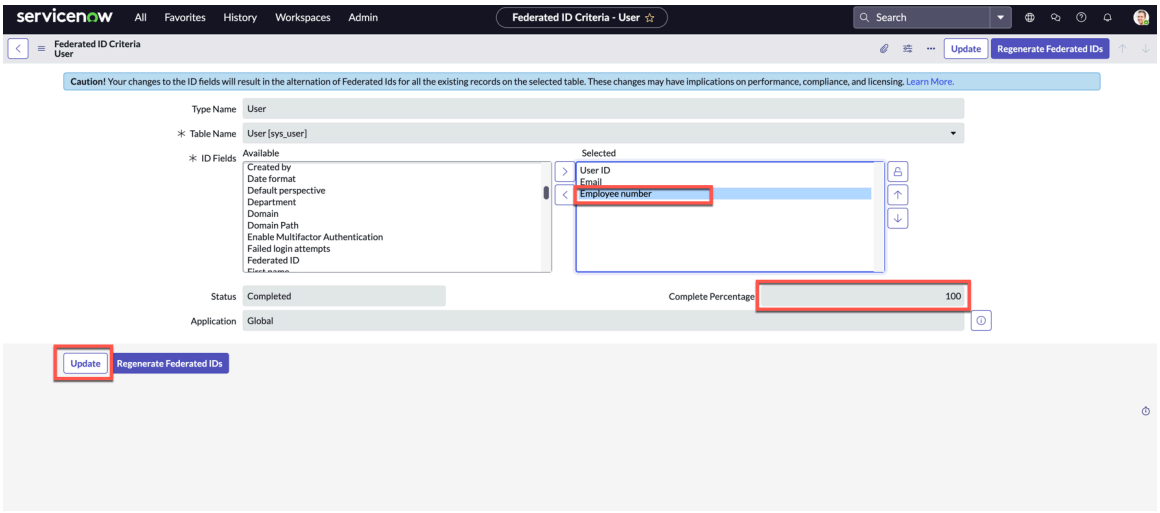
Prozedur

1. Navigieren zu **Alle** > **Verbund-ID verwalten** > **Kriterien für Verbund-ID**.
2. Auf der Seite „Kriterien für föderierte ID“ wird der Datensatz mit den folgenden Details angezeigt:
   - Typname: **Benutzer**
   - Tabellenname: **Benutzer [sys_user]**
   - ID-Felder: **user_name (Benutzer-ID), E-Mail** (Standardfelder, die für die Generierung der Verbund-ID verwendet werden).
   - Status: **Abgeschlossen** (Status der föderierten ID-Generierung). Verfügbare Status: **Bereit**, **Wird ausgeführt**, **Abgeschlossen**, **Fehler**.

Hinweis:

- Benutzername ist zum Generieren von Verbund-IDs erforderlich.
- Benutzername und E-Mail-Adresse werden standardmäßig zum Generieren von Verbund-IDs verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Nur die ID-Felder können aktualisiert werden, um eine neue Verbund-ID für die vorhandenen Datensätze zu generieren. Weitere Informationen finden Sie unter ID-Felder werden aktualisiert.

ID-Felder werden aktualisiert

Aktualisieren Sie die ID-Felder, um die Verbund-IDs basierend auf den aktualisierten Feldern neu zu generieren.

Vorbereitungen

Erforderliche Rolle: iamsync_admin

Hinweis:
Alle Änderungen an den ID-Feldern führen zu einer Änderung der Verbund-IDs für alle vorhandenen Datensätze in der ausgewählten Tabelle. Diese Änderungen können Auswirkungen auf Leistung, Compliance und Lizenzierung haben.

Prozedur

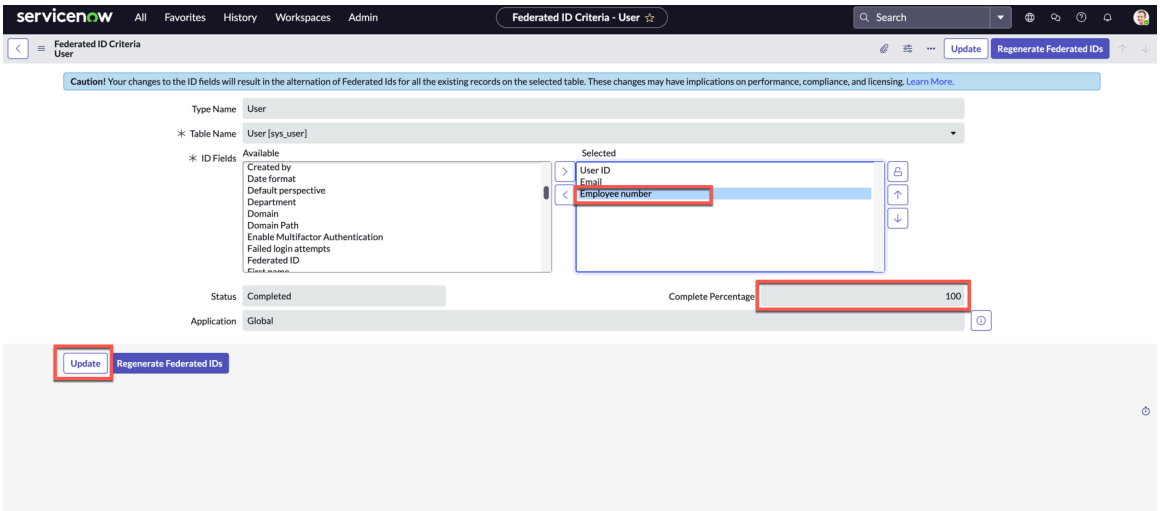
1. Navigieren zu **Alle** > **Verbund-ID verwalten** > **Kriterien für Verbund-ID**.
2. Wählen Sie den Typnamen (**Benutzer**) aus.
3. Wählen Sie die neuen ID-Felder auf der Seite „Anwender der föderierten ID-Kriterien“, die Sie hinzufügen möchten, mithilfe der Pfeilschaltflächen von „Verfügbar“ zu „Ausgewählt“ aus.

   Beispiel: **Mitarbeiternummer**.

Hinweis:

- Benutzername ist zum Generieren von Verbund-IDs erforderlich.
- Benutzername und E-Mail-Adresse werden standardmäßig zum Generieren von Verbund-IDs verwendet.
- Wenn Benutzer mit doppelten Benutzernamen und E-Mail-Adressen vorhanden sind, wird die Verbund-ID nur für einen Benutzer generiert. Wenn der Benutzername NULL oder leer ist, ist die Verbund-ID NULL.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Jetzt wird die ausgewählte **Mitarbeiternummer** zu einem weiteren Attribut für die Generierung der Verbund-ID.

4. Wählen Sie **Aktualisieren** aus, um Verbund-IDs zu generieren.

   Hinweis:
   Wählen Sie zuerst **Aktualisieren** aus, und überprüfen Sie dann den Prozentsatz der Fertigstellung (100), bevor Sie ein weiteres Update initiieren.

   Der Statusprozentsatz gibt die Generierung der Verbund-ID für alle Identitäten in Instanzen an.

   Hinweis:
   - Ändern Sie das Feld nicht, bis der vorherige Aktualisierungsauftrag abgeschlossen ist.
   - Felder, die aktualisiert werden, müssen vom Typ „Zeichenfolge“ sein.
   - Folgende Felder können nicht als ID-Felder ausgewählt werden:
     - Felder auf Systemebene
     - Edge Encryption-Felder
     - Passwortfelder.

5. Navigieren Sie zur Tabelle sys_user, um die neuen Verbund-IDs anzuzeigen, die aufgrund der Aktualisierung der ID-Felder generiert werden.

   Hinweis:
   Wählen Sie Verbund- **IDs erneut generieren** aus, wenn ein Benutzer über XML-Importe, Datenbankaktualisierungen auf niedriger Ebene oder eine nicht ordnungsgemäß funktionierende Instanz erstellt oder aktualisiert wird. Wenn Sie Verbund- **IDs**erneut generieren auswählen, werden die IDs für alle Benutzer unter Verwendung der aktuellen ID-Feldkriterien neu generiert.

Identitäts- und Zugriffsaudit

Verwenden Sie das Identitäts- und Zugriffsaudit, um Änderungen an Benutzern, Gruppen, Rollen und ACLs zu verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Identity and Access Audit.

Konfigurieren

Machen Sie sich mit der Konfiguration von Identity and Access Audit vertraut.

Audit-Ergebnisse

Zeigen Sie die Ergebnisse des Identitäts- und Zugriffsaudits an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identitäts- und Zugriffsaudit erkunden

Verwenden Sie das Identitäts- und Zugriffsaudit, um Änderungen an Benutzern, Gruppen, Rollen und ACLs zu verstehen.

Identity and Access Audit hilft, die kritischen Informationen darüber zu verstehen, wer was, wo und wann in Benutzerkonten, Gruppen und Rollen geändert hat.

Hilft bei der Erkennung böswilliger Benutzer und der Nachverfolgung ungewöhnlicher Aktivitäten in der Instanz ServiceNow® sowie bei der Einhaltung von Compliance-Standards für die Nachverfolgung von Zugriffsänderungen.

Identity and Access Audit (Identity Security Audit) ist ein Plugin (com.glide.security.audit), das automatisch installiert wird.

Die Audit-Funktion kann durch Umschalten der Systemeigenschaft „glide.identity.security.audit.enabled “ ein- oder ausgeschaltet werden. Standardmäßig ist die Eigenschaft auf truefestgelegt.

Mit Identity and Access Audit können Sie:

- Zeigen Sie die Änderungen an, die in den letzten 30 Tagen an Benutzern, Gruppen, Rollen-ACL-Attributen, Rollenmitgliedschaften, Gruppenmitgliedschaften und ACL-Rollen vorgenommen wurden.
- Verfolgen Sie die Änderungen in Ihrer ServiceNow -Instanz nach.
- Helfen Sie, potenzielle Sicherheitsrisiken und regulatorische Risiken zu minimieren.
- Nachweis der Compliance mit Auditoren für verschiedene Gruppen innerhalb der Organisation.
- Zeigen Sie, dass die Organisation nicht angreifbar für Bedrohungen im Zusammenhang mit fehlender Transparenz der Benutzergruppe und Rollenänderungen ist.

Benutzerpersonas in Identitätszugriff und Audit

Im Folgenden sind die verschiedenen Benutzerpersonas in Identity and Access Audit aufgeführt:

- **Administrator**: Zeigen Sie die Audit-Datensätze und die Konfiguration an
- **Sicherheitsadministrator**: Zeigen Sie diese Audit Trails an. Ändern Sie die Konfiguration, um die Prüfung für eine bestimmte Tabelle zu aktivieren oder zu deaktivieren, oder ändern Sie die geprüften Felder.

Audit-Tabellen

Die folgenden Tabellen können mit Identity and Access Audit geprüft werden:

- Gruppe [sys_user_group]
- Rolle [sys_user_role].
- Zugriffskontrolle [sys_security_acl].
- Benutzer [sys_user]
- Gruppenrolle [sys_group_has_role].
- Benutzerrolle [sys_user_has_role].
- Zugriffsrollen [sys_security_acl_role].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember].

Module im Identitäts- und Zugriffsaudit

Identity and Access Audit verfügt über die folgenden Module in der Instanz ServiceNow :

Modul	Beschreibung
Audit-Ergebnisse	Zeigt die Audits an, die in der Instanz ServiceNow aufgetreten sind.
Konfigurieren Sie Tabelle und Felder	Konfigurieren Sie die Systemtabellen und -felder mit den verfügbaren Feldern aus dem Identitäts- und Zugriffsaudit.
Aufbewahrungszeitraum konfigurieren	Konfigurieren Sie die Aufbewahrungsdauer der geprüften Daten. Der maximale Zeitraum, der festgelegt werden kann, beträgt 30 Tage.
Benutzerpfade	Zeigt Audits von Benutzern an.
Gruppenpfade	Zeigt Audits von Gruppen an.
Rollenpfade	Zeigt Audits von Rollen an.
ACL-Pfade	Zeigt Audits von ACLs an.

Audit-Ergebnisse

Zeigt Audits an, die in der Instanz ServiceNow® aufgetreten sind.

Audit-Ergebnisse zeigt Änderungen an, die für Benutzer, Gruppen, Rollen und ACLs in der Instanz ServiceNow vorgenommen wurden.

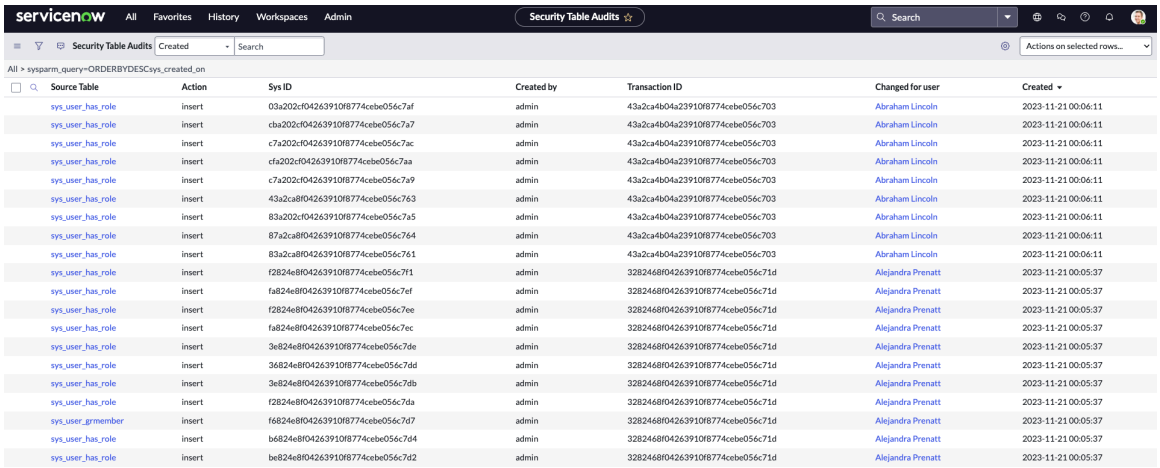
Um auf die Audit-Ergebnisse zuzugreifen, navigieren Sie **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Audit-Ergebnisse**. Die Seite Sicherheitstabellen-Audits wird mit den folgenden Informationen angezeigt.

Sicherheitstabellen-Audits

Spaltenname	Beschreibung
Quelltabelle	Details der Quelltabelle, in der das Audit aufgetreten ist.
Aktion	Beschreibt die Audit-Aktion.
Sys_id	Details zur sys_id für den geprüften Datensatz.
Erstellt von	Details des Audits, das von erstellt wurde.
Transaktion-ID	Eine eindeutige ID, die jede Aktion für das jeweilige durchgeführte Audit darstellt.
Für Benutzer geändert	Name des Benutzers, wenn das Audit durchgeführt wurde.
Erstellt	Uhrzeit und Datum, an dem das Audit durchgeführt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Benutzerpfade

Zeigt Audits von Benutzern in der Instanz ServiceNow® an.

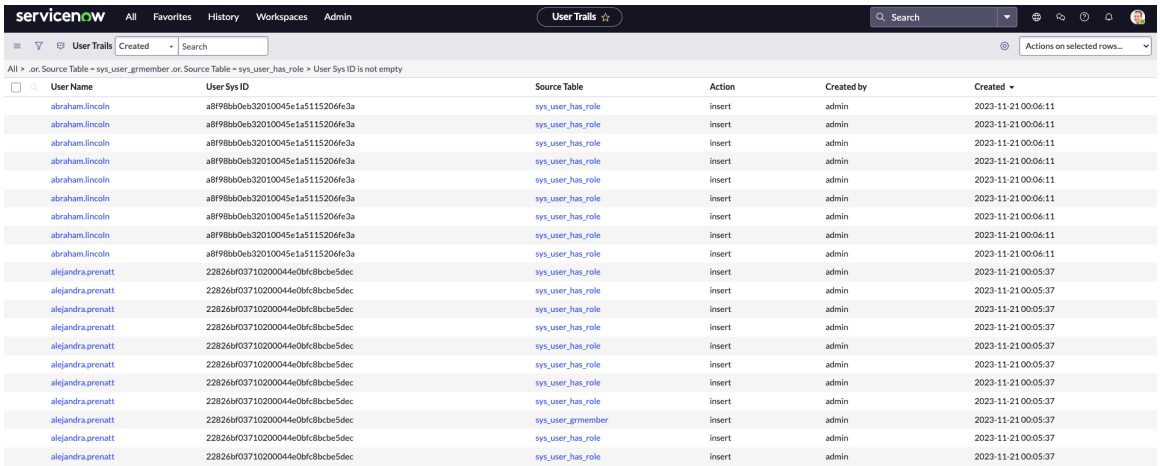
Benutzerpfade zeigen Änderungen an Identitätsattributen, Rollenmitgliedschaften und Gruppenmitgliedschaften für einen Benutzer an.

Um auf User Trails zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Benutzerpfade**. Die Seite „Benutzerpfade“ wird mit den folgenden Informationen angezeigt.

Benutzerpfade

Benutzername	Der Name des Benutzers.
Benutzer-Sys-ID	Details zur Benutzer-sys_id für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Benutzer, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum, an dem das Audit durchgeführt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Gruppenpfade

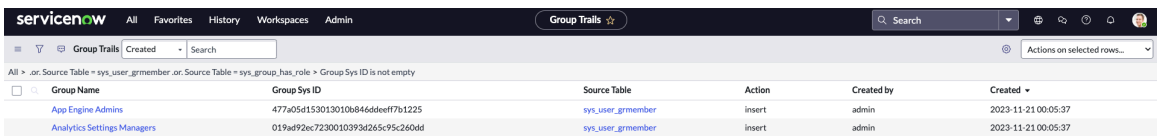
Zeigt Audits von Gruppen in der Instanz ServiceNow® an.

Gruppenpfade zeigen Attributänderungen, Mitgliedschaftsänderungen und Rollenänderungen für eine Gruppe an.

Um auf Gruppenpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Gruppenpfade**. Die Seite „Gruppenpfade“ wird mit den folgenden Informationen angezeigt.

Gruppenpfade

Gruppenname	Name der Gruppe.
Gruppen-Sys-ID	Details zur sys_id der Gruppe für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Benutzer, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum, an dem das Audit durchgeführt wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenpfade

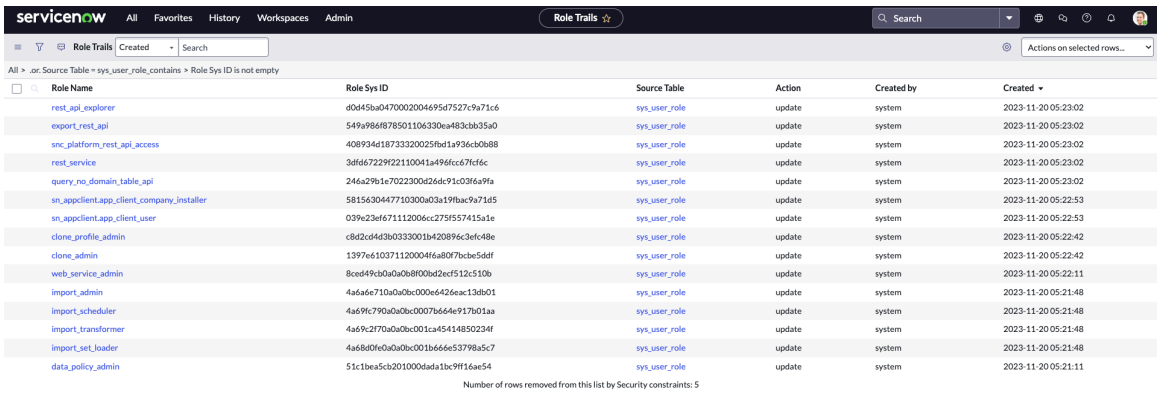
Zeigt Audits von Rollen in der Instanz ServiceNow® an.

Rollenpfade zeigen Attributänderungen und Änderungen der Übergeordnet-Untergeordnet-Beziehung für eine Rolle an.

Um auf Rollenpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Rollenpfade**. Die Seite „Rollenpfade“ wird mit den folgenden Informationen angezeigt.

Rollenpfade

Rollenname	Name der Rolle.
Sys-ID der Rolle	Details zur sys_id der Rolle für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Benutzer, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum, an dem das Audit durchgeführt wurde.



ACL-Pfade

Zeigt Audits von ACLs in der Instanz ServiceNow® an.

ACL-Pfade zeigen Attributänderungen und erforderliche Rollenbeziehungsänderungen für eine ACL an.

Um auf die ACL-Pfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **ACL-Pfade**. Die Seite „ACL-Pfade“ wird mit den folgenden Informationen angezeigt.

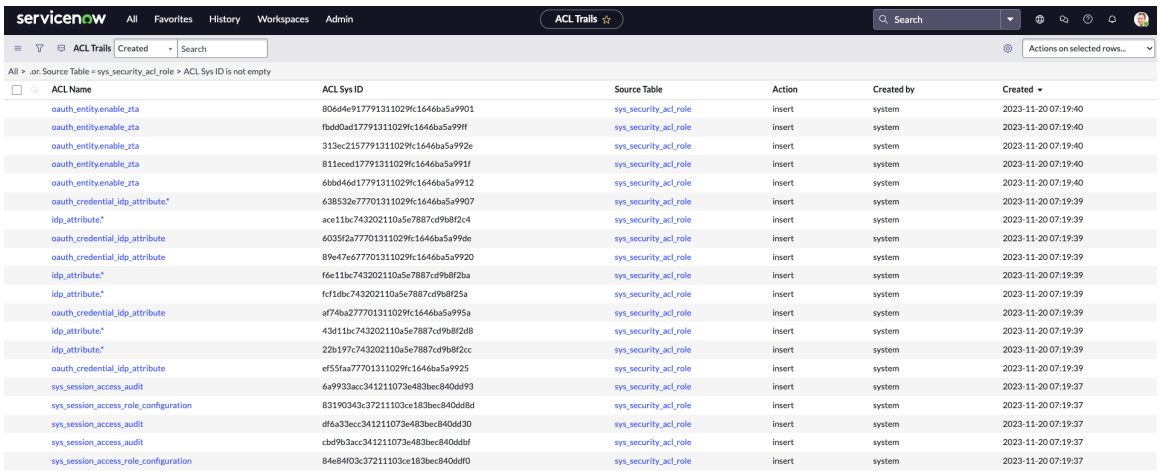
ACL-Pfade

ACL-Name	Name der ACL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Pfade (Fortsetzung)

ACL-Sys-ID	Details zur ACL-sys_id für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Benutzer, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum, an dem das Audit durchgeführt wurde.



Prüfbare Felder für Sicherheit

Zeigt Details auf Tabellen- und Feldebene an, die in der Instanz ServiceNow® geprüft werden.

Prüfbare Sicherheitsfelder zeigt die Details der Tabellen und Felder an, die in der Instanz ServiceNow geprüft werden.

Um auf die Seite „Überprüfbare Sicherheitsfelder“ zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Tabellen und Felder konfigurieren**. Die Seite „Überprüfbare Sicherheitsfelder“ wird mit den folgenden Informationen angezeigt.

Prüfbare Felder für Sicherheit

Spaltenname	Beschreibung
Zu prüfende Tabelle	Details der geprüften Tabelle.
Audit-Speicherziel	Details des Ziels, in dem die Audit-Details gespeichert werden.
Feldliste	Auditing wird für in der Liste angegebene Felder durchgeführt.
Erstellen	Überprüft die Änderungen, die sich auf den Erstellungsvorgang beziehen.
Aktualisieren	Überprüft die Änderungen, die sich auf den Aktualisierungsvorgang beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfbare Felder für Sicherheit (Fortsetzung)

Spaltenname	Beschreibung
Löschen	Überprüft die Änderungen, die sich auf den Löschvorgang beziehen.
Aktiv	Audit nur, wenn die Konfiguration für die Tabelle aktiv ist.

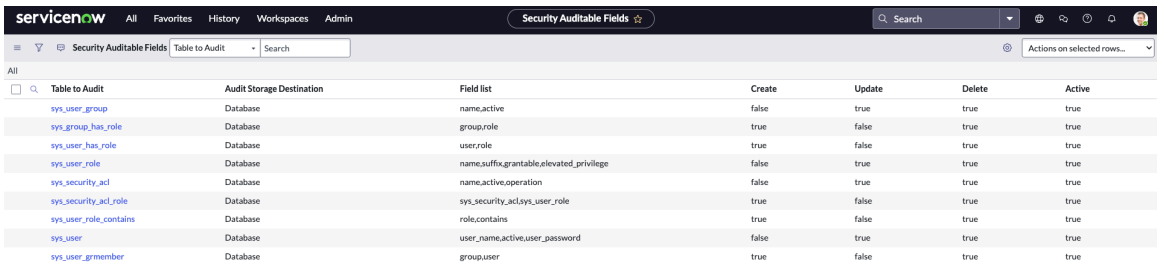


Table to Audit	Audit Storage Destination	Field list	Create	Update	Delete	Active
sys_user_group	Database	name,active	false	true	true	true
sys_group_has_role	Database	group,role	true	false	true	true
sys_user_has_role	Database	user,role	true	false	true	true
sys_user_role	Database	name,suffix,grantable,elevated_privilege	false	true	true	true
sys_security_acl	Database	name,active,operation	false	true	true	true
sys_security_acl_role	Database	sys_security_acl,sys_user_role	true	false	true	true
sys_user_role_contains	Database	role,contains	true	false	true	true
sys_user	Database	user_name,active,user_password	false	true	true	true
sys_user_grmember	Database	group,user	true	false	true	true

Die folgenden Tabellen können mit dem Identitäts- und Zugriffsaudit geprüft werden:

- Gruppe [sys_user_group]
- Rolle [sys_user_role].
- Zugriffskontrolle [sys_security_acl].
- Benutzer [sys_user]
- Gruppenrolle [sys_group_has_role].
- Benutzerrolle [sys_user_has_role].
- Zugriffsrollen [sys_security_acl_role].
- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember].

Tabellen und Felder konfigurieren

Identitäts- und Zugriffsaudit, um die für einen Benutzer, eine Gruppe, eine Rolle und eine ACL vorgenommenen Änderungen zu verstehen.

Vorbereitungen
Erforderliche Rolle: security_admin

Sie müssen Ihre Rolle auf Sicherheitsadministrator erhöhen, um Tabellen und Felder für Identitäts- und Zugriffsaudits zu konfigurieren.

Die folgenden Tabellen können für Audits konfiguriert werden☒

- Gruppe [sys_user_group]
- Rolle [sys_user_role].
- Zugriffskontrolle [sys_security_acl].
- Benutzer [sys_user]
- Gruppenrolle [sys_group_has_role].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

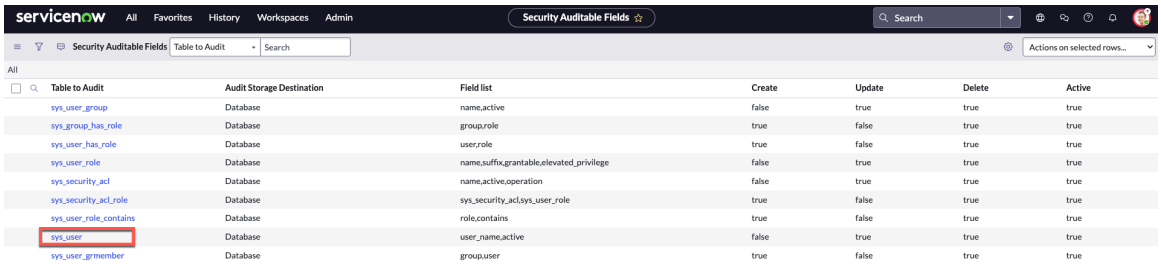
- Benutzerrolle [sys_user_has_role].
- Zugriffsrollen [sys_security_acl_role].
- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember].

Hinweis:
Informationen dazu, welche Felder für die Tabellen konfiguriert werden können, finden Sie unter Felder, die für Identitätszugriff und -audit unterstützt werden und nicht unterstützt werden.

Prozedur

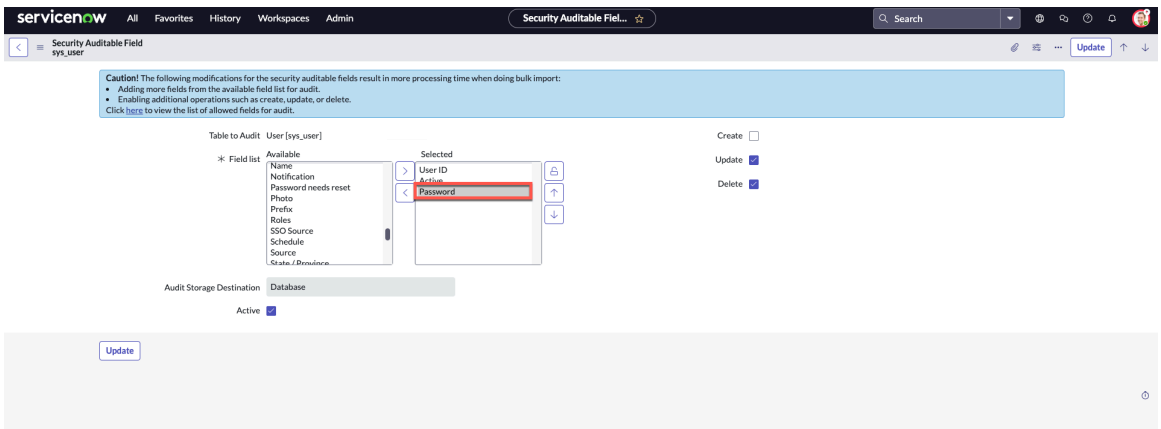
1. Navigieren zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Tabellen und Felder konfigurieren**.
2. Wählen Sie die Tabelle aus, aus der Sie ein Feld prüfen möchten.

   Beispiel: **sys_user**.



3. Fügen Sie das zu prüfende Feld hinzu.

   Beispiel: **Passwort**.



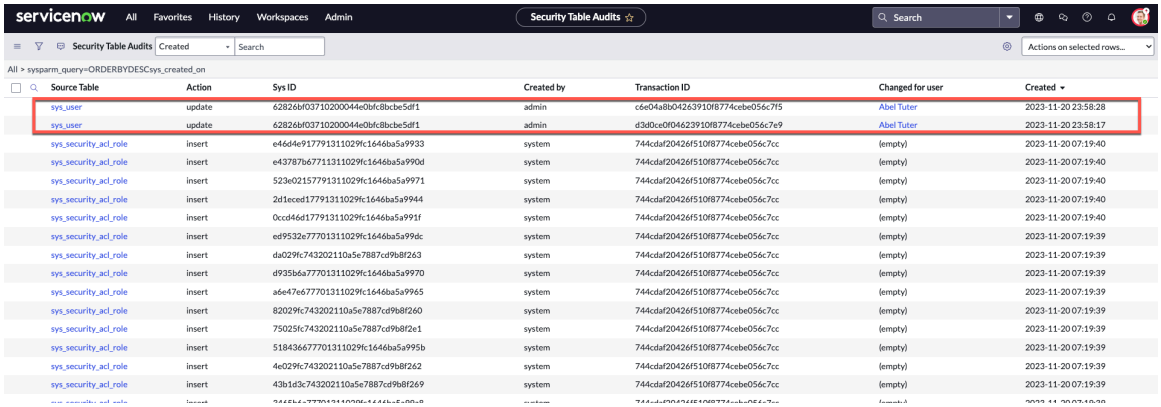
Hinweis:
Die folgenden Änderungen für die überprüfbaren Sicherheitsfelder führen zu einer höheren Verarbeitungszeit beim Massenimport:

- Hinzufügen weiterer Felder aus der Liste der verfügbaren Felder für Audit.
- Aktivieren zusätzlicher Vorgänge wie Erstellen, Aktualisieren oder Löschen.

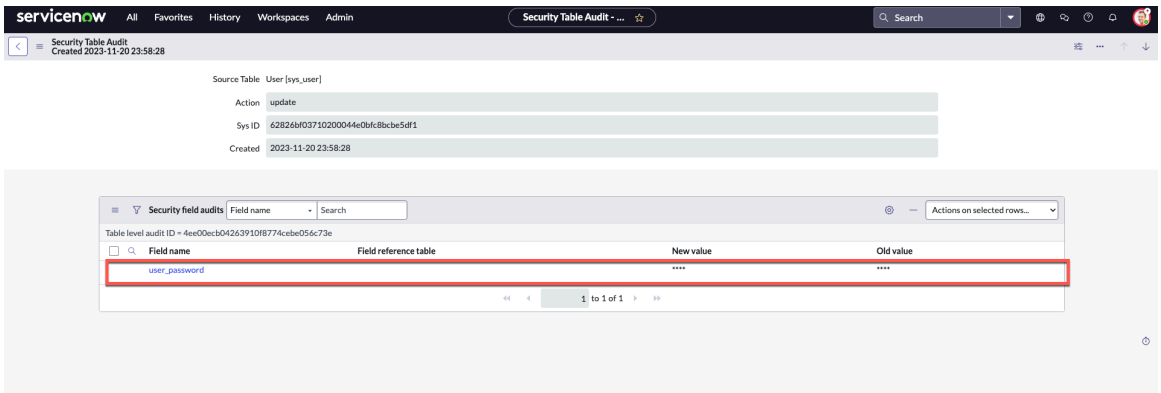
4. Aktualisieren Sie den Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Änderungen am Passwortfeld fügen einen neuen Datensatz zu den Sicherheitstabellen-Audits hinzu. In diesem Beispiel zeigt das Audit ein geändertes Passwortfeld für den Benutzer **Abel Tuter**.



Wenn Sie den erstellten Datensatz auswählen, werden die Details der Änderungen angezeigt.



Aufbewahrungszeitraum konfigurieren

Konfigurieren Sie die Aufbewahrungsdauer für Identitäts- und Zugriffsaudits.

Vorbereitungen

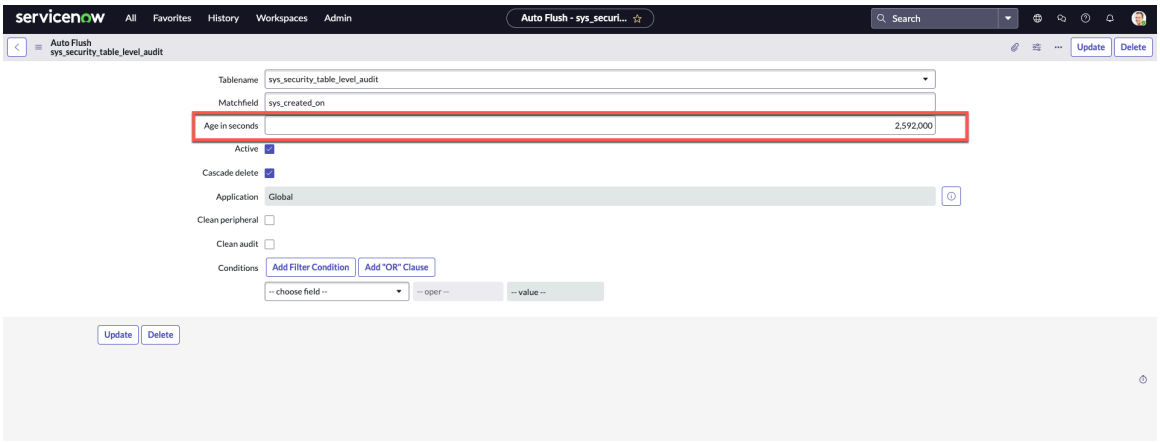
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Aufbewahrungszeitraum konfigurieren**.
2. Im Formular können Sie das Alter in Sekunden ändern.

> **Hinweis:**
> Die maximale Anzahl von Tagen für das Identitäts- und Zugriffsaudit beträgt 30 Tage (2.592.000 Sekunden).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Speichern oder aktualisieren Sie den Datensatz.

Felder, die für Identitätszugriff und -audit unterstützt werden und nicht unterstützt werden

Liste der Felder, die für Audits unterstützt werden und nicht unterstützt werden.

Die Validierung von Audit-Feldern verhindert, dass einige Felder in „field_list“ in der Tabelle „Sicherheitsfeld-Audit-Konfiguration“ (sys_sec_field_audit_config) ausgewählt werden.

Feld unterstützt oder nicht unterstützt für Audit

Tabelle	Felder unterstützt oder nicht unterstützt
Alle Tabellen	Felder, die nicht unterstützt werden: • Erstellt am (sys_created_on) • Erstellt von (sys_created_by) • Aktualisiert von (sys_updated_by) • Aktualisiert am (sys_updated_on)
Benutzer hat Rolle (sys_user_has_role)	Unterstützte Felder: • Benutzer • Rolle • Geerbt • Anzahl
Benutzer (sys_user)	Felder, die nicht unterstützt werden: • Letzte Anmeldung (last_login) • Zeit der letzten Anmeldung (last_login_time) • Letztes Anmeldegerät (last_login_device) • Multifaktor-Authentifizierung aktivieren (enable_multifactor_authn)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld unterstützt oder nicht unterstützt für Audit (Fortsetzung)

Tabelle	Felder unterstützt oder nicht unterstützt
	• Standardperspektive (default_perpektive) • Kalenderintegration (calendar_integration) • Föderierte ID (federated_id) • Passwort muss zurückgesetzt werden (password_needs_reset) • Fehlgeschlagene Versuche (failed_attempts) • Letztes Passwort (last_password) • LDAP-Server (ldap_server) • Ausgesperrt (locked_out) • Benachrichtigung (Benachrichtigung) • Rollen (roles) • Domäne (sys_domain) • Domänenpfad (sys_domain_path) • Zeitformat (time_format) • Anwender-ID mit Hash (hashed_user_id) • Klassenname (sys_class_name) • Mod-Anzahl (sys_mod_count)

Identity Center

Ermöglicht die Überwachung, Verwaltung und Minimierung identitätsbasierter Risiken und Sicherheitslücken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Machen Sie sich mit den Funktionen und dem Geschäftsnutzen von Identity Center vertraut.

Aktivieren

Machen Sie sich mit der Aktivierung von Identity Center vertraut.

Identitätsmetriken für Administratoren

Identity Center für -Benutzer

Erhalten Sie Details zu den häufig gestellten Fragen zur Zugriffsanalyse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wissen, wie die Berechtigungen ausgewertet werden.

Identity Center erkunden

Identity Center ist eine Sammlung von Benutzerattributen, Zugriff, Geräten, Anmeldeverlauf, Sicherheitsaktivitäten und vielem mehr.

Identity Center bietet Funktionen zum Überwachen, Verwalten und Minimieren identitätsbasierter Risiken und Sicherheitslücken.

Identity Center ist eine zentrale Anlaufstelle für die Überwachung, Verwaltung und Minimierung identitätsbasierter Risiken und Sicherheitslücken in ServiceNow.

Zum Aktivieren von Identity Center installieren Sie das Plugin „Identity Center“ (com.snc.identity_center). Identity Center ist für Endbenutzer verfügbar, um die Details zu aktiven Sitzungen, Anmeldeverlauf und vertrauenswürdigen Geräten mit Identity Center anzuzeigen. Weitere Informationen finden Sie unter Identity Center für -Benutzer.

Identity Center wird aktiviert

Installieren Sie für Identity Center das Plugin „Identity Center“ (com.snc.identity_center).

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Identity Center“ (com.snc.identity_center).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Identity Center für -Benutzer

Zeigen Sie mit dem Identitätscenter Details zu Ihren aktiven Sitzungen, dem Anmeldeverlauf und den vertrauenswürdigen Geräten an.

Identity Center ist eine Sammlung von Benutzerattributen, Geräten, Anmeldeverlauf, Sicherheitsaktivitäten und vielem mehr. Sie bietet eine Einzelbereichsansicht aller Daten mit zusätzlichen Sicherheitskontrollen und Benachrichtigungsfunktionen.

Mit Identity Center können Sie Details zu Ihren aktiven Sitzungen, dem Anmeldeverlauf und den vertrauenswürdigen Geräten anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

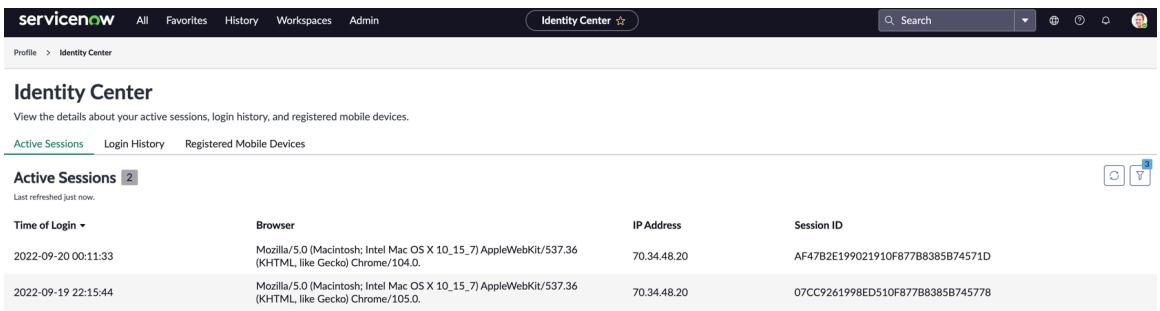
Um für Benutzer auf das Identitätscenter zuzugreifen, navigieren Sie zu einem der folgenden:

- Navigieren Sie auf Now Platformzu **Alle** > **Selfservice** > **Mein Profil** und wählen Sie **Identity Center** anzeigen im Abschnitt „Zugehörige Links“ aus.

  Hinweis:
  Sie können auch auf Ihr Profil zugreifen, indem Sie Ihren Benutzernamen im Instanz-Header auswählen.

- Wählen Sie in Now Supportdas Profil und dann am unteren Rand der Seite **Identity Center** anzeigen aus.

Die Identity Center-Seite wird wie folgt angezeigt:



Identity Center verfügt über die folgenden Registerkarten:

- Aktive Sitzungen
- Anmeldungsverlauf
- Registrierte Mobilgeräte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese Registerkarten auswählen, um Details wie Browser, IP-Adressen, Informationen zur Sitzungsbeziehung, Anmeldeinformationen und Ihre registrierten Mobilgeräte anzuzeigen.

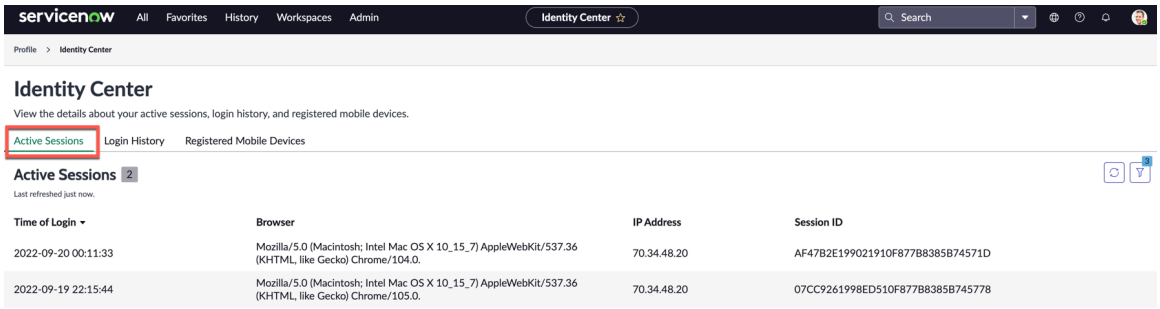
Aktive Sitzungen anzeigen

Zeigt die Informationen zu den Benutzersitzungen an.

Aktive Sitzungen sind die Sitzungen, die in der aktuellen Instanz ServiceNow®mit verschiedenen Browsern oder Geräten geöffnet sind.

Die Registerkarte Aktive Sitzungen im Identitätscenter hilft Ihnen, Ihre Sitzungen basierend auf Browser, IP-Adresse und Sitzungs-ID zu identifizieren. Mit diesen Informationen können Sie erforderliche Aktionen ausführen, z. B. die Sitzung verlängern oder beenden.

Anhand dieser Informationen können Sie feststellen, ob die Sitzungen real sind und kein Sicherheitsrisiko darstellen.



Anmeldeverlauf anzeigen

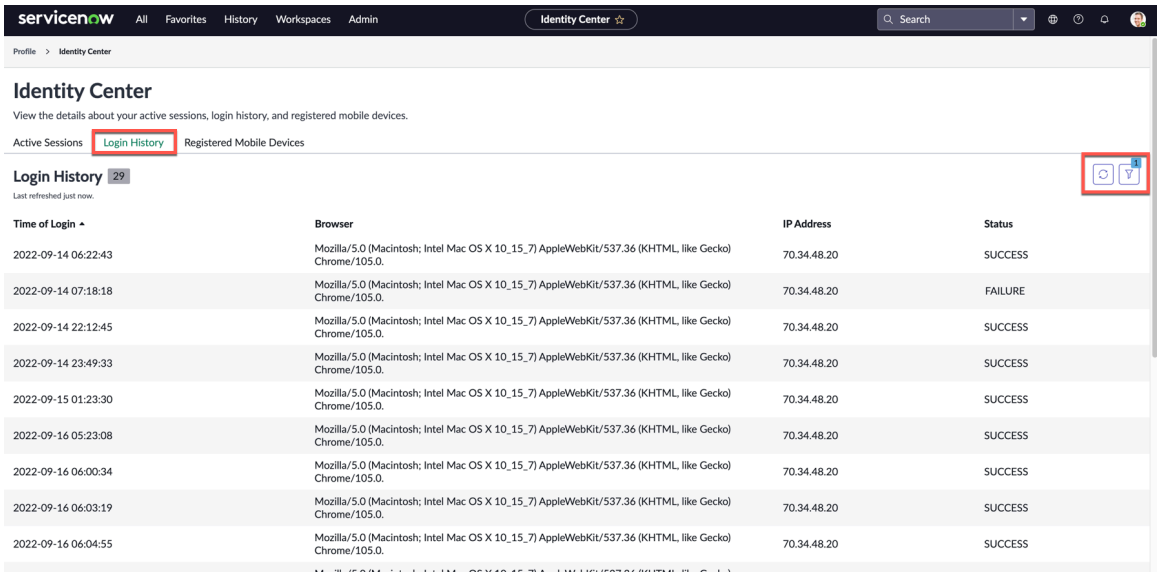
Stellt Details zu Ihrem Anmeldeverlauf bereit.

Die Registerkarte „Anmeldeverlauf“ in Identity Center hilft Ihnen bei Ihren Anmeldeinformationen und dem Status Ihrer Anmeldung.

Sie können die Filter verwenden, um Anmeldeaktionen zur Unterstützung von Sicherheitsuntersuchungen anzugeben. Filter kann dabei helfen, festzustellen, ob die Aktivität echt oder verdächtig war, und die Informationen an Ihren Administrator zu melden.

Die Paginierung im Anmeldeverlauf beträgt standardmäßig 20 und kann auf maximal 100 festgelegt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Folgenden sind einige der anderen Details aus dem Anmeldeverlauf aufgeführt:

- Die Zeit der Anmeldung ist die aktualisierte Zeit, zu der die Mobilgeräte für den Zugriff auf die Instanz verwendet werden.
- Die Datensätze werden 30 Tage lang in Identity Center gespeichert.

Zeigen Sie registrierte Mobilgeräte an

Geben Sie Details zu Ihrem registrierten Mobiltelefon in der Instanz ServiceNow an.

Die Registerkarte Registered Mobile Devices (Registrierte Mobilgeräte) in Identity Center zeigt die Details zu Ihren registrierten Geräten an, die für den Zugriff auf die Instanz ServiceNow verwendet wurden.

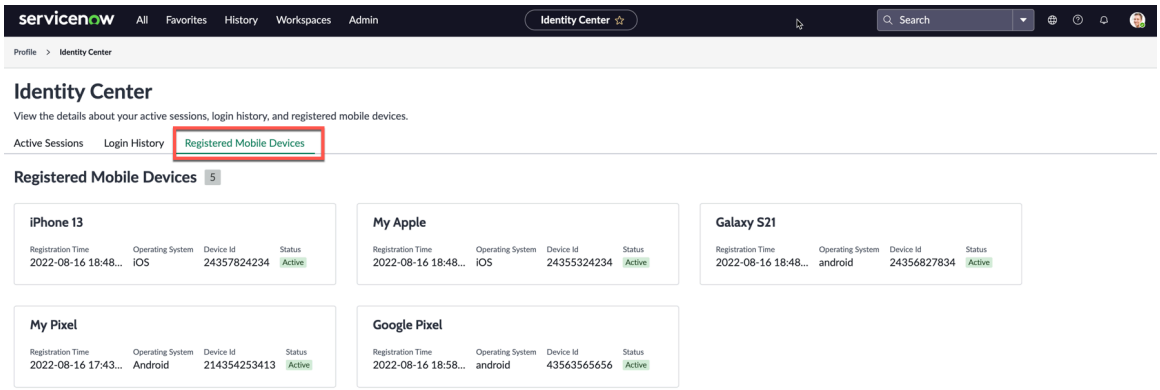
Wenn das Modul „Adaptive Authentifizierung“ aktiviert und ein registriertes Mobilgerät registriert ist, zeigt Identity Center die Details zu Ihren registrierten Geräten an.

Darüber hinaus werden Details zu den Geräten wie Betriebssystem, Geräte-ID und Status des Geräts zusammen mit der Registrierungszeit des Geräts angezeigt.

Um Ihr Mobilgerät zu registrieren, müssen Sie sicherstellen, dass das Plugin „Adaptive Authentifizierung“ (`com.snc.adaptive_authentication`) installiert ist und Sie die Funktion „Trusted Mobile App“ aktiviert haben. Weitere Informationen finden Sie unter Aktivieren Sie Trusted Mobile App.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Identitätsmetriken für Administratoren

Zeigen Sie Trends der Benutzer, privilegierten Benutzer, aktiven Sitzungen und des integrierten Kontos in Ihrer Instanz ServiceNow an.

Identitätsmetriken für Administratoren weisen die Trends für Folgendes auf:

- Benutzer
- Privilegierte Benutzer
- Integration oder nicht menschliche Accounts
- Aktive Sitzungen
- Inaktive Sitzungen

Weitere Informationen finden Sie unter Security Center-Metriken.

System für domänenübergreifendes Identitätsmanagement (SCIM)

Die SCIM-API (System for Cross-Domain Identity Management) bietet Endpunkte zum Erstellen, Lesen, Aktualisieren und Löschen von Vorgängen für Benutzer und Gruppen mithilfe des SCIM-Protokolls.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Anbieter

Der SCIM-Provider synchronisiert die Änderungen an Identitäten im IdP, einschließlich Erstellen, Aktualisieren oder Löschen von Datensätzen.

SCIM-Client

Der SCIM-Client wird zum Erstellen, Aktualisieren und Löschen von Identitätsressourcen in einem System verwendet, das SCIM-konforme REST-Anforderungen unterstützt.

Das SCIM-Protokoll ist ein HTTP-basiertes Protokoll auf Anwendungsebene, das auf dem HTTP-Standard (RFC7230) basiert. Verwenden Sie diese API für die Bereitstellung und Verwaltung von Identitätsdaten, z. B. Benutzer und Gruppen. Verwenden Sie die API im Web und in domänenübergreifenden Umgebungen, z. B. von Unternehmen zu Cloud-Service Providern oder Inter-Cloud-Szenarien.

Um auf diese API zuzugreifen, müssen Sie das Plugin „SCIM v2 – ServiceNow® Cross-domain Identity Management“ (com.snc.integration.scim2) aktivieren.

Weitere Informationen zur SCIM-API finden Sie unter System for Cross-Domain Identity Management (SCIM) API .

SCIM-Anbieter

Der Service Provider stellt Benutzer und Gruppen mithilfe der SCIM-API bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Erfahren Sie mehr über den SCIM-Provider.

Aktivieren

Aktivieren Sie SCIM.

SCIM-Anpassung

Erfahren Sie, wie Sie SCIM anpassen können.

Quelldefinition

Erfahren Sie mehr über die Quelldefinition für SCIM.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Provider erkunden

Der Service Provider stellt Benutzer und Gruppen mithilfe der SCIM-API bereit.

Als SCIM-Provider unterstützen die ServiceNow -Schemata SCIM-APIs zur Bereitstellung von Benutzern und Gruppen.

Der SCIM-Provider synchronisiert die Änderungen an Identitäten im IdP, einschließlich Erstellen, Aktualisieren oder Löschen von Datensätzen. Diese Änderungen werden gemäß dem SCIM-Protokoll automatisch mit dem Provider synchronisiert. Außerdem kann der IdP Identitäten des Providers lesen, die dem IdP-Verzeichnis hinzugefügt werden sollen. Der IdP kann dann falsche Werte beim Provider erkennen, die Sicherheitsschwachstellen verursachen könnten. Die Synchronisierung ermöglicht Endbenutzern nahtlosen Zugriff auf Anwendungen, denen sie zugewiesen sind, mit aktuellen Profilen und Berechtigungen.

Konfigurationen für SCIM-Provider

Führen Sie die folgenden Aufgaben aus, um den SCIM-Provider zu konfigurieren:

- Aktivieren Sie das Plugin **„SCIM v2 – ServiceNow Cross-Domain Identity Management“**. Weitere Informationen finden Sie unter Aktivieren des SCIM-Plugins.
- Aktivieren Sie die anderen Plugins, die für SCIM erforderlich sind:
  - OAuth 2.0
  - REST-API-Provider
  - REST API-Zugriffsrichtlinie
- Fügen Sie die Rolle scim_admin als Teil des SCIM-Service hinzu

Warnung:
Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Zuweisung der Rolle admin an den Benutzer, in der scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Tabellen

Zwei Tabellen, sys_user und sys_group, enthalten die SCIM-Attribute, die nicht vorhandenen ServiceNow -Tabellen zugeordnet sind. Weitere Informationen zu den Tabellen finden Sie unter SCIM-spezifische Tabellen .

Aktivieren des SCIM-Plugins

Installieren Sie für die SCIM-Aktivierung das Plugin „SCIM v2 - ServiceNow Cross-domain Identity Management“ (com.snc.integration.scim2).

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „SCIM v2 – ServiceNow Cross-Domain Identity Management“ (com.snc.integration.scim2).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Tutorial: Konfigurieren Sie SCIM für die Benutzerbereitstellung mit Azure AD

Durch die Konfiguration von Azure AD für ServiceNow SCIM werden Benutzer und Gruppen mithilfe des Azure AD-Bereitstellungsservice automatisch bereitgestellt bzw. aufgehoben.

Vorbereitungen

Installieren Sie das SCIM-Plugin

Erforderliche Rolle: scim_admin

Warnung:
Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Zuweisung der Rolle admin an den Benutzer, in der scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Benutzer mit SCIM über die folgenden Authentifizierungsmethoden bereitstellen:

- Basic Authentication
- OAuth

Benutzer wird mit Standardauthentifizierung bereitgestellt

Durch die Konfiguration von Azure AD für SCIM wird die Bereitstellung von Benutzern und Gruppen für ServiceNow automatisch bereitgestellt bzw. aufgehoben, indem der Azure AD-Bereitstellungsservice mit Standardauthentifizierung verwendet wird.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung:
Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Zuweisung der Rolle admin an den Benutzer, in der scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

- Aktivieren Sie das SCIM-Plugin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien** , um die Details der REST-API-Zugriffsrichtlinien zu überprüfen.
2. Klicken Sie auf der Seite „API-Zugriffsrichtlinie“ auf den Datensatz **SCIM-API-Richtlinie**.
3. Vergewissern Sie sich, dass der Datensatz für die **SCIM-API** -Standardauthentifizierung in den Abschnitten „Authentifizierungsprofile“ verfügbar ist.
4. Überprüfen Sie, ob das Feld Standardauthentifizierung mit einem **SCIM** - **API** -Datensatz angegeben ist, der zuvor als Anwendungsregistrierung konfiguriert oder überprüft wurde.
5. Melden Sie sich beim Azure-Portal an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Navigieren zu **Unternehmensanwendungen** > **Alle Anwendungen**.
7. Wählen Sie in der Liste der Anwendungen ServiceNow aus, oder erstellen Sie eine neue ServiceNow Anwendung.
8. Wechseln Sie zur Registerkarte Bereitstellung, und legen Sie den Bereitstellungsmodus auf **Automatisch**fest.
9. Geben Sie im Abschnitt „Administratoranmeldeinformationen“ Folgendes an:
   - Authentifizierungsmethode: Standardauthentifizierung
   - Instanzname
   - Administrator-Anwendername
   - Admin-Passwort
10. Wählen Sie Testverbindung aus, um sicherzustellen, dass Azure AD eine Verbindung zu ServiceNowherstellen kann.

Hinweis:
Wenn die Verbindung fehlschlägt, stellen Sie sicher, dass Ihr Konto ServiceNow über Administratorberechtigungen verfügt, und versuchen Sie es erneut.

Benutzer wird mit OAuth bereitgestellt

Durch die Konfiguration von Azure AD für ServiceNow SCIM werden Benutzer und Gruppen automatisch bereitgestellt bzw. aufgehoben, indem der Azure AD-Bereitstellungsservice mit OAuth verwendet wird.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung:
Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Zuweisung der Rolle admin an den Benutzer, in der scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

- Aktivieren Sie das SCIM-Plugin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**.
2. Klicken Sie auf der Seite „Anwendungsregistrierungen“ auf den **SCIM-API** -Datensatz.
3. Überprüfen Sie die **SCIM-API** -Datensatzdetails.

   Diese Details sollten bei der Konfiguration der Anwendung ServiceNow in Azure AD angegeben werden.
4. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien** , um die Details der REST-API-Zugriffsrichtlinien zu überprüfen.
5. Klicken Sie auf der Seite „API-Zugriffsrichtlinie“ auf den Datensatz **SCIM-API-Richtlinie**.
6. Vergewissern Sie sich, dass der **SCIMAPIOAuthOnly** -Datensatz in den Abschnitten „Authentifizierungsprofile“ verfügbar ist.
7. Überprüfen Sie, ob das Feld **OAuth-Entität** mit dem **SCIM-API** -Datensatz angegeben ist, der zuvor als Anwendungsregistrierung konfiguriert oder überprüft wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Melden Sie sich beim Azure-Portal an.
9. Navigieren zu **Unternehmensanwendungen** > **Alle Anwendungen**.
10. Wählen Sie in der Liste der Anwendungen ServiceNow aus, oder erstellen Sie eine neue ServiceNow Anwendung.
11. Wechseln Sie zur Registerkarte Bereitstellung, und legen Sie den Bereitstellungsmodus auf **Automatisch**fest.
12. Geben Sie im Abschnitt „Administratoranmeldeinformationen“ Folgendes an:
    - Authentifizierungsmethode: OAuth.

      Hinweis:
      Um den für die Bereitstellung eingereichten OAuth mit SCIM auszufüllen, müssen Sie die Anwendung auf den SCIM 2.0-Endpunkt aktualisieren. Weitere Informationen zum Aktualisieren von finden Sie in der Azure-Dokumentation .

    - Instanzname
    - Administrator-Anwendername
    - Admin-Passwort
13. Wählen Sie Testverbindung aus, um sicherzustellen, dass Azure AD eine Verbindung zu ServiceNowherstellen kann.

    Hinweis:
    Wenn die Verbindung fehlschlägt, stellen Sie sicher, dass Ihr Konto ServiceNow über Administratorberechtigungen verfügt, und versuchen Sie es erneut.

SCIM-Fehlerbehebung

Häufige Fehlerszenarien bei der Integration mit SCIM.

Ungültige REST-API-URL

Aktion: Geben Sie eine gültige API-URL ein. Es wäre möglich, die REST-API-URL im **REST-API-Explorer**zu überprüfen.

In der Instanz ServiceNow ist keine Umleitungs-URL festgelegt

Aktion: Geben Sie eine gültige Umleitungs-URL für die SCIM-OAuth-Entität in ServiceNowein. Geben Sie die Umleitungs-URL ein, während Sie die OAuth-Entität in ServiceNowkonfigurieren.

Wenn sich die Umleitungs-URL von der Anforderung unterscheidet.

Aktion: „**redirect_url**“ in „**Autorisierungsendpunkt“** muss mit der in ServiceNowkonfigurierten OAuth-Entität identisch sein.

Hinweis:

Dieser Fehler tritt auf, wenn zwischen Azure „Autorisierungsendpunkt“ undServiceNow „Umleitungs-URL“ eine Diskrepanz besteht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein ungültiger geheimer Clientschlüssel übergeben wird

Aktion: Der in „Geheimer Clientschlüssel“ eingegebene Wert muss mit der in ServiceNowkonfigurierten OAuth-Entität identisch sein.

Wenn eine ungültige „ClientId“ in Azure „Autorisierungsendpunkt“ übergeben wird

Aktion: Der für den Parameter „client_id“ in „Autorisierungsendpunkt“ eingegebene Wert muss mit der in ServiceNowkonfigurierten OAuth-Entität übereinstimmen.

SCIM-Anpassung

Passen Sie SCIM-Protokolle für Ihr Identitätsmanagement an.

Mit der SCIM-Anpassung können Sie Folgendes tun:

- Unterstützen Sie benutzerdefinierte Felder in den Tabellen „sys_user“ und „sys_user_group“ durch die Generierung dynamischer Erweiterungsschemata.
- Bieten Sie die Möglichkeit, die standardmäßigen SCIM-Zuordnungen zu überschreiben.

Ein SCIM-Administrator kann benutzerdefinierte Erweiterungsschemata für Benutzer- und Gruppenressourcen definieren. Die im benutzerdefinierten Erweiterungsschema definierten Attribute können Feldern in den Tabellen „sys_user“ oder „sys_user_group“ zugeordnet werden.

Konfigurationen für die SCIM-Anpassung

Für die SCIM-Anpassung sollten Sie die folgenden Aufgaben ausführen:

- Definieren Sie ein benutzerdefiniertes Erweiterungsschema für Benutzer und Gruppen in der SCIM-Erweiterungsschematabelle. Weitere Informationen finden Sie unter Erstellen Sie ein SCIM-Erweiterungsschema.
- Erstellen Sie Entitäten in einer ETL-Definition für benutzerdefinierte Schemaattribute. Die Entitäten werden für die Zieltabelle erstellt, die entweder dem Attribut sys_user oder sys_user_group zugeordnet ist. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM ETL-Definition.
- Erstellen Sie eine RTE-Zuordnung zwischen diesen beiden Entitäten. Weitere Informationen finden Sie unter Schritt 5 in Erstellen Sie eine SCIM ETL-Definition.
- Senden Sie benutzerdefinierte Schemaattribute mit Daten in der Nutzlast der SCIM-API-Anforderung.

Die SCIM-API ruft die RTE-Engine mit der definierten Zuordnung auf. Die Daten werden in den entsprechenden Feldern in der Zieltabelle gespeichert, wie in der Zuordnung definiert.

SCIM-Anpassungseigenschaften und -schemata

Die SCIM-Anpassung umfasst die folgenden Eigenschaften, unterstützten Schemas und nicht unterstützten Schemas.

Eigenschaften

Die SCIM-Anpassung fügt die folgenden Systemeigenschaften hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften

Name	Beschreibung
com.snc.integration.scim2.max.member.count	Die maximale SCIM-Mitgliederanzahl.
com.snc.integration.scim2.resolve.external.id.scim.list	Lösen Sie SCIM-Ressourcen basierend auf der Quelldefinition des anfordernden Clients auf, wenn mehrere Ressourcen mit einem externen ID-SCIM-Filter gefunden werden. **Hinweis:** Wenn die Bereitstellung aus mehreren Quellen erfolgt, müssen die Quellen in der SCIM-Quelldefinitionstabelle definiert sein. Wenn keine Quellen definiert sind oder diese Eigenschaft inaktiv ist, werden alle übereinstimmenden Ressourcen mit einer externen ID-Filterantwort zurückgegeben.
com.snc.integration.scim2.user.etl.definition	ID der ETL-Definition des SCIM-Benutzers.
com.snc.integration.scim2.group.etl.definition	ID der ETL-Definition der SCIM-Gruppe.
com.snc.integration.scim2.rte.verbose.logging	Aktivieren Sie die ausführliche Protokollierung für RTE-Definitionen von SCIM-Benutzern und -Gruppen.
com.snc.integration.scim2.string.field.length.validation.enabled	Die Eingabevalidierung für Feldlänge. Diese Eigenschaft ermöglicht die Validierung, anstatt das Feld zu kürzen und zu speichern.
com.snc.integration.scim2.provider.custom.script.id	Die ID des Skripts, das zum Anpassen der SCIM-Antworten.

Unterstützte Schemas

Die SCIM-Anpassung fügt die folgenden unterstützten Schemas hinzu.

Unterstützte Schemas

Schemen	Beschreibung	Präfix	Beispiel
urn:ietf:params:scim:schemas:core:2.0:User	Enthält Attribute, die sich auf die Ressourcen.		name.middleName
urn:ietf:params:scim:schemas:extension:servicenow:2.0:User	Enthält Attribute, die sich auf ServiceNow beziehen.		servicenow.manager.value
urn:ietf:params:scim:schemas:extension:servicenow:custom:2.0:User	Enthält Attribute, die nicht als Teil der Core-Erweiterung oder des Erweiterungsschemas ServiceNow zugeordnet sind.		customUserId

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht unterstütztes Schema

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: Enthält Attribute, die häufig zur Darstellung von Benutzern verwendet werden, die zu einem Unternehmen gehören oder in dessen Namen handeln.

Hinweis:
Das Enterprise-Schema ist ein gültiges Schema, aber seine Attribute werden einer beliebigen Tabelle zugeordnet. Da die Datenbankpersistenz nicht unterstützt wird, wird kein Fehler angezeigt, wenn ein Enterprise-Schema im Anforderungstext enthalten ist.

Erstellen Sie ein SCIM-Erweiterungsschema

Erstellen Sie benutzerdefinierte Attribute, um sie Feldern zuzuordnen, die nicht als Teil des Kernschemas oder des Erweiterungsschemas ServiceNow zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: scim_admin

Warnung:
Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin ist gleichbedeutend mit der Zuweisung der Rolle admin an den Benutzer, wobei die Rolle scmin_admin neue Datensätze in die Tabellen einfügen kann, die Geschäftslogik oder ACL-Schutz umgehen können.

Prozedur

1. Navigieren zu **Alle** > **SCIM** > **SCIM-Erweiterungsschemas**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

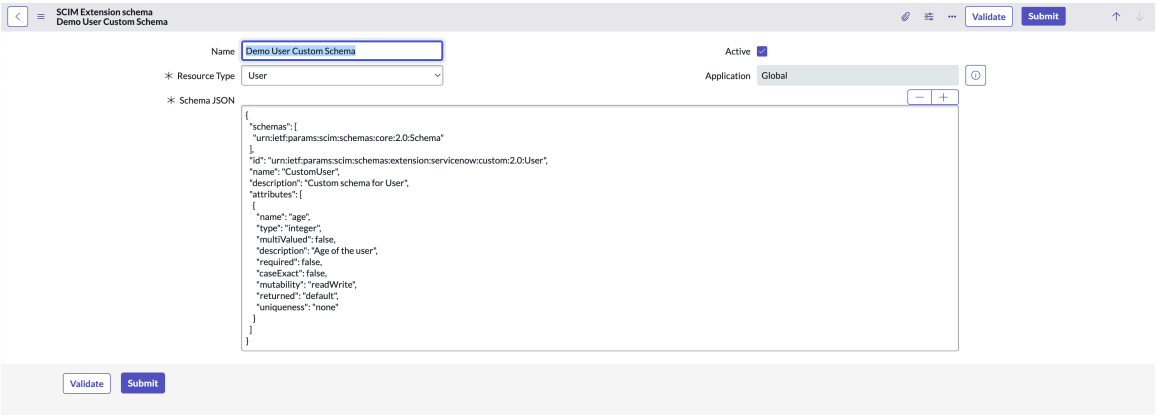
Hinweis:
Dem Feld **Ressourcentyp** kann nur ein Erweiterungsschema zugeordnet werden. Beispielsweise kann Benutzer als Ressourcentyp einem Benutzererweiterungsschema zugeordnet werden.

SCIM-Erweiterungsschema

Feld	Beschreibung
Name	Name des Erweiterungsschemas.
Aktiv	Option zum Aktivieren des Schemas. Wählen Sie dieses Feld aus, wenn der Datensatz als benutzerdefiniertes Erweiterungsschema betrachtet werden muss. Für einen bestimmten Ressourcentyp kann jeweils nur ein benutzerdefinierter Erweiterungsschema-Datensatz aktiv sein, unabhängig davon, ob es sich um den Typ „Benutzer“ oder „Gruppe“ handelt.
Ressourcentyp	Ressourcentyp, der dem Erweiterungsschema zugeordnet werden muss. Im Folgenden sind die Optionen aufgeführt: ○ **Benutzer** ○ **Gruppe**
Anwendung	Anwendungsbereich für diesen Datensatz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schema-JSON	Details innerhalb der JSON-Schemata. Weitere Informationen zum Definieren des Erweiterungsschemas mit Attributen finden Sie unter Datatracker .



4. Validieren Sie die Attribute, indem Sie auf **Validieren**klicken.
5. Klicken Sie auf **Absenden**.

Ergebnisse

Das Erweiterungsschema mit benutzerdefinierten Attributen im Zusammenhang mit dem Ressourcentyp „Benutzer“ oder „Gruppe“ wird erstellt. Verwenden Sie die SCIM-ETL-Definitionen, um die Ressourcen basierend auf dem Erweiterungsschema in den Tabellen „sys_user“ und „sys_user_group“ zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM ETL-Definition.

Erstellen Sie eine SCIM ETL-Definition

Verwenden Sie die SCIM-ETL-Definitionen, um die benutzerdefinierten Attribute den Tabellen „sys_user“ oder „sys_user_group“ zuzuordnen.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung:
Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin ist gleichbedeutend mit der Zuweisung der Rolle admin an den Benutzer, wobei die Rolle scmin_admin neue Datensätze in die Tabellen einfügen kann, die Geschäftslogik oder ACL-Schutz umgehen können.

Hinweis:

- ETL-Definitionen für SCIM-Gruppen und SCIM-Benutzer sind Teil des Basissystems für die Ressourcenzuordnung. Sie können dieselben Ressourcenzuordnungen verwenden und die Kriterien nach Bedarf ändern, oder Sie können neue Ressourcenzuordnungen erstellen.
- [*]-Felder werden über RTE in der SCIM-Zuordnung nicht unterstützt.

Prozedur

1. Befolgen Sie die Anweisungen unter ETL-Definitionen (Extract Transform Load) erstellen .
2. Öffnen Sie den neu erstellten Datensatz, und zeigen Sie die Details an.
3. Erstellen Sie im Abschnitt ETL-Entitäten eine Entität, indem Sie auf **Neu**klicken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie müssen Entitäten für die folgenden Benutzer erstellen:

- scim-user: Für die Felder, die aus SCIM stammen.
- Tabelle „Benutzer“ (sys_user) oder „Gruppe“ (sys_user_group): Für die Felder, die Sie aus der Datenbanktabelle mit SCIM zuordnen möchten. Beispielsweise können Sie für die Anpassung von Benutzerdetails über SCIM die Tabelle sys_user verwenden.

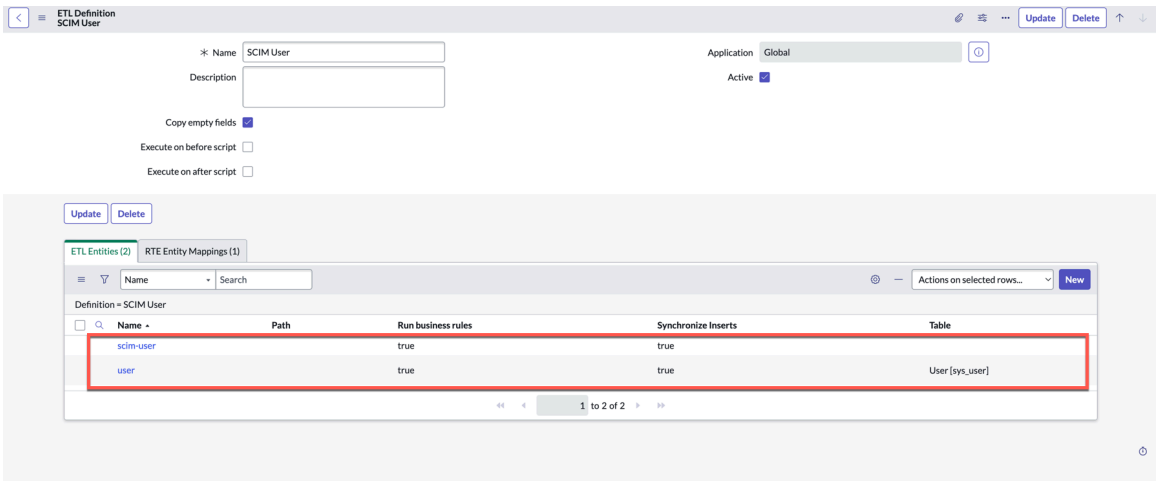
a. Füllen Sie die Felder des Formulars aus.

ETL-Entitätsformular

Feld	Beschreibung
Name	Name der ETL-Entität.
Anwendung	Anwendungsbereich für diesen Datensatz
Tabelle	Zieltabelle für die ETL-Entität.
Definition	Ausgewählte ETL-Entität.
Pfad	Eindeutiger Pfad für diese Entität. Geben Sie keinen Pfad für die Entität an, die die Import Set-Tabelle darstellt. Wenn eine Entität eine Sammlung darstellt, muss der Pfad mit einem Sternchen [*] enden. Diese Anforderung gilt für Zwischeneinträge und die Zieltabellenentität.
Einfügungen synchronisieren	Option, um sicherzustellen, dass nur ein Datensatz mit eindeutigen zusammengefügten Feldwerten vorhanden ist, indem Datensatzeinfügungen synchronisiert werden.
Business-Regeln ausführen	Option zum Ausführen von Business Rules.

b. Klicken Sie auf **Absenden**.

Die ETL-Entitäten werden für die Tabellen scim-user und user erstellt. Sie müssen ETL-Entitätsfelder innerhalb dieser ETL-Entitäten erstellen und beide Entitäten zuordnen, indem Sie eine RTE-Entitätszuordnung erstellen.



4. Erstellen Sie die Entitäten, und ordnen Sie sie zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

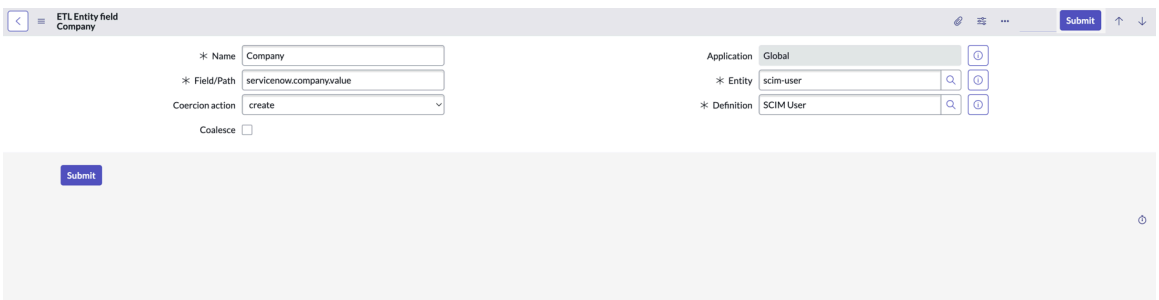
a. Öffnen Sie den übermittelten Datensatz (scim-user und user).

b. Fügen Sie in den ETL-Entitätsfeldern die Felder hinzu, indem Sie auf **Neu**klicken.

c. Füllen Sie die Felder des Formulars aus.

ETL-Entitätsformular

Feld	Beschreibung
Name	Name der Felddefinition der ETL-Entität.
Anwendung	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Feld/Pfad	Dieses Feld ist entweder eine Spalte oder ein Pfad. ▪ Das Feld ist ein Spaltenname, wenn die Entität die Import- oder Zieltabelle ist. ▪ Das Feld ist ein Pfad, wenn das Feld verschachtelte Strukturen aufweist.
Entität	Entität, für die dieser Vorgang gilt. Wählen Sie die Entität mithilfe des Suchsymbols aus.
Zwangsaktion	Was das System tun soll, wenn eine Referenz oder Auswahl nicht gefunden werden konnte. Die Optionen sind wie folgt: ▪ **Erstellen**: Erstellen Sie eine neue Referenz oder Auswahl. Weisen Sie die Referenz oder Auswahl dem aktuellen Datensatz zu. ▪ **Ablehnen**: Speichern Sie nicht den gesamten Datensatz in der Datenbank. ▪ **Ignorieren**: Legen Sie den aktuellen Wert als leer fest.
Definition	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Zusammenfügen	Option zum Abfragen der vorhandenen Datensätze.



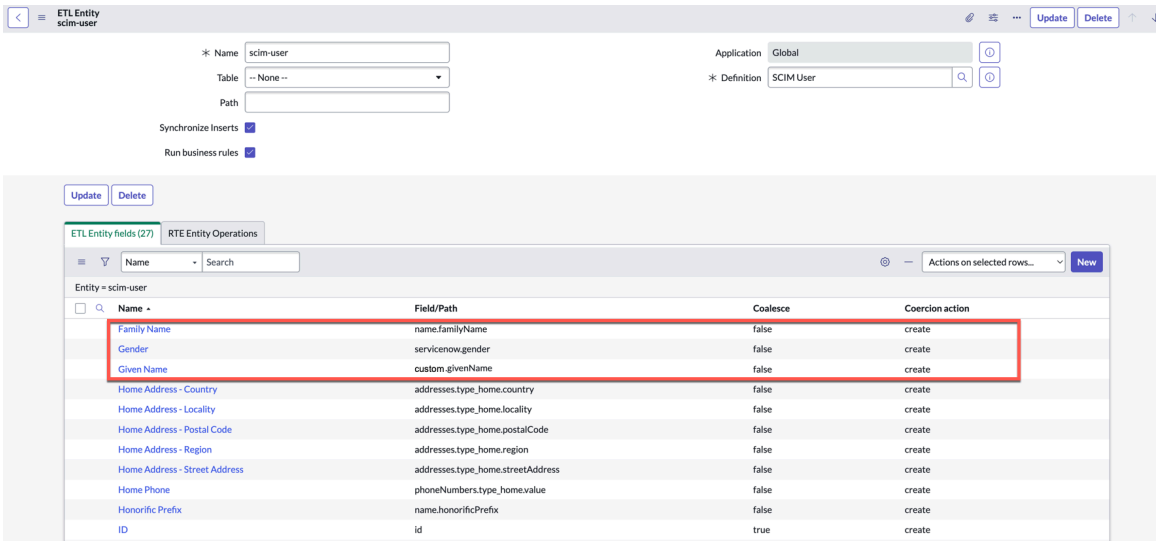
d. Übermitteln Sie die Einträge, indem Sie auf **Absenden**klicken.

Sie können basierend auf Ihren Anforderungen mehrere Einträge als ETL-Entitätsfeld hinzufügen.

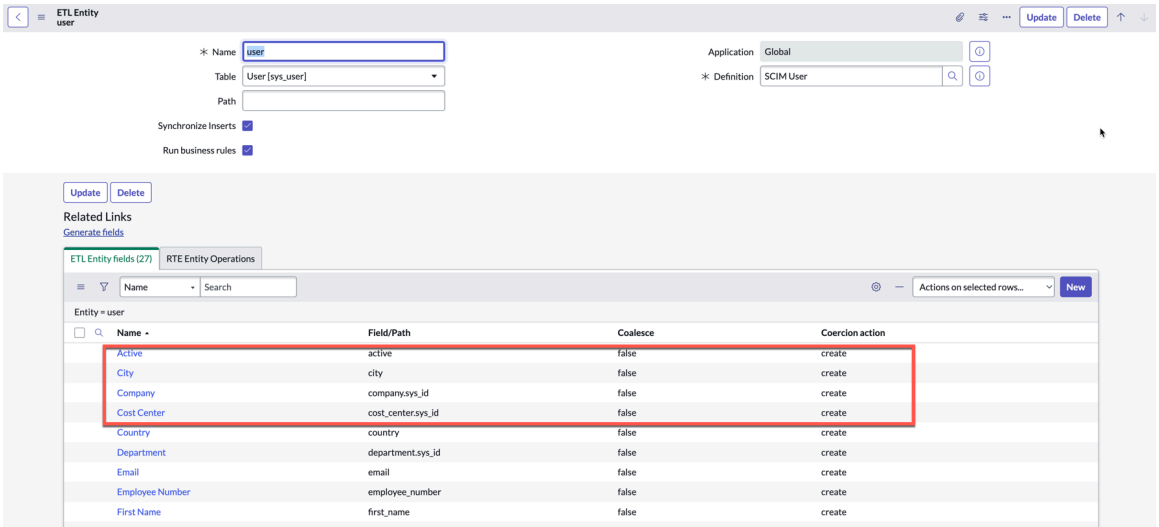
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ETL-Entität scim-user kann Entitäten mit der Core-Erweiterung (Benutzer), der Erweiterung ServiceNow oder der benutzerdefinierten Erweiterung haben.



Die Benutzer-ETL-Entität kann Entitäten aus der Datenbanktabelle haben. Beispiel: Tabelle sys_user.



Hinweis:

Um einen Filter in den eingehenden SCIM-Feldern hinzuzufügen, verwenden Sie einen Unterstrich (_). Dieser Unterstrich wird in einen EQ-Filter übersetzt. Zum Beispiel wendet das Attribut `email.type_work.value` den SCIM-Filter der E-Mail `[type eq "work"].value`an.

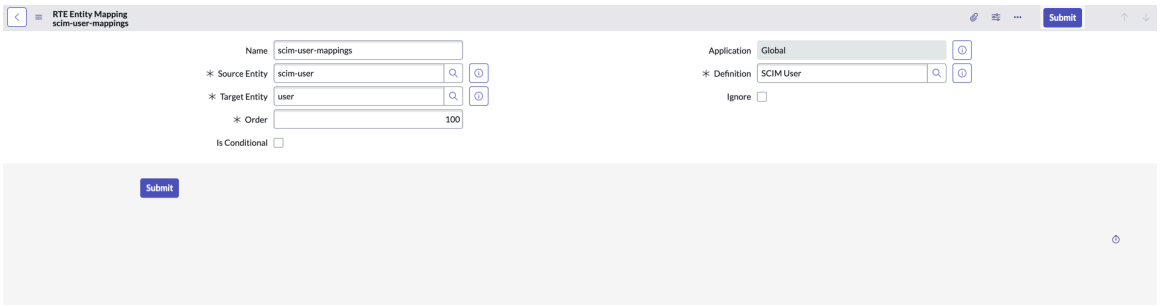
Nachdem die Felder in den ETL-Entitätsdatensätzen scim-user und user erstellt wurden, müssen Sie einen RTE-Entitätszuordnungsdatensatz erstellen. Sie müssen dann die Quell- und Zieldefinition angeben, um beide Felder zuzuordnen.

5. Erstellen Sie im Abschnitt RTE-Entitätszuordnungen eine Entitätszuordnung, indem Sie auf **Neu**klicken
6. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Name der Feldzuordnung.

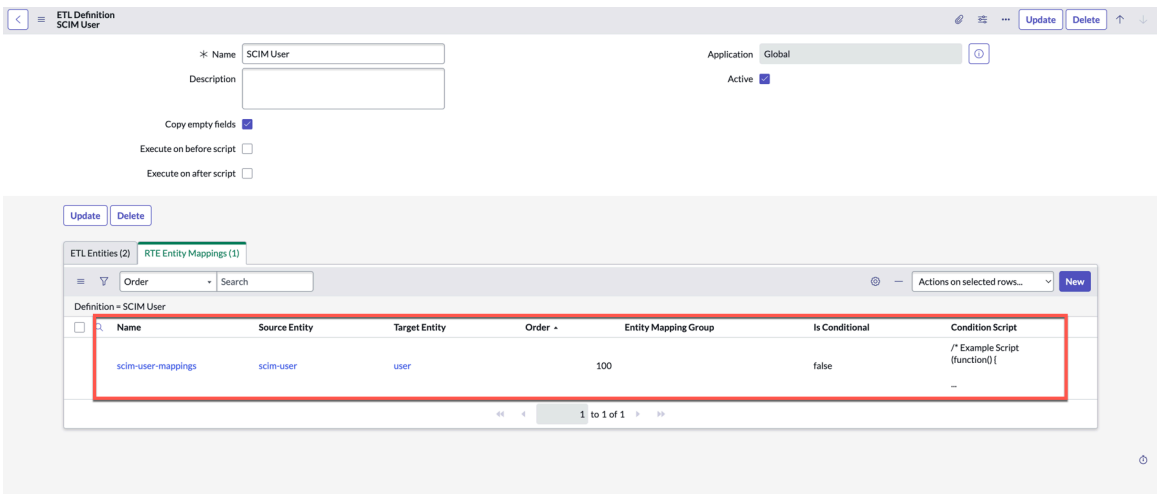
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quellentität	Quellentität für die Zuordnung.
Zielentität	Zielentität für die Zuordnung.
Reihenfolge	Reihenfolge, in der die Zuordnung verarbeitet werden soll.
Ist bedingt	Option zum Festlegen der Zuordnung als bedingt.
Bedingungsskript	Skript, das die Bedingungen definiert, die für die Zuordnung erfüllt sein müssen.
Anwendung	Anwendungsbereich für diesen Datensatz
Definition	Ausgewählte ETL-Entität, zu der diese Zuordnung gehört.
Ignorieren	Option, um anzugeben, ob diese ETL-Entitätszuordnung bei Datenintegrationen mit Robust Import Set Transformation (RTE) ignoriert werden soll.



7. Klicken Sie auf **Absenden**.

   Das folgende Beispiel zeigt einen Datensatz, der für die Zuordnung der ETL-Entitätsdatensätze scim-user und user erstellt wurde.



8. Öffnen Sie den übermittelten Datensatz (scim-user-mappings), und erstellen Sie eine Zuordnung zwischen den ETL-Entitätsdatensätzen scim-user und user.

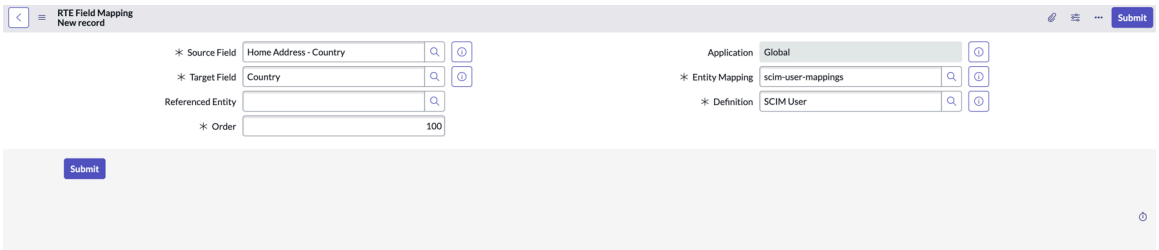
   a. Klicken Sie im Abschnitt RTE-Feldzuordnungen auf **Neu**.

   b. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ETL-Entitätsfelder

Feld	Beschreibung
Quellfeld	Anwendungsbereich für diesen Datensatz
Anwendung	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Zielfeld	Ausgabe-ETL-Feld für den Vorgang, wenn der Vorgang eine einzelne Ausgabe annimmt.
Entitätszuordnung	Entitätszuordnung, für die dieser Vorgang gilt.
Referenzierte Entität	Entität, auf die verwiesen wird, und der Vorgang, für den sie gilt.
Definition	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Reihenfolge	Reihenfolge, in der der Vorgang für die Entität ausgeführt wird.

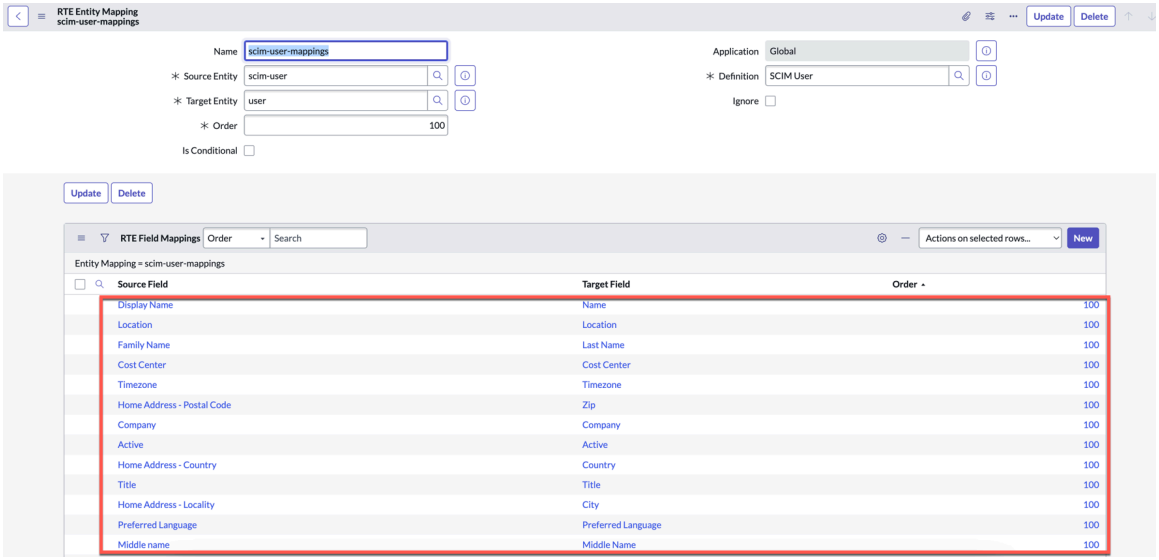


Das Quellfeld Privatadresse **- Land** (scim-user ETL-Entität) ordnet das Zielfeld als **Land** (user ETL-Entität) zu.

c. Übermitteln Sie die Einträge, indem Sie auf **Absenden**klicken.

Sie können basierend auf Ihren Anforderungen mehrere Einträge als RTE-Entitätszuordnungen hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Quell- und Zielfelder werden wie konfiguriert zugeordnet. Wenn Sie CRUD-Vorgänge mit SCIM ausführen, werden die benutzerdefinierten Werte in der entsprechenden Tabelle aktualisiert.

Ergebnisse

Mit diesen ETL-Definitionen und -Zuordnungen können Sie Daten aus einer Quelltabelle extrahieren, die Daten wie gewünscht umwandeln und die Daten in eine Zieltabelle laden.

Zugehörige Informationen

Erstellen Sie ETL-Definitionen (Extract Transform Load).

Umgang mit nicht zugeordneten Feldern

Sie können nicht zugeordnete Felder in der SCIM-Anpassung auf verschiedene Arten behandeln.

Während der SCIM-Anpassung können die Felder, die nicht Teil der Tabellen „sys_user“ und „sys_user_group“ sind, durch Ausführen der folgenden Funktionen zugeordnet werden.

SCIM anpassen (Erstellen oder Aktualisieren)

Sie können den SCIM-Client erstellen oder aktualisieren.

- Der SCIM-Administrator kann benutzerdefinierte Skripts in den Skripts *`onBefore`* und *`onAfter`* für Felder hinzufügen, die nicht in der ETL-Definition oder RTE zugeordnet sind.
- Der SCIM-Administrator kann RTE-Zuordnungen überschreiben, indem er benutzerdefinierte Skripts in den Skripts *`onBefore`* und *`onAfter`* hinzufügt.
- Sie können eine skriptfähige API in den RTE-Skripts *`onBefore`* oder *`onAfter`* aufrufen, um auf eingehende Anforderungen zuzugreifen und Transformationen für andere Tabellen, Listen und nicht zugeordnete Attribute durchzuführen.
- Sie können die Methode *`sn_auth.SCIM2Util.getScimProviderCustomizationContext()`* verwenden, um den SCIM-Anforderungskontext bereitzustellen, der das Objekt *`scimResource`* enthält. *`scimResource`* im Kontext stellt in jedem Vorgang Folgendes dar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **POST**: Die in der Anforderungsnutzlast gesendete SCIM-Ressource.
- **PUT**: Die aktuelle SCIM-Ressource aus der Datenbank, ersetzt durch die in der Anforderungsnutzlast gesendete SCIM-Ressource.
- **PATCH**: Die aktuelle SCIM-Ressource aus der Datenbank nach den Patch-Vorgängen.

Das Folgende ist ein Beispiel für ein *onAfter* -Skript.

```
(function onAfter(source, target, importLog) {

   var ctx = sn_auth.SCIM2Util.getScimProviderCustomizationContext();
   gs.info("scim context ee: " + JSON.stringify(ctx.scimResource));

   var roles = ctx.scimResource.roles;
   if(roles) {
      var removingRolesGR = new GlideRecord("sys_user_has_role");
      removingRolesGR.addQuery("user", target.sys_user[0].sys_id);
      removingRolesGR.query();
      removingRolesGR.deleteMultiple();

   for (var i = 0; i < roles.length; i++) {
      var addingRolesGR = new GlideRecord("sys_user_has_role");
      addingRolesGR.setValue("user", target.sys_user[0].sys_id);
      addingRolesGR.setValue("role", roles[i].value);
      addingRolesGR.setValue("state", "active");
      addingRolesGR.insert();
      }
      }
      var customUserExtn = new
global.SCIMProviderCustomization().getCustomExtensionUrn('User');
      var salary = ctx.scimResource[customUserExtn].salary;
      if (salary) {
         var gr = new GlideRecord("u_user_salary");
         gr.addQuery("user", target.sys_user[0].sys_id);
         gr.query();
         if (gr.next()) {
            gr.setValue("salary", salary);
            gs.info("scim update: " + gr.update());
         } else {
         gr.setValue("salary", salary);
         gr.setValue("user", target.sys_user[0].sys_id);
         gr.insert();
         }
        }

})(source, target, importLog);
```

Passen Sie die SCIM-Antwort an

Für die GET-API-Aufrufe kann jede Antwort an den SCIM-Client mithilfe des Skripts angepasst werden, indem das Skript *SCIMProviderCustomization* erweitert wird.

Beim Erweitern des Skripts kann der Autor die Methoden *customizeUserResponse* und *customizeGroupResponse* überschreiben, um die Antworten für Benutzer- und Gruppenressourcen zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Eigenschaft *com.snc.integration.scim2.provider.customization.script.id* ermöglicht es dem SCIM-Plugin, das Skript zu verwenden, das für die Antwortanpassung verwendet werden soll.

Das Folgende ist ein Beispiel für die Erweiterung des Basisskripts.

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype = Object.extendsObject(SCIMProviderCustomization, {
   initialize: function() {
      SCIMProviderCustomization.prototype.initialize.call(this);
   },
   customizeUserResponse: function(context) {
      try {
         var rolesGR = new GlideRecord("sys_user_has_role");
         rolesGR.addQuery("user", context.scimResource.id);
         rolesGR.query();
         var i = 0;
         context.scimResource.roles = [];
         while (rolesGR.next()) {
            context.scimResource.roles[i] = {
               display: rolesGR.getElement('role.name').getValue(),
               value: rolesGR.getElement('role.sys_id').getValue()
            };
            i++;
         }
         var userGR = new GlideRecord("u_user_salary");
         userGR.addQuery("user", context.scimResource.id);
         userGR.query();
         if (userGR.next()) {
            var salary = userGR.getValue("salary");
            if (salary) {
               var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
context);
               customExtensionValue.salary = salary;
               SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this,
"User", context, customExtensionValue);
            }
         }
      } catch (ex) {
         gs.error("err: " + ex);
      }
      return context;
   },
   customizeGroupResponse: function(context) {
      return context;
   },
   type: 'SCIMCustomizationScript'
});
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Der Parameter, den die Methoden *customizeUserResponse* und *customizeGroupResponse* enthalten, ist ein Kontextobjekt mit einem Attribut namens *scimResource*. Dieses Attribut weist alle Attribute eines Benutzer- oder Gruppenressourcenobjekts auf.
- Eine benutzerdefinierte Skripteinbindung kann nur vom Administrator erstellt und angezeigt werden.
- Wenn eine Benutzer- oder Gruppenressource geändert wird, müssen Sie den Kontext wiederherstellen.
- Wenn ein Attribut im Ressourcenobjekt nicht geändert wird, legen Sie *com.snc.integration.scim2.provider.customization.script.id* auf leer fest, oder geben Sie NULL zurück.
- Wenn bestimmte Attribute über das Skript *onAfter* beibehalten werden, müssen sie im benutzerdefinierten Skript mit Datenbankwerten im Objekt *scimResource* ausgefüllt werden. Diese Aktion ist erforderlich, damit das System Folgendes ausführen kann:
  - So erhalten Sie das richtige *scimResource* -Objekt in *onAfter* -Skripts während des PUT- und PATCH-Vorgangs.
  - Um die Attribute, die über das Skript *onAfter* beibehalten wurden, in die Antwort an den Client aufzunehmen.

Hilfsfunktionen

Im Folgenden sind einige der Hilfsfunktionen für die SCIM-Anpassung aufgeführt. Mit diesen Funktionen können Sie verschiedene Arten von Informationen abrufen oder festlegen.

Hilfsfunktionen

Funktion	Zweck
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");	Rufen Sie den benutzerdefinierten Erweiterungsschemas ab.
SCIMProviderCustomization.prototype.getServiceNowExtensionUrn.call(this, "User");	Rufen Sie den ServiceNow Erweiterungsschemas ab.
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User", context);	Rufen Sie den benutzerdefinierten Schemaknoten aus der Antwort ab.
SCIMProviderCustomization.prototype.getServiceNowExtensionNodeValue.call(this, "User", context);	Rufen Sie den ServiceNow Schemaknoten aus der Antwort ab
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this, "User", context, customExtensionValue);	Legen Sie den benutzerdefinierten Schemaknoten in der Antwort fest.

Das folgende Beispiel zeigt die Verwendung der Hilfsfunktion:

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
 context);
customExtensionValue.age = "18";
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue call(this, "User", context,
 customExtensionValue);
```

Hinweis:
RTE unterstützt das Festlegen von Daten in anderen Tabellen als den Tabellen „sys_user“ und „sys_user_group“.

Erstellen einer Quelldefinition

Erstellen Sie eine Quelldefinition, um Informationen darüber zu erfassen, aus welcher Identitätsquelle eine Ressource bereitgestellt wird.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung:
Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Zuweisung der Rolle admin an den Benutzer, in der scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Warum und wann dieser Vorgang ausgeführt wird

Mithilfe einer Quelldefinition kann die Identitätsquelle der Bereitstellung einer OAuth-Entität zugeordnet werden, mit der sie sich während der Bereitstellung authentifiziert.

Nachdem eine Quelldefinition erstellt wurde, werden alle Ressourcen, die aus dieser Identitätsquelle bereitgestellt werden, der entsprechenden Quelldefinitions-ID zugeordnet.

Die Quelldefinition erfasst die erforderlichen Quellinformationen, indem Sie beispielsweise wie folgt vorgehen:

- Gibt den SCIM-Client an, von dem die Ressource bereitgestellt wird.
- Löst doppelte Informationen auf, die von der externen ID bereitgestellt werden:
  - Wenn mehrere Identitätsquellen Ressourcen bereitstellen, können zwei oder mehr Ressourcen denselben externen ID-Wert haben, da die externe ID nur für die Identitätsquelle eindeutig ist.
  - Wenn mehrere Ressourcen mit einem externen ID-SCIM-Filter zurückgegeben werden, können die Ressourcen basierend auf der Quelldefinition der anfordernden Identitätsquelle aufgelöst werden.

Hinweis:
Eine Quelldefinition kann nur für die Identitätsquelle erstellt werden, die eine OAuth-Authentifizierungsmethode verwendet.

Prozedur

1. Navigieren zu **Alle** > **SCIM** > **Quellendefinition**.
2. Klicken Sie auf der Seite „SCIM-Quelldefinitionen“ auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

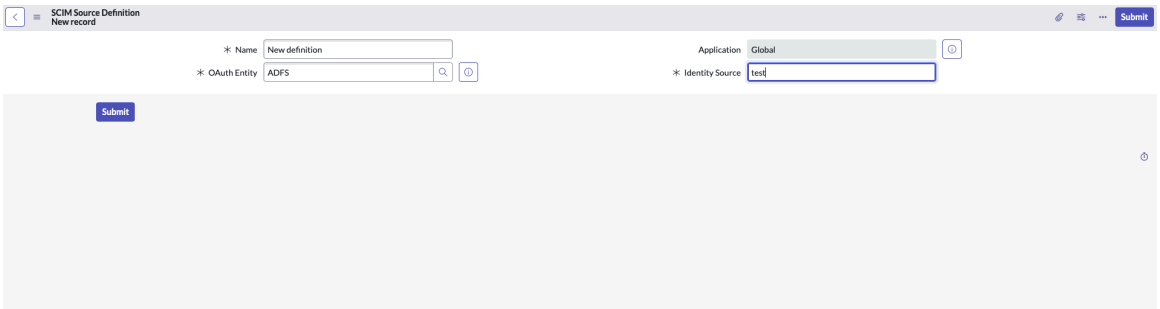
SCIM-Quellendefinition

Feld	Beschreibung
Name	Name der Quelldefinition.
Anwendung	Anwendungsbereich für diesen Datensatz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
OAuth-Entität	Die OAuth-Entität des Integrationsbenutzers. Die Entität wird für die Bereitstellung des Benutzers durch den Identitätsquellenanbieter verwendet.
Identitätsquelle	Der Name des Identitätsquellanbieters. Beispiele: Azure AD, Okta usw

Hinweis:
Aktivieren Sie die Eigenschaft `com.snc.integration.scim2.resolve.externalid.conflict`, um nur SCIM-Ressourcen zurückzugeben, die von der anfordernden Identitätsquelle erstellt wurden. Standardmäßig werden alle übereinstimmenden Ressourcen mit einem externen ID-Filter zurückgegeben.



4. Klicken Sie auf **Absenden**.

Ergebnisse
Die SCIM-Quelldefinition wird erstellt. Verwenden Sie die SCIM-ETL-Definitionen, um die Ressourcen basierend auf dem Erweiterungsschema in den Tabellen „sys_user“ und „sys_user_group“ zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM ETL-Definition.

SCIM-Client

Der SCIM-Client erleichtert die Bereitstellung und Aktualisierung von Identitätsressourcen durch CRUD-Vorgänge, die vom SCIM-Endpunkt auf einem externen System verfügbar gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Erfahren Sie mehr über den SCIM-Client.

Aktivieren

Aktivieren Sie den SCIM-Client.

Eigenschaften des SCIM-Clients

Erfahren Sie, wie Sie SCIM anpassen können.

Problembehandlung

Erfahren Sie mehr über die Quelldefinition für SCIM.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Client erkunden

Der SCIM-Client erleichtert die Bereitstellung und Aktualisierung von Identitätsressourcen durch CRUD-Vorgänge, die vom SCIM-Endpunkt auf einem externen System verfügbar gemacht werden.

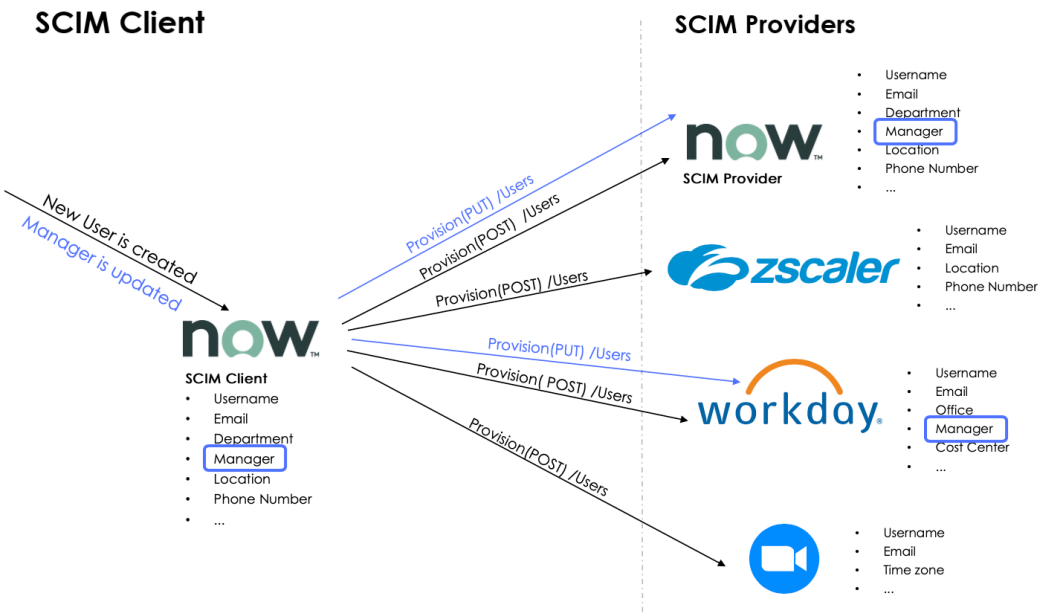
Der SCIM-Client wird zum Erstellen, Aktualisieren und Löschen von Identitätsressourcen in einem System verwendet, das SCIM-konforme REST-Anforderungen unterstützt. Der Client wird für die Identitätslebenszyklusverwaltung und für die Synchronisierung von Identitätsattributen zwischen [ServiceNow Instanzen oder zwischen ServiceNow und anderen SCIM-Providern verwendet.

Da die APIs vom Client verfügbar gemacht werden, können Sie den Prozess des Erstellens, Aktualisierens oder Löschens von Ressourcen für einen einzelnen oder mehrere SCIM-Provider automatisieren. Wenn beispielsweise ein Entwickler der Organisation beitritt, müssen Sie Zugriff auf Git, Arbeitsplatz usw. gewähren.

Mit dem SCIM-Client können Sie die folgenden Aktionen ausführen:

- Stellen Sie Identitäten und Zugriff für die Benutzer- oder Gruppenmitgliedschaft bereit.
- Identität und zugehörige Ressourcen mit SCIM-konformen Systemen synchronisieren
- Integrieren Sie einen beliebigen SCIM-Provider in ServiceNow®.
- Bereitstellung von Identitäten und Zugriff aufheben

Der SCIM-Client stellt skriptfähige APIs bereit, mit denen der Integrationsentwickler Workflows oder Automatisierungen erstellen kann, um bestimmte Aufgaben auszuführen. Weitere Informationen zur skriptfähigen API finden Sie unter SCIM2Client-API .



Konfigurationen für SCIM-Client

Führen Sie die folgenden Aufgaben aus, um den SCIM-Client zu konfigurieren:

- Erstellen Sie eine REST-Nachricht für alle ausgehenden Anrufe für einen bestimmten SCIM-Provider. Weitere Informationen finden Sie unter REST-Nachrichten erstellen.
- Erstellen Sie einen SCIM-Provider, um Ressourcentypen und Schemainformationen vom SCIM-Provider mit der REST-Nachricht abzurufen. Aktivieren Sie die Konfiguration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der HTTP-Methode (PUT oder PATCH), um eine Ressource im SCIM-Provider zu aktualisieren. Weitere Informationen finden Sie unter Erstellen Sie einen SCIM-Provider.

- Erstellen Sie die Zuordnungen von SCIM-Attributen zu ServiceNow -Attributen für einen bestimmten Ressourcentyp und SCIM-Provider. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Provider-Ressourcenzuordnung.
- Führen Sie die Zuordnung des SCIM-Felds zur Datenbanktabelle und zum Feldnamen durch. Übergeben Sie den Standardwert, oder schreiben Sie ein Skript, um den Wert abzurufen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Attributzuordnung.

Aktivieren Sie das SCIM-Client-Plugin

Installieren Sie für die Aktivierung des SCIM-Clients das Plugin „SCIM v2 – ServiceNow Cross-Domain Identity Management Client“ (com.snc.integration.scim2.client).

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „SCIM v2 - ServiceNow Cross-Domain Identity Management Client“ (com.snc.integration.scim2.client).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Eigenschaften, Tabellen, skriptfähige APIs und Protokolle des SCIM-Clients

Das Plugin „SCIM v2 – ServiceNow Cross-Domain Identity Management Client“ (com.snc.integration.scim2.client) enthält die folgenden Systemeigenschaften, Tabellen, skriptfähigen APIs und Protokolle.

Eigenschaften

SCIM-Client fügt die folgenden Systemeigenschaften hinzu.

Eigenschaften

Name	Beschreibung
`com.snc.integration.scim2.client.log.`	Diese Eigenschaft bestimmt, ob alle Protokolldatensätze oder nur die Fehlerprotokolldatensätze geschrieben werden sollen. Die möglichen Werte sind **FAILURE** oder **ALL**. Standardwert: **ALLE**

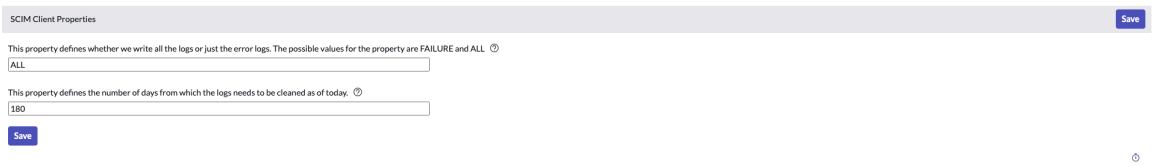
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften (Fortsetzung)

Name	Beschreibung
com.snc.integration.scim2.client.log.cleanup.duration	Diese Eigenschaft bestimmt die Anzahl der Tage zum Löschen der Protokolle. Standardwert: **180**

Um die Eigenschaften festzulegen, navigieren Sie zu **Alle** > **SCIM** > **Eigenschaften des SCIM-Clients**.



Tabellen

Der SCIM-Client fügt die folgenden Tabellen hinzu.

Tabellen

Name	Beschreibung
SCIM-Provider (sys_scim_provider)	Speichert Daten für jeden SCIM-Provider, z. B. Name, REST-Nachrichtenressourcendefinitionen usw.
SCIM-Provider-Ressourcenzuordnung (sys_scim_provider_resource_mapping)	Speichert die primären Tabelleninformationen für jeden Provider- und Ressourcennamen.
SCIM-Attributzuordnung (sys_scim_attribute_mapping)	Speichert die Quelldetails, aus denen jeder SCIM-Attributwert stammen soll, z. B. das Tabellenfeld, das Skript usw.
SCIM-Clientprotokoll (sys_scim_client_logs)	Speichert den Status jedes Anrufs, der beim SCIM-Provider ausgelöst wird.

Skriptfähige API

Die SCIM2Client-API ruft den System for Cross-Domain Identity Management (SCIM) Provider (Serverrolle) auf, um Daten in einem Service Provider (SP) zu erstellen, zu aktualisieren oder zu löschen. Die skriptfähige API des SCIM-Clients sollte in den Skripts verwendet werden, die im Systemkontext oder von einem Systemadministrator ausgeführt werden.

Beispielsweise können Sie das Skript verwenden, während Sie den Integration Hub-Workflow als Systembenutzer ausführen, während Sie die geplanten Aufgaben ausführen usw.

Im Folgenden finden Sie einige Anwendungsfälle für die Verwendung der skriptfähigen APIs:

- Als Administrator stellen Sie Identitätsinformationen aus Hintergrundskripts, Business Rules, Skripteinbindungsaufrufen, Workflows usw. bereit.
- Führen Sie als Administrator eine regelmäßige Aufgabe oder eine On-Demand-Aufgabe für die Identitätsbereitstellung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Führen Sie einen Workflow oder Sub-Workflow mit dem Skriptschritt mithilfe des skriptfähigen API-Aufrufs für die Bereitstellung aus.
- Fügen Sie das Bereitstellungsskript direkt in einer Business Rule oder Skripteinbindung hinzu. Das Skript kann von Nicht-Administratoren ausgelöst werden. Dieser Anwendungsfall funktioniert in den folgenden Situationen:
  - Der Benutzer hat Zugriff auf das Token, was bedeutet, dass der Benutzer die Rolle hat, das Token aus der REST-Vorlage zu generieren.
  - Der Benutzer hat Zugriff zum Abrufen der SCIM-Attributwerte aus den zugeordneten Tabellen.

Weitere Informationen zur skriptfähigen API finden Sie unter SCIM2Client-API .

SCIM-Clientprotokolle

Die SCIM-Clientprotokolle zeigen den Bereitstellungsstatus der SCIM-APIs an. Um den Bereitstellungsstatus anzuzeigen, navigieren Sie zu **Alle** > **SCIM** > **SCIM-Clientprotokolle**.

REST-Nachrichten erstellen

Konfigurieren Sie eine REST-Nachricht für alle ausgehenden Anrufe für einen bestimmten SCIM-Provider.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **Ausgehend** > **REST-Nachricht**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

SCIM-Anbieter

Feld	Beschreibung
Name	Beschreibender Name für diese Nachricht.
Endpunkt	Basis-URL des SCIM-Providers. Beispiel: `https://example.service-now.com/api/now/scim`.
Authentifizierungstyp	Typ der Authentifizierung, die für die Verbindung mit dem externen SCIM-Provider verwendet werden soll. Weitere Informationen finden Sie unter Ausgehende REST-Authentifizierung .
REST-Nachrichtenheader	Inhaltstyp, der vom externen SCIM-Provider erwartet wird. Zum Beispiel ist Headername der Inhaltstyp im folgenden API -Anforderungstext: Inhaltstyp: `application/scim+json`

4. Klicken Sie in der zugehörigen Liste „HTTP-Methoden“ auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Konfigurieren Sie die folgenden HTTP-Methoden.

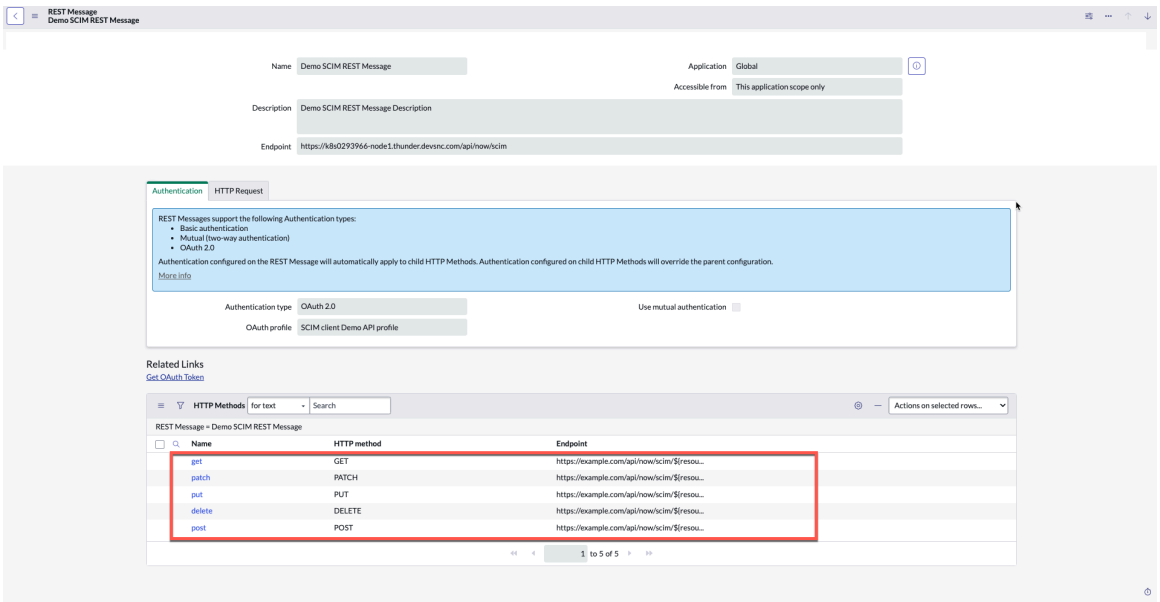
Hinweis:
Die URLs enthalten Variablen, die Sie ersetzen müssen.

HTTP-Methoden

REST-Nachrichtenfunktionen	Beispiel-URL
GET	https://example.com/api/now/scim/${resourceName}
PATCH	https://example.com/api/now/scim/${resourceName}/${resourceId}
PUT	https://example.com/api/now/scim/${resourceName}/${resourceId}
LÖSCHEN	https://example.com/api/now/scim/${resourceName}/${resourceId}
POST	https://example.com/api/now/scim/${resourceName}/${resourceId}

Hinweis:

- Sie müssen alle HTTP-Methoden für den Betrieb des SCIM-Clients erstellen.
- Das Basissystem enthält eine Beispiel-REST-Nachricht.



6. Klicken Sie auf **Absenden**.

Ergebnisse

Der REST-Nachrichtendatensatz wird erstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Verwenden Sie die REST-Nachricht, um einen SCIM-Provider zu erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen SCIM-Provider.

Weitere Informationen zum Erstellen einer REST-Nachricht finden Sie unter REST-Nachrichten erstellen .

Erstellen Sie einen SCIM-Provider

Erstellen Sie einen SCIM-Provider, um Ressourcentypen und Schemainformationen vom SCIM-Provider mit der REST-Nachricht abzurufen. Aktivieren Sie die Konfiguration der HTTP-Methode (PUT oder PATCH), um eine Ressource im SCIM-Provider zu aktualisieren.

Vorbereitungen

Hinweis:
Ein Beispiel-SCIM-Provider ist Teil des Basissystems. Sie können verwenden und basierend auf Ihren Anforderungen konfigurieren oder einen neuen Datensatz erstellen.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **SCIM-Client** > **SCIM-Anbieter**.
2. Klicken Sie auf der Seite „SCIM-Provider“ auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

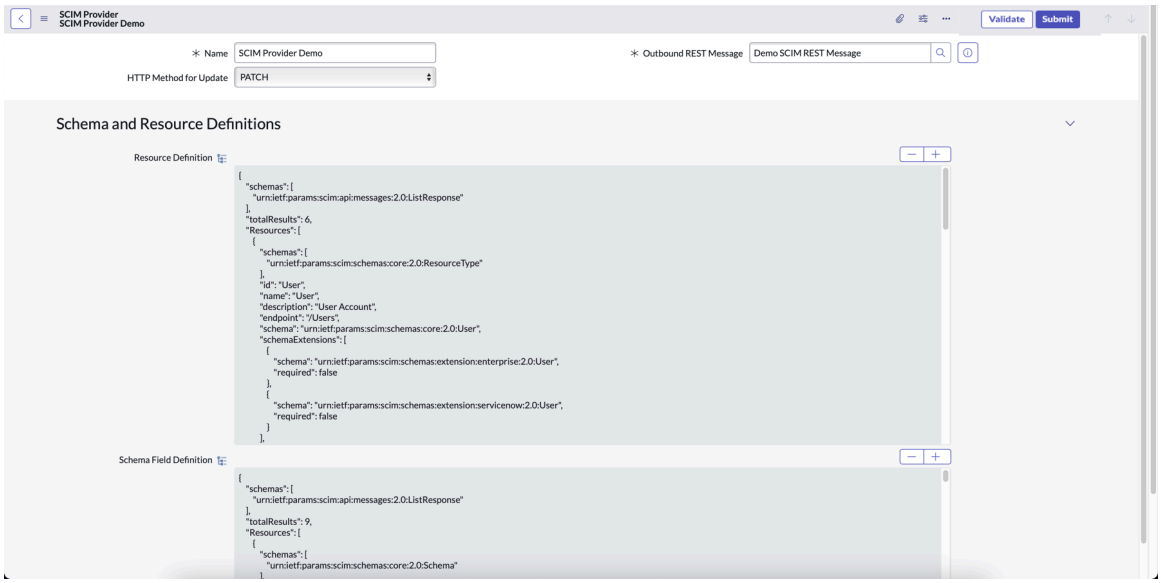
Formular „SCIM-Provider“

Feld	Beschreibung
Name	Name des SCIM-Providers
Ausgehende REST-Nachricht	Nachricht, die zum Aufrufen der API des SCIM-Providers verwendet wird. Weitere Informationen finden Sie unter REST-Nachrichten erstellen.
HTTP-Methode für Aktualisierung	Typ der HTTPS-Methode, die zum Aktualisieren der Ressourcenzuordnung verwendet wird. Die PATCH- oder PUT-Methode kann vom Client beim Aktualisieren der Identitätsressource während der Bereitstellung einer bereits vorhandenen Ressource verwendet werden.

Hinweis:

- Die Felder **Ressourcendefinition** und **Schemafelddefinition** werden aus den öffentlichen Endpunkten `/ResourceTypes` und `/Schemas` des SCIM-Providers abgerufen. Diese Felder werden automatisch ausgefüllt, nachdem die REST-Nachricht ausgewählt wurde.
- Wenn die REST-Nachricht, Schemas oder Ressourcentypen für den SCIM-Provider aktualisiert werden, klicken Sie auf Aktualisieren und dann auf **Aktualisieren**, um die **FelderRessourcendefinition** und **Schemafelddefinition** zu aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Absenden**.

Ergebnisse

Die SCIM-Provider-Details wurden erfolgreich erstellt. Verwenden Sie die SCIM-Provider-Ressourcenzuordnung, um die SCIM-Provider-Details den Ressourcen wie Benutzern oder Gruppen zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Provider-Ressourcenzuordnung.

Erstellen Sie eine SCIM-Provider-Ressourcenzuordnung

Definieren Sie die Zuordnungen von SCIM-Attributen zu ServiceNow -Attributen für einen bestimmten Ressourcentyp und SCIM-Provider.

Vorbereitungen

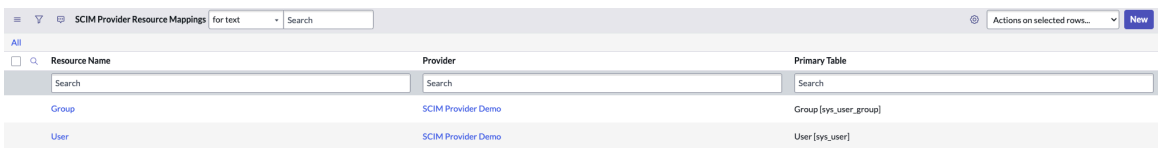
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **SCIM-Client** > **Ressourcenzuordnung des SCIM-Anbieters**.

   Die SCIM-Provider-Ressourcenzuordnung wird standardmäßig mit der Benutzer- und Gruppenzuordnung geliefert.

   Hinweis:
   Die Benutzer- oder Gruppenzuordnungen enthalten Beispielzuordnungen, die Sie als Referenz verwenden können. Sie können Zuordnungen auch basierend auf den Benutzer- oder Gruppenressourcen erstellen.

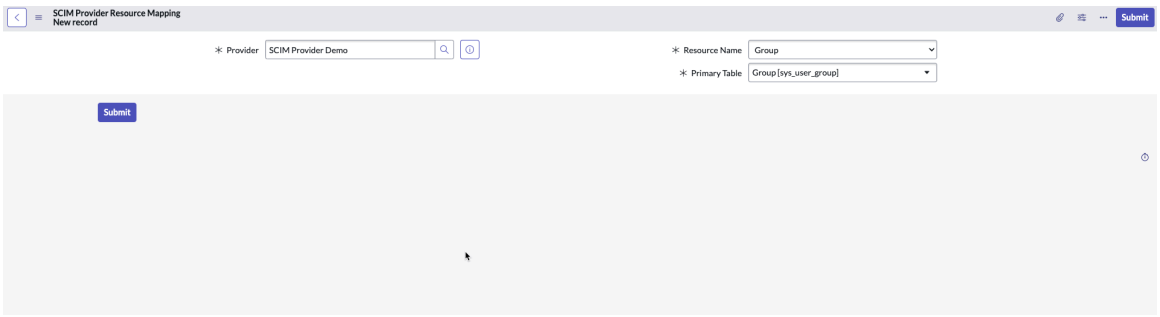


2. Erstellen Sie eine Ressourcenzuordnung, indem Sie auf **Neu**klicken.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenzuordnung

Felder	Beschreibung
Anbieter	Name des SCIM-Providers. Verweisen Sie beim Erstellen eines SCIM-Providers auf den konfigurierten Provider-Namen.
Ressourcenname	Ressource, für die die Zuordnung definiert werden muss.
Primäre Tabelle	Die Tabelle, die die sys_id der zugeordneten Ressource enthält.



4. Klicken Sie auf **Absenden**.

Ergebnisse
Der Datensatz wird erstellt und auf der Seite „SCIM-Provider-Ressourcenzuordnung“ angezeigt. Verwenden Sie die SCIM-Attributzuordnungen, um die Attribute aus Schemas weiter zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Attributzuordnung.

Erstellen Sie eine SCIM-Attributzuordnung

Erstellen Sie eine SCIM-Attributzuordnung, und verwenden Sie sie als einzelne Ressourcenquelle für die Tabellenfelder ServiceNow.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Im Folgenden finden Sie die Attributzuordnungstypen und ihre Beschreibungen.

Attributzuordnungstypen

Attributzuordnungstyp	Beschreibung
Direkt	Das SCIM-Attribut wird mithilfe der Felder **Datenbanktabellenname** und **Datenbankfeldname ausgefüllt**.
Konstante	Das SCIM-Attribut wird mit Hilfe eines angegebenen Standardwerts ausgefüllt.
Skript/Benutzerdefiniert	Das SCIM-Attribut wird mit Hilfe des Rückgabewerts eines Skripts ausgefüllt. Dieses Attribut erfordert die Aktivierung der Option „Skript ausführen“.

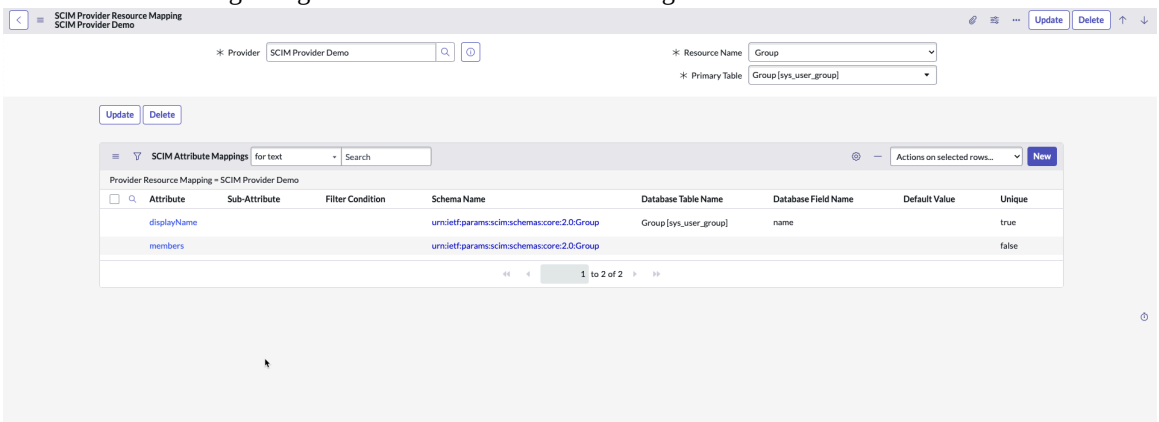
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Das Passwortattribut wird nicht unterstützt
- Eine Beispielattributzuordnung für die Benutzer- und Gruppenressourcen ist Teil des Basissystems. Sie können die Zuordnungen basierend auf Ihren Anforderungen verwenden und konfigurieren oder einen neuen Datensatz erstellen.

Prozedur

1. Navigieren zu **Alle** > **SCIM-Client** > **Ressourcenzuordnung des SCIM-Anbieters**.
2. SCIM-Ressourcenzuordnung ausgewählt, die für die Konfiguration erstellt wird.
3. Klicken Sie in der zugehörigen Liste SCIM-Attributzuordnungen auf **Neu**.



4. Füllen Sie die Felder des Formulars aus.

Formular „SCIM-Attributzuordnungen“.

Felder	Beschreibung
Ressourcenzuordnung des Anbieters	Attributzuordnung für eine Kombination aus Anbieter und Ressource. Wenn dieses Feld nicht automatisch ausgefüllt wird, verwenden Sie die Suchoption. Wählen Sie den Datensatz Provider-Ressourcenzuordnung aus.
Schemaname	Schemaname des SCIM-Attributs, für das die Zuordnung definiert werden muss. Zum Beispiel `urn:ietf:params:scim:schemas:core:2.0:User`.
Attribut	Attribut, für das die Zuordnung definiert werden muss. Zum Beispiel `userName`.
Unterattribut	Unterattribut (falls vorhanden), für das die Zuordnung definiert werden muss. Beispiel: Wenn ein komplexes Attribut wie `name.familyName`vorhanden ist, lautet

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	das Attribut **name** und das **Unterattribut FamilyName**.
Feldtyp	Datentyp des SCIM-Attributs. Dieses Feld wird automatisch aus den vom SCIM-Provider definierten Schemas ausgefüllt. Beispiel: **boolean**.
Mehrwertig	Mehrere Werte, die dem Attribut zugewiesen sind. Ein Attribut kann mehrere Werte haben, z. B. geschäftliche E-Mail-Adresse, private E-Mail-Adresse oder eine andere E-Mail-Adresse. Zum Beispiel *emails*. Dieses Feld wird mit den vom SCIM-Provider definierten Schemas ausgefüllt.
Filterbedingung	Einige mehrwertige Attribute können zusätzliche Informationen enthalten, die mithilfe einer Filterbedingungangegeben werden können. Die Auswahlmöglichkeiten der Filterbedingung werden anhand der vom SCIM-Provider definierten Schemas ausgefüllt. Zum Beispiel weist das Attribut *phoneNumbers* mehrere Typen auf, z. B. „Arbeit“, „Mobile“, „Zu Hause“ usw
Eindeutig	Option zum eindeutigen Identifizieren einer Ressource zwischen den SCIM-Client- und SCIM-Provider-Systemen. Mehrwertige Attribute können nicht als eindeutig markiert werden. Beispielsweise kann für eine Benutzerressource das Attribut *username* eindeutig gemacht werden.
Name der Datenbanktabelle	Verwenden Sie dieses Feld, um den Attributtabellennamen dem Tabellennamen ServiceNow zuzuordnen. Wenn Sie die direkte Attributzuordnung wählen, müssen Sie dieses Feld definieren. Beispielsweise kann das SCIM-Attribut *username* dem Feld **Benutzer** im Feld **Name der Datenbanktabelle** zugeordnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
Name des Datenbankfelds	DasFeld „Datenbankfeldname “ ordnet das SCIM-Attribut dem Feldnamen ServiceNow zu, der dem SCIM-Attribut zugeordnet werden soll. Wenn Sie die direkte Attributzuordnung wählen, müssen Sie dieses Feld definieren. Beispielsweise kann das SCIM-Attribut *username* dem Feld **Benutzer-ID** im Feld **Datenbankfeldname** zugeordnet werden.
Standardwert	Details zum Standardwert , der an den SCIM-Provider übergeben wird. Kann verwendet werden i, wenn die direkte Attributzuordnung des Feldsnull zurückgibt oder wenn der Standardwert verwendet werden kann, um einen hartcodierten Wert zurückzugeben. Bei einem hartcodierten Wert müssen der Name der Datenbanktabelle und der Feldname **None**lauten. Zum Beispiel kann der primäre Unterattributwert der geschäftlichen E-Mail als **true**hartcodiert werden.
Skript ausführen	Option zum Abrufen des Werts des Attributs per Skript. Diese Option ist für Attribute mit mehreren Werten erforderlich, die keine Filterbedingung enthalten. Für einen komplexen Attributtyp kann ein Skript den Wert auf Attribut- oder Unterattributebene bereitstellen. Zum Beispiel weist das Attribut **Mitglieder** der Gruppenressource keine Filterbedingung auf. Daher sollte die Skriptoption auf der übergeordneten Attributebene des Attributs **Mitglieder** definiert werden.
Skript	Skript, das zum Abrufen des Attributwerts verwendet wird. Der Rückgabetyp des Skripts muss eine Zeichenfolge oder ein als Zeichenfolge konvertiertes JSON sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Die Ausgabe des Skripts muss im richtigen Format vorliegen, wie vom Provider für dieses Attribut erwartet.

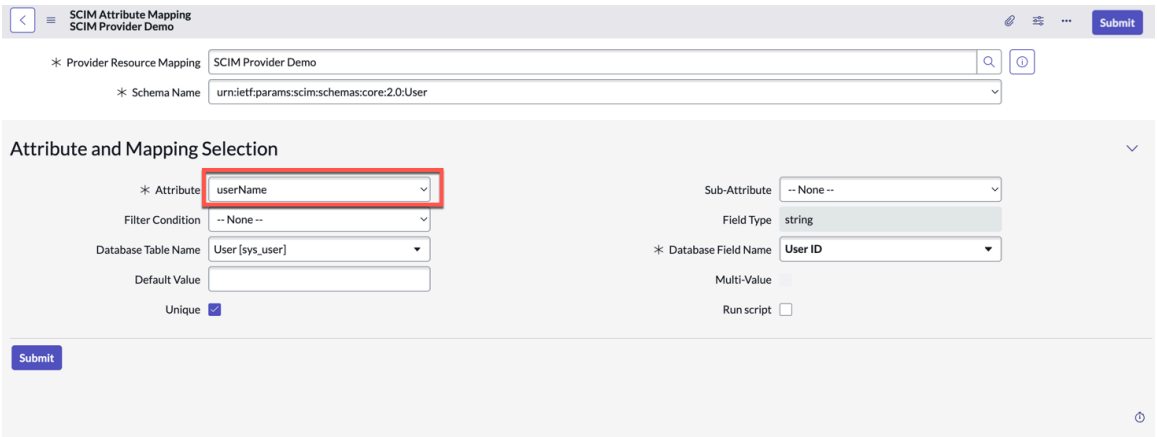
5. Klicken Sie auf **Absenden**.

Attributzuordnungsreferenzen

Mit den Attributzuordnungen können Sie die Attribute als einzelne Ressourcenquelle für die Tabellenfelder ServiceNow verwenden.

Attribut

Das Attribut, für das die Zuordnung definiert werden muss. Zum Beispiel *`userName`*.

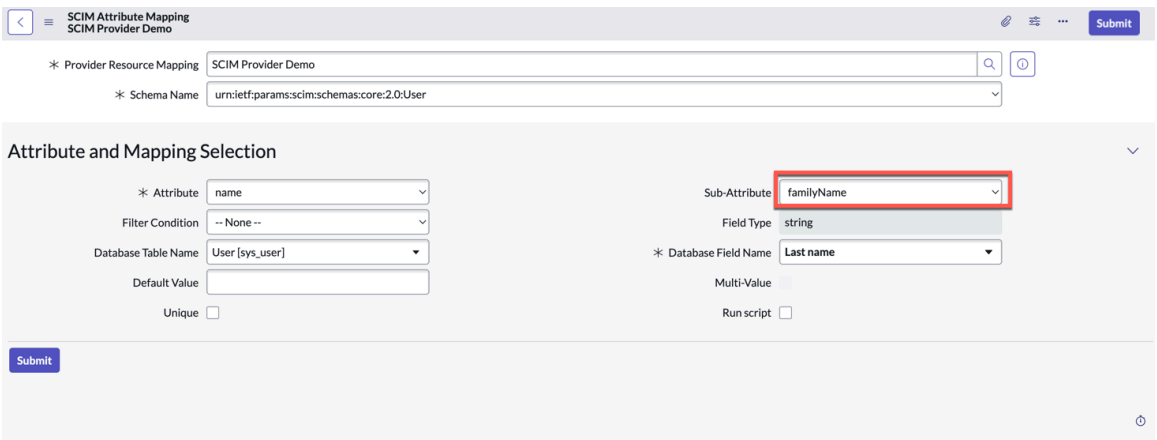


Unterattribut

Wählen Sie ggf. das Unterattribut aus, für das eine Zuordnung definiert werden muss.

Wenn beispielsweise ein komplexes Attribut wie *`name.familyName`*vorhanden ist, lautet das Attribut *`name`* und das Unterattribut *`familyName`*.

Für einfache Attribute wie den Benutzernamen **lautet der** Wert für **Unterattribut Keine**.



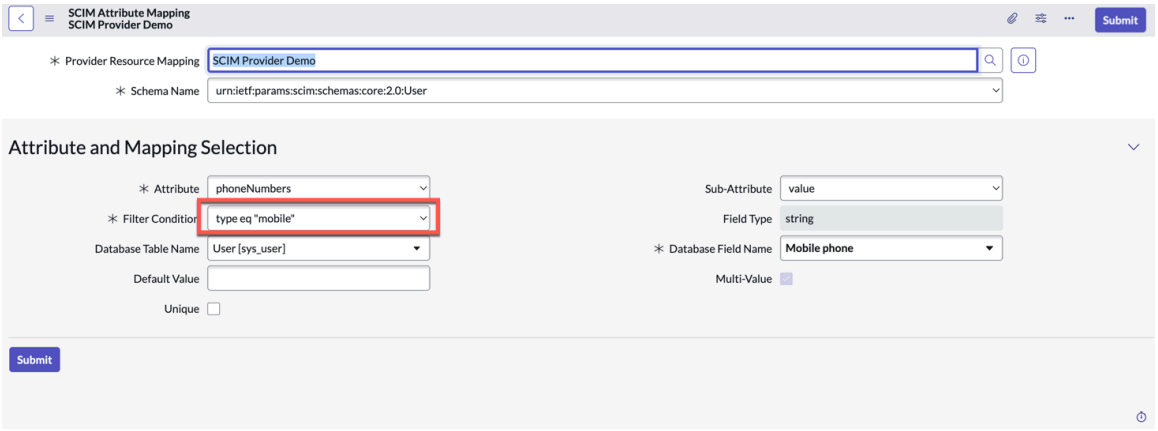
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterbedingung

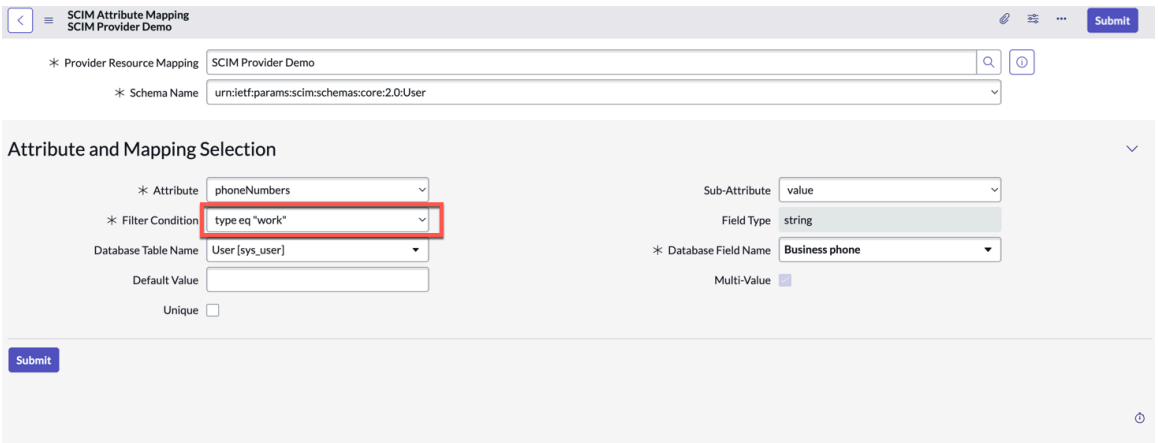
Ein Attribut mit mehreren Werten kann zusätzliche Informationen enthalten, die mithilfe einer Filterbedingung angegeben werden können. Die Auswahlmöglichkeiten für die Filterbedingung werden anhand der vom SCIM-Provider definierten Schemas ausgefüllt.

Zum Beispiel weist das Attribut *phoneNumbers* mehrere Typen auf, z. B. „Arbeit“, „Mobile“, „Zu Hause“ usw.

Sie können eine Filterbedingung aus einem Satz möglicher Werte angeben. Zum Beispiel kann das Attribut *phoneNumber* die Filterbedingung als **Typ eq "mobile"**haben.



Das Attribut *phoneNumber* kann stattdessen eine Filterbedingung **vom Typ eq "work"**haben.

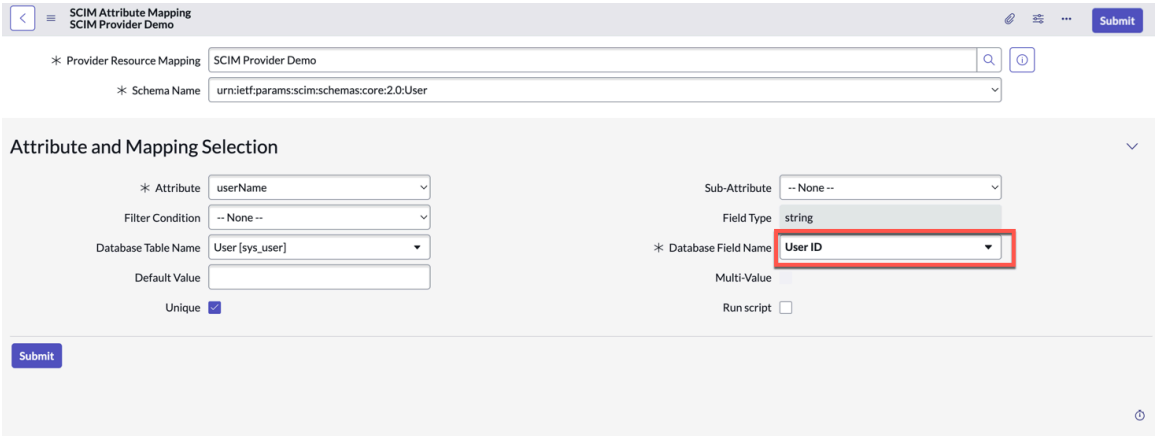


Name des Datenbankfelds

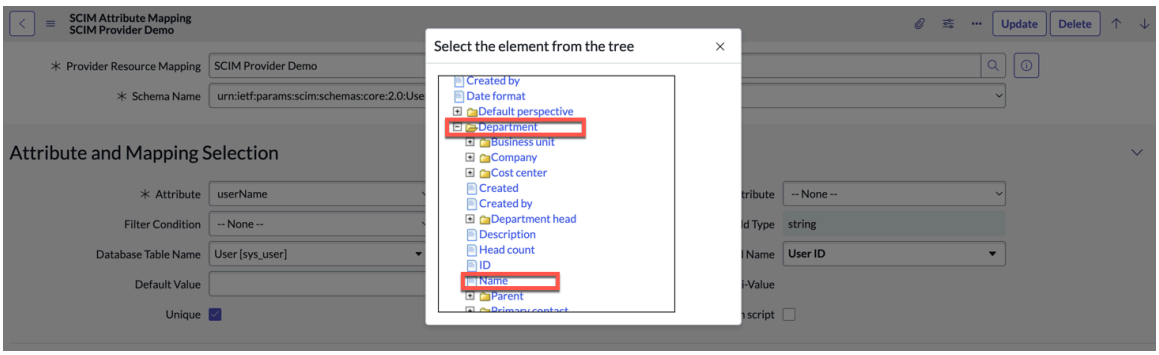
Wenn die Option für die direkte Attributzuordnung ausgewählt wird, muss dieses Attribut definiert werden. Das **Feld Datenbankfeldname** stellt den Feldnamen ServiceNow dar, der dem SCIM-Attribut zugeordnet ist.

Beispielsweise kann das SCIM-Attribut *username* einem Benutzer als Feld „ **Datenbanktabellenname** “ und dem Feld „Benutzer-ID“ als Feld „ **Datenbankfeldname** “ zugeordnet werden.

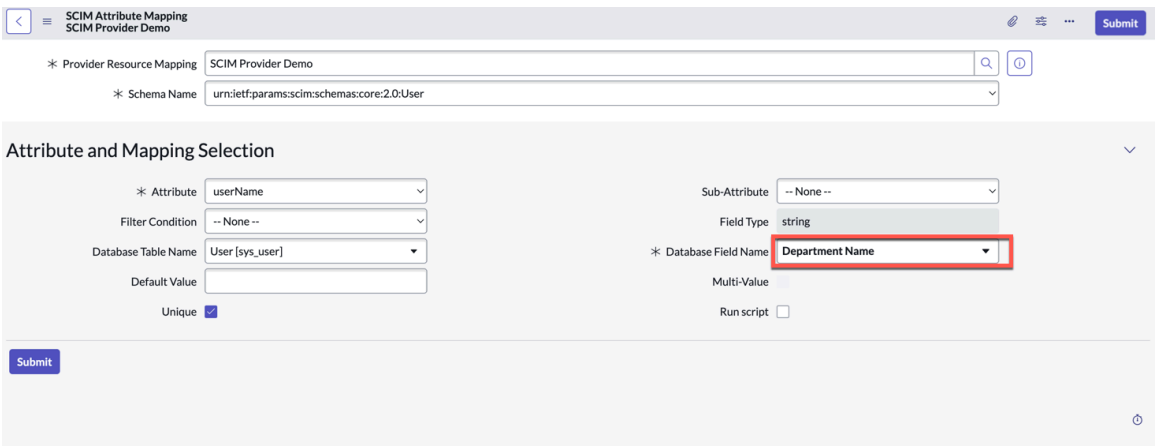
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können auch Dot-Walking mit dem **Datenbankfeldnamen durchführen**. Beispielsweise kann das SCIM-Attribut der **Abteilung** dem Feld **Abteilungsname** zugeordnet werden.



Hier ist die Datenbanktabelle **Benutzer** und der Name des Datenbankfelds lautet **Abteilungsname**.



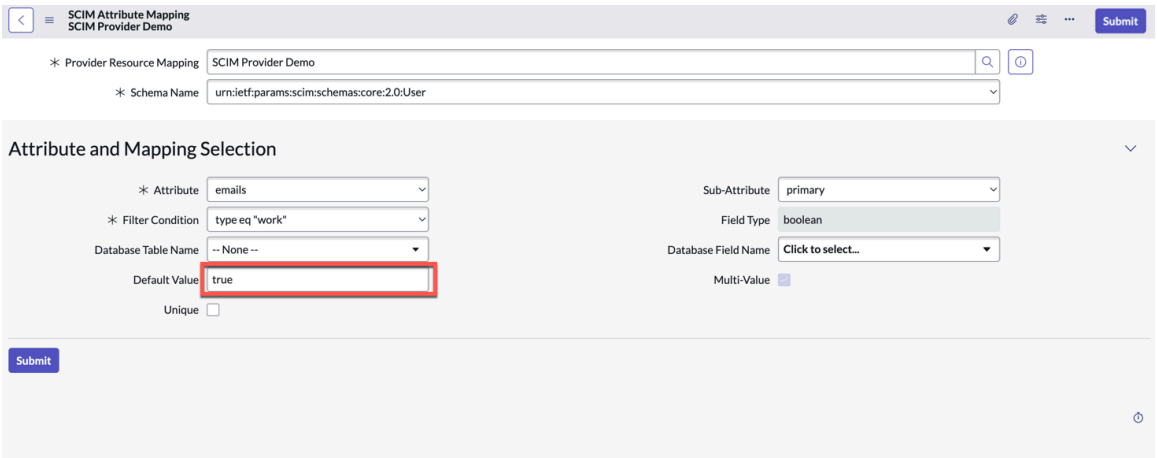
Standardwert

Der Standardwert wird an den SCIM-Provider übergeben, wenn die direkte Attributzuordnung dieses Felds NULL zurückgibt. Der Standardwert kann auch verwendet werden, um einen hartcodierten Wert zurückzugeben.

Bei einem hartcodierten Wert müssen der Name der Datenbanktabelle und der Feldname **None**lauten.

Zum Beispiel kann der primäre Unterattributwert der geschäftlichen E-Mail als **true**hartcodiert werden.

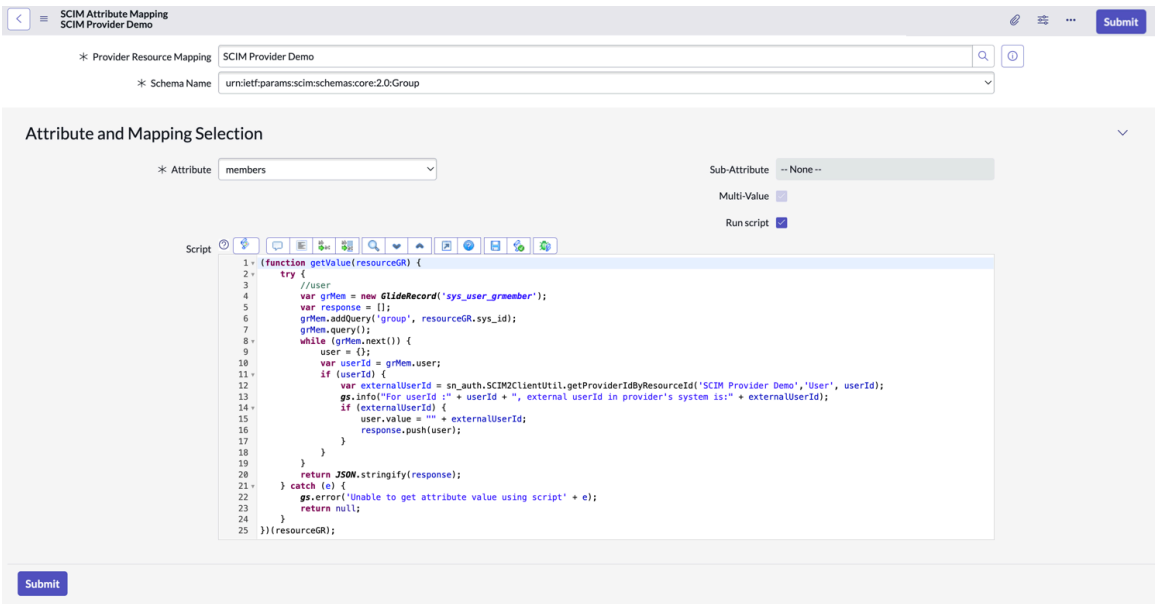
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Skript

Das Skript wird verwendet, um den Attributwert abzurufen. Der Rückgabetyp des Skripts muss immer eine Zeichenfolge oder ein als Zeichenfolge konvertiertes JSON sein. Die Ausgabe des Skripts muss im richtigen Format vorliegen, wie vom Provider für dieses Attribut erwartet.

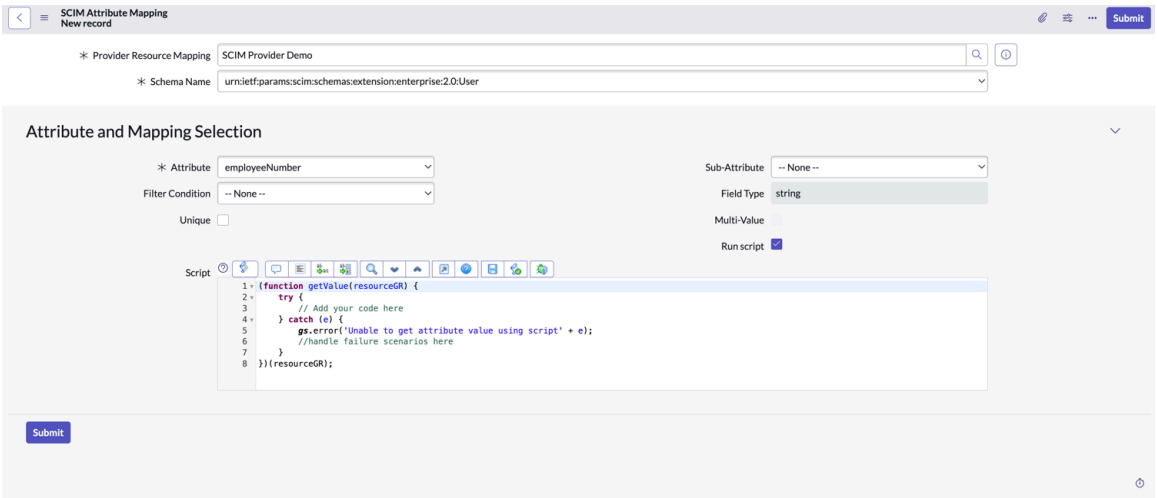
Das folgende Beispielskript zeigt ein mehrwertiges Attribut.



Die Ausgabe des Skripts muss ein JSON-Array in Zeichenfolgen enthalten.

Das Folgende ist ein Beispielskript für ein Attribut mit einfachem Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Ausgabe des Skripts muss eine Zeichenfolge sein.

Problembehandlung für SCIM-Client

Aktionen zur Problembehandlung können helfen, häufige Probleme beim Einrichten oder Ausführen des SCIM-Clients zu beheben.

Problembehandlung

Vorfall	Aktion
Antwort enthält die folgende Nachricht: `“message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"`	Die Nachricht wird angezeigt, wenn die API in einem Benutzerkontext aufgerufen wird und der Benutzer keinen Zugriff auf die Tabelle hat. Sie müssen sicherstellen, dass die skriptfähige API im Systemkontext aufgerufen wird.
Antwort enthält die folgende Nachricht: `{"message":"User Not Authenticated","detail":" Required to provide Auth information”}`	• Stellen Sie sicher, dass das Token durch die entsprechende REST-Nachricht generiert wird und gültig ist. • Stellen Sie sicher, dass die skriptfähige API im Systemkontext aufgerufen wird.
Antwort enthält die folgende Nachricht: `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	Wenn das Feld in der SCIM-Attributzuordnung so definiert ist, dass es aus einem Skript mit diesem Problem abgerufen wird, stellen Sie sicher, dass der Rückgabetyp immer eine Zeichenfolge sein muss.
Antwort enthält die folgende Nachricht: `"status": "400", "scimType": "invalidValue",`	Für jedes SCIM-Attribut, das die ID erwartet, gehört diese ID immer zum Provider-System. Stellen Sie sicher, dass die in der Nutzlast übergebene ID im Provider-System gültig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung (Fortsetzung)

Vorfall	Aktion
"detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"	

Bereiche, die für die Problembehandlung überprüft werden sollen

Im Folgenden sind einige der Bereiche aufgeführt, die bei Verwendung des SCIM-Clients auf Behebungsfehler überprüft werden können:

- Wenn beim Ausführen einer der skriptfähigen APIs ein Problem gefunden wird, lesen Sie den Abschnitt „SCIM-Client-Protokolle“.

Protokollfelder

Feld	Beschreibung
Anforderungs-ID	Eindeutige ID, die eine skriptfähige API namens darstellt.
SCIM-Anbieter	Anbietername, für den die API aufgerufen wird.
Ressource	Name der Ressource, für die die API aufgerufen wird.
Ressourcen-ID	ID, für die die API aufgerufen wird. Beim Löschen stellt die ID die Ressourcen-ID im Provider-System dar, und die ID befindet sich im Client-System.
Aktion	API, die aufgerufen wird
Status	Status des Protokolls als Erfolg oder Fehler
Nachricht	Erfolgs- oder Fehlermeldung. Die Fehlermeldung kann vom SCIM-Provider oder aufgrund von Konfigurationsproblemen im SCIM-Client stammen.

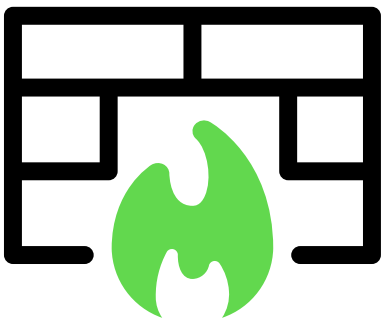
- Überprüfen Sie den Anforderungstext, indem Sie ausgehende Anrufe konfigurieren und anzeigen. Weitere Informationen finden Sie unter Protokollierung für ausgehende Webservices .
- Aktualisieren Sie Protokollebenen, indem Sie den Inhaltstyp hinzufügen, das Beispiel testen und in der REST-Nachricht des entsprechenden Providers zum entsprechenden HTTP-Methodenformular navigieren.
- Wenn der Anforderungstext abgeschnitten ist, erhöhen Sie den Grenzwert mithilfe der Systemeigenschaft `glide.outbound_http.content.max_limit`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsverwaltung

Mit Access Management haben Sie sicheren Zugriff auf die Instanz ServiceNow®.

Authentifizierung

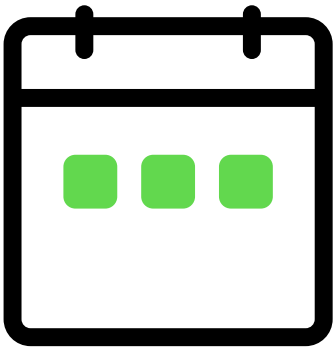


ServiceNow® Die Authentifizierung von überprüft die Identität eines Benutzers, der auf eine Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Auftragsfunktion des Benutzers entsprechen.

Verbindung und Anmeldeinformationen

Anmelde- und Verbindungsinformationen sind erforderlich, um auf einen Computer oder ein Netzwerkgerät für Discovery, Service-Mapping und Cloud-Management zuzugreifen oder um mit Orchestration zu arbeiten.

Sicherheit bei Anmeldung und Authentifizierung



Konfigurieren Sie Anmeldesicherheitsoptionen, um den Zugriff auf Ihre Instanz zu steuern.

Webservice-Sicherheit

Erzwingen Sie Sicherheit mithilfe von Basic Authentication, gegenseitiger Authentifizierung oder WS-Security.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierung

ServiceNow®Die Authentifizierung von überprüft die Identität eines Benutzers, der auf eine Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Auftragsfunktion des Benutzers entsprechen.

Verbindung und Anmeldeinformationen

Anmelde- und Verbindungsinformationen sind erforderlich, um auf einen Computer oder ein Netzwerkgerät für Discovery, Service-Mapping und Cloud-Management zuzugreifen oder um mit Orchestration zu arbeiten.

Sicherheit bei Anmeldung und Authentifizierung

Konfigurieren Sie Anmeldesicherheitsoptionen, um den Zugriff auf Ihre Instanz zu steuern.

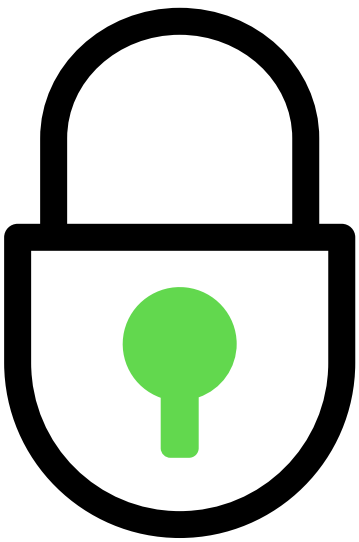
Webservice-Sicherheit

Erzwingen Sie Sicherheit mithilfe von Basic Authentication, gegenseitiger Authentifizierung oder WS-Security.

Authentifizierung

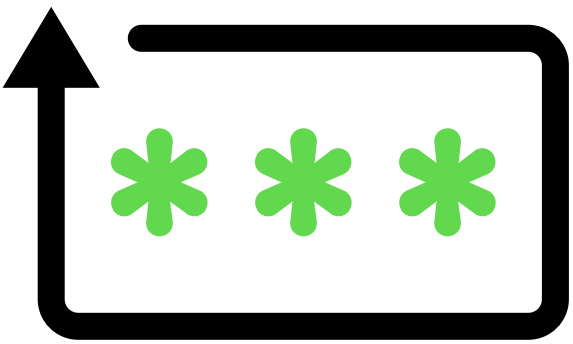
ServiceNow®Die Authentifizierung von überprüft die Identität eines Benutzers, der auf eine Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Auftragsfunktion des Benutzers entsprechen.

Erste Schritte



Single Sign-on (SSO) für mehrere Anbieter

Benutzername und Passwort, die in Identitätsanbietern konfiguriert sind, die über einen übereinstimmenden Benutzeraccount in der Datenbank verfügen.

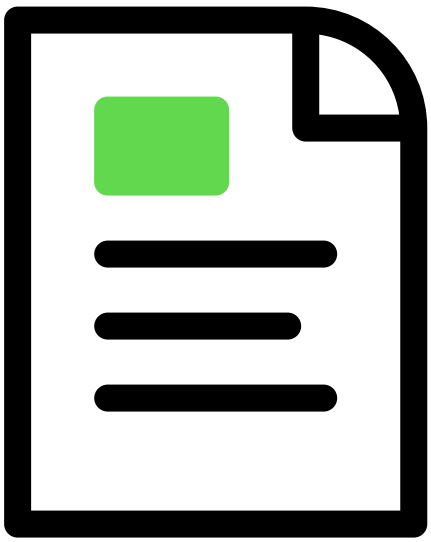


OAuth eingehend und ausgehend

Benutzername und Passwort des OAuth-Identitätsanbieters, der über einen übereinstimmenden Benutzeraccount in der Datenbank verfügt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

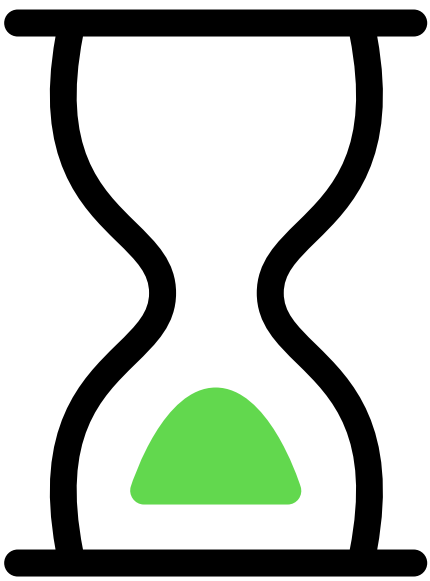


API-Zugriffsrichtlinie

Die API-Zugriffsrichtlinie definiert die Berechtigungen und die Dauer des Zugriffs auf eine API.

Digest-Token-Authentifizierung

Benutzername und Geheimnis in der Tabelle führen einen benutzerspezifischen Hash-Vorgang aus, z. B. SHA1, SHA 256 oder MD5. Dieser Wert muss als Teil des URL-Suffixes angehängt werden, das für den Abfrageparameter funktioniert.



Zeitlich begrenzte Authentifizierung

Multifaktor-Authentifizierung (MFA)

Passcode aus QR-Code, der unten einen Geheimcode mit Informationen wie Instanzname, Benutzername oder Benutzerkontoinformationen und Code für die Authentifizierung enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

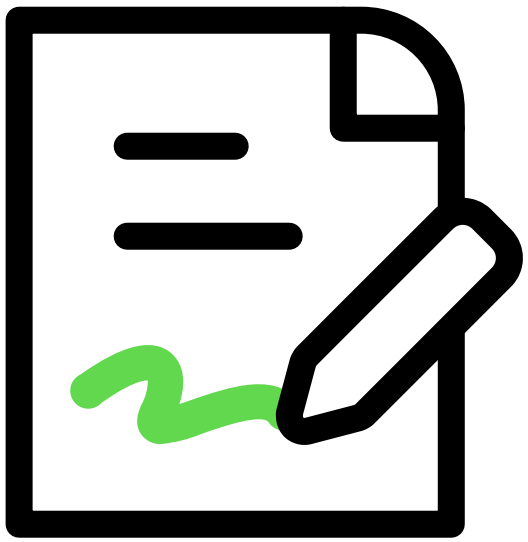
Konfigurieren Sie die linkbasierte Authentifizierung auf der

[qa: BEGIN review][End]

ServiceNow-Instanz Der konfigurierte Link kann per E-Mail oder SMS für den Benutzer freigegeben werden, und der Benutzer kann sich über diese Links bei der Instanz anmelden.

Zertifikatsbasierte Authentifizierung

Eindeutige PEM-codierte Zertifikate, die Benutzern anstelle von Benutzername und Passwort zugeordnet werden.



Selbstregistrierung

Benutzername und Passwort in ihrem Benutzerdatensatz in der Instanzdatenbank.

Zero Trust-Zugriff

LDAP

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zero Trust Access stellt sicher, dass jeglicher Zugriff auf Anwendungen und Daten erst nach Identitätsverifizierung und Risikobewertung des Benutzers auf der Grundlage der geringsten Berechtigung gewährt wird.	Benutzername und Passwort in ihrem LDAP-Konto, das über ein übereinstimmendes Benutzerkonto in der Datenbank verfügt.

Sie können verschiedene Methoden verwenden, um Benutzer zu authentifizieren. Benutzeranmeldeinformationen werden für jede Methode mit anderen gespeicherten Anmeldeinformationen abgeglichen.

Hinweis:

- Das SSO-Plugin Okta ist veraltet.
- Weitere Informationen zu den Sicherheitseigenschaften, die sich auf die Autorisierungsverarbeitung auswirken, finden Sie unter Zugriffskontrolle in Härtungseinstellungen für Instanzsicherheit.
- Sie können die SAML- und Digest-Authentifizierung über die Anwendung Mehrfachanbieter-SSO verwenden.

Adaptive Authentifizierung

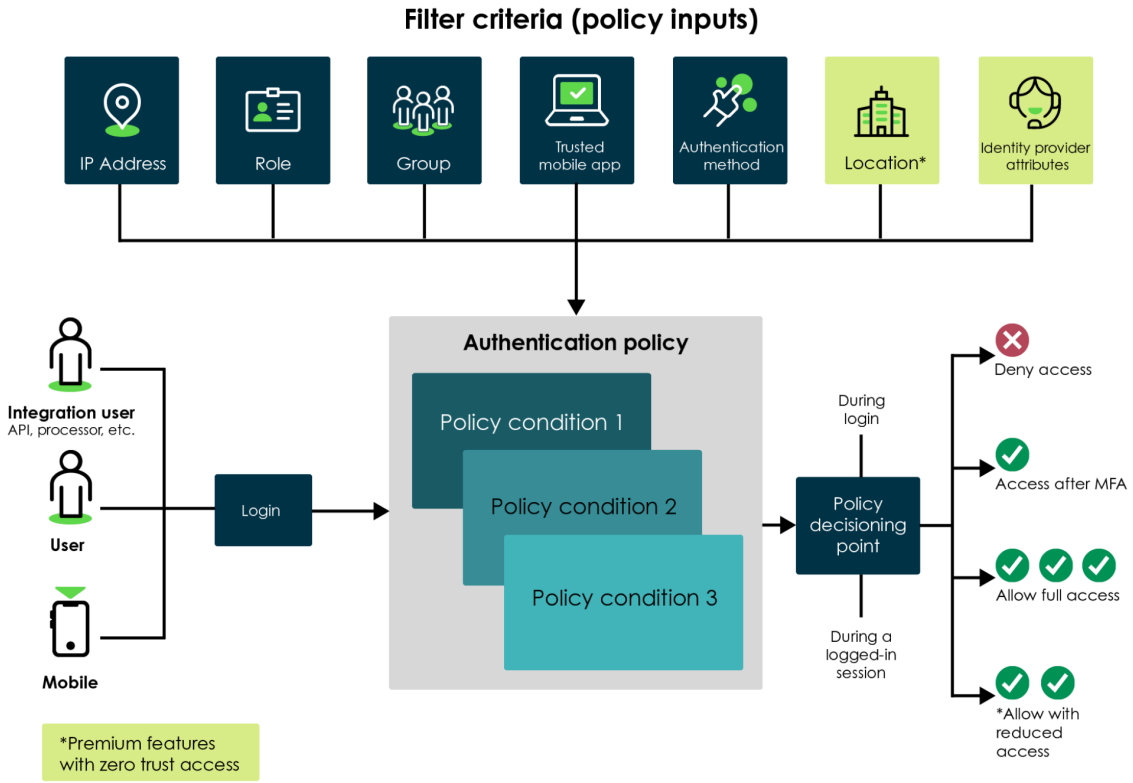
Verwenden Sie das Framework für adaptive Authentifizierungsrichtlinien, um kontextbezogene Authentifizierungskontrollen für die richtigen Benutzer zum richtigen Zeitpunkt durchzusetzen. Die adaptive Authentifizierung verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten und dann basierend auf den angegebenen Richtlinienbedingungen den Zugriff auf Ihre Instanz entweder zu verweigern oder zuzulassen.

Verwenden Sie Richtlinien und Kontexte für die adaptive Authentifizierung, um den Zugriff auf Ihre Instanz für Benutzer und APIs basierend auf Kriterien wie IP-Adresse, Benutzerrolle und Benutzergruppe einzuschränken. Sie können die integrierten Authentifizierungsrichtlinien entsprechend Ihren Sicherheitsanforderungen konfigurieren.

Beispielsweise kann ein Administrator *`Allow Access Policy`* so konfigurieren, dass Anmeldungen von Benutzern nur innerhalb eines vertrauenswürdigen Bereichs von IP-Adressen zugelassen werden, die Mitglieder einer bestimmten Rolle sind. Bei Zuweisung zu *`Post-authentication context`*verweigert die Zugriffsrichtlinie den Zugriff von nicht vertrauenswürdigen IP-Adressen.

Um eine benutzerdefinierte Nachricht in der Sprache Ihrer Instanz festzulegen, müssen Sie Schlüssel und Wertpaar in sys_ui_message.list hinzufügen und den sys_ui_message-Datensatz aktualisieren. Wenn Sie sich mit einem falschen Passwort anmelden, wird die benutzerdefinierte Nachricht in der bevorzugten Sprache angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Komponenten der adaptiven Authentifizierung

Authentifizierungsrichtlinien

Authentifizierungsrichtlinien werten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen aus und erlauben oder verweigern den Zugriff abhängig von der Ausgabe der Auswertung der Richtlinienbedingungen. Beispielsweise ist der Zugriff nur zulässig, wenn alle in der **Zugriffsrichtlinie angegebenen Richtlinienbedingungen** als „wahr“ ausgewertet werden.

Authentifizierungsrichtlinien verwenden Informationen, die von Filterkriterien bereitgestellt werden, um sie mit den Bedingungen der Richtlinie zu vergleichen und zu bestimmen, ob Zugriff auf die Instanz gewährt werden soll. Beispielsweise stellt ein Filterkriterium die IP-Adresse eines Benutzers bereit, und eine Richtlinienbedingung bestimmt, ob sich diese Adresse innerhalb des angegebenen Bereichs befindet, bevor Zugriff gewährt wird. Weitere Informationen zu Authentifizierungsrichtlinien finden Sie unter Authentifizierungsrichtlinien.

Kontexte der Authentifizierungsrichtlinie

Authentifizierungsrichtlinienkontexte definieren, wie und wann Richtlinien während des Anmeldevorgangs erzwungen werden. Der Vorauthentifizierungskontext wird ausgeführt, bevor dem Benutzer ein Anmeldebildschirm angezeigt wird. Der Kontext nach der Authentifizierung wird ausgeführt, nachdem der Benutzer seine Anmeldeinformationen eingegeben hat. Um eine Richtlinie zu verwenden, muss sie einem Richtlinienkontext zugewiesen werden. Weitere Informationen zu diesen Kontexten finden Sie unter Kontexte der Authentifizierungsrichtlinie.

Filterkriterien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterkriterien (auch Richtlinieneingaben genannt) werden als Eingaben für Richtlinienbedingungen verwendet. Richtlinienbedingungen verwenden diese Eingaben, um die Anforderungen von Authentifizierungsanforderungen zu überprüfen und zu erfüllen. Diese Eingaben enthalten Informationen wie Benutzerrolle, IP-Bereich und Identitätsanbieter. Weitere Informationen zu Filterkriterien finden Sie unter Filterkriterien.

Authentifizierungseigenschaften

Verwenden Sie Authentifizierungseigenschaften, um zu steuern, ob die adaptive Authentifizierung für Ihre Instanz aktiv ist. Sie können auch Eigenschaften verwenden, um das Debugging zu aktivieren, und definieren, welche Messaging-Benutzer angezeigt werden, wenn der Zugriff blockiert wird. Weitere Informationen zu diesen Eigenschaften finden Sie unter Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.

REST API-Zugriffsrichtlinien

Sie können die Filterkriterien des adaptiven Authentifizierungs-Frameworks verwenden, um den Zugriff auf eingehende ServiceNow REST APIs einzuschränken. Weitere Informationen finden Sie unter REST API-Zugriffsrichtlinien.

Domänentrennung und adaptive Authentifizierung

Die adaptive Authentifizierung wird für domänengetrennte Instanzen auf der Ebene der Authentifizierungsrichtlinienbedingung unterstützt. Richtlinienbedingungen wirken sich auf die **Domäne** im Datensatzdomäne-Feld [sys_domain] aus. Richtlinienbedingungen in der globalen Domäne wirken sich auf alle Domänen aus.

Aktivieren Sie die adaptive Authentifizierung

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „ Adaptive Authentifizierung “ (com.snc.adaptive_authentication) für die adaptive Authentifizierung aktivieren.

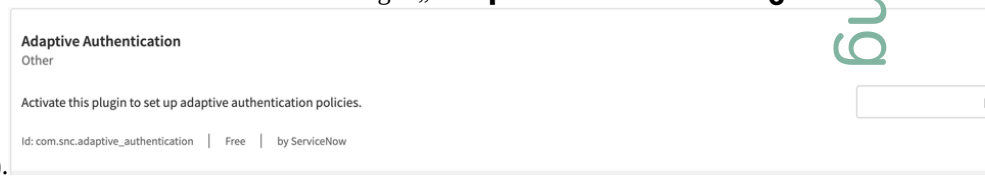
Vorbereitungen

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „ **Adaptive Authentifizierung** “ (com.snc.adaptive_authentication).



Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

> **Hinweis:**
> Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nächste Maßnahme

Konfigurieren Sie Ihre Authentifizierungsrichtlinien, um kontextbezogene Authentifizierungskontrollen für Ihre Instanz zu erzwingen.

Sobald Ihre Richtlinien konfiguriert sind. Aktivieren Sie die adaptive Authentifizierung mithilfe der **Richtlinie** „Authentifizierungsrichtlinie aktivieren“. Weitere Informationen zu den Eigenschaften der adaptiven Authentifizierung finden Sie unter Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.

Filterkriterien

Filterkriterien (auch Richtlinieneingaben genannt) werden als Eingaben für Richtlinienbedingungen verwendet, um die Anforderungen einer Authentifizierungsanforderung zu überprüfen und zu erfüllen.

Verwenden Sie Filterkriterien, um Richtlinien für die Informationsauthentifizierung bereitzustellen, z. B. IP-Adresse, Rollen oder Gruppen eines Benutzers. Fügen Sie diese Kriterien im Abschnitt **Richtlinienbedingungen** Ihrer Richtlinien hinzu.

Bei der adaptiven Authentifizierung werden sieben Arten von Filterkriterien verwendet. Ihre Authentifizierungsrichtlinien können eines oder mehrere dieser Kriterien verwenden, um Authentifizierungsanforderungen auszuwerten.

Filterkriterientypen

Typ	Beschreibung
IP-Filterkriterien	Verwenden Sie IP-Filterkriterien, um Benutzer basierend auf ihren IP-Adressen zu filtern. Sowohl IPv4 als auch IPv6 werden unterstützt.
Rollenfilterkriterien	Verwenden Sie Rollenfilterkriterien, um Benutzer basierend auf ihren Rollen zu filtern.
Gruppenfilterkriterien	Verwenden Sie Gruppenfilterkriterien, um Benutzer basierend auf der Benutzergruppe zu filtern, der der Benutzer angehört.
Standortfilterkriterien	Verwenden Sie Standortfilterkriterien, um Benutzer basierend auf dem Benutzerstandort zu filtern.
Filterkriterien für Identitätsanbieterattribut	Verwenden Sie die Attribute des Identitätsanbieters, die von der SAML-Antwort vom IdP empfangen werden, als Filterkriterien für die Authentifizierung.

Allgemeine Kriterien

Zusätzlich zu den zuvor aufgeführten Typen gibt es vier generische Filterkriterien. Diese Kriterien werden nicht in Ihrem Filternavigator angezeigt, Sie können sie jedoch auswählen, wenn Sie Ihren Authentifizierungsrichtlinien Richtlinieneingaben hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Generische Filterkriterientypen

Typ	Beschreibung
Authentifizierungsschema	Verwenden Sie diese Option, um basierend auf dem Authentifizierungsschema des Anwenders zu filtern. Dieses Kriterium ist ein Auswahltyp mit zwei Optionen: • Benutzername und Passwort, die eine lokale Anmeldung kennzeichnen • SSO, was eine auf Multi-SSO (SAML, OIDC oder Digest) basierende Anmeldung bezeichnet. **Hinweis:** Diese Filterkriterien sind nur verfügbar, wenn das Plugin „ **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter**“ [com.snc.integration.sso.multi.installer] installiert ist.
Identitätsanbieter	Verwenden Sie diese Option, um basierend auf dem Identitätsanbieter des Benutzers zu filtern. Verwenden Sie diese Option zusammen mit den Kriterien des Authentifizierungsschemas, um eine granulare Steuerung des Anmeldevorgangs zu erhalten. Dieses Kriterium verweist auf die Tabelle „ **Identitätsanbieter** “ [sso_properties]. **Hinweis:** Diese Filterkriterien sind nur verfügbar, wenn das Plugin „ **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter**“ [com.snc.integration.sso.multi.installer] installiert ist.
Rollenbasierte MFA	Verwenden Sie diese Option, um basierend auf der rollenbasierten MFA-Funktion zu filtern. Dieses Kriterium ist ein boolesches Filterkriterium, das angibt, ob rollenbasierte MFA für den Benutzer aktiviert ist
Benutzerbasierte MFA	Verwenden Sie diese Option, um basierend auf der benutzerbasierten MFA-Funktion zu filtern. Dieses Kriterium ist ein boolesches Filterkriterium, das angibt, ob benutzerbasierte MFA für den Benutzer aktiviert ist
Vertrauenswürdige Mobile-App	Vertrauenswürdiger Filter für Mobile-Apps zum Aktivieren des Instanzzugriffs über die Mobile-App.

IP-Filter

Verwenden Sie IP-Filterkriterien, um die Benutzer basierend auf den IP-Adressen der Benutzer zu filtern. Sowohl IPv4 als auch IPv6 werden unterstützt.

Mit IP-Filterkriterien können Sie Benutzer basierend auf ihren IP-Adressen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich zuzulassen oder zu verweigern.

Erstellen Sie IP-Filterkriterien

Mit IP-Filterkriterien können Sie Benutzer basierend auf ihren IP-Adressen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich zuzulassen oder zu verweigern.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

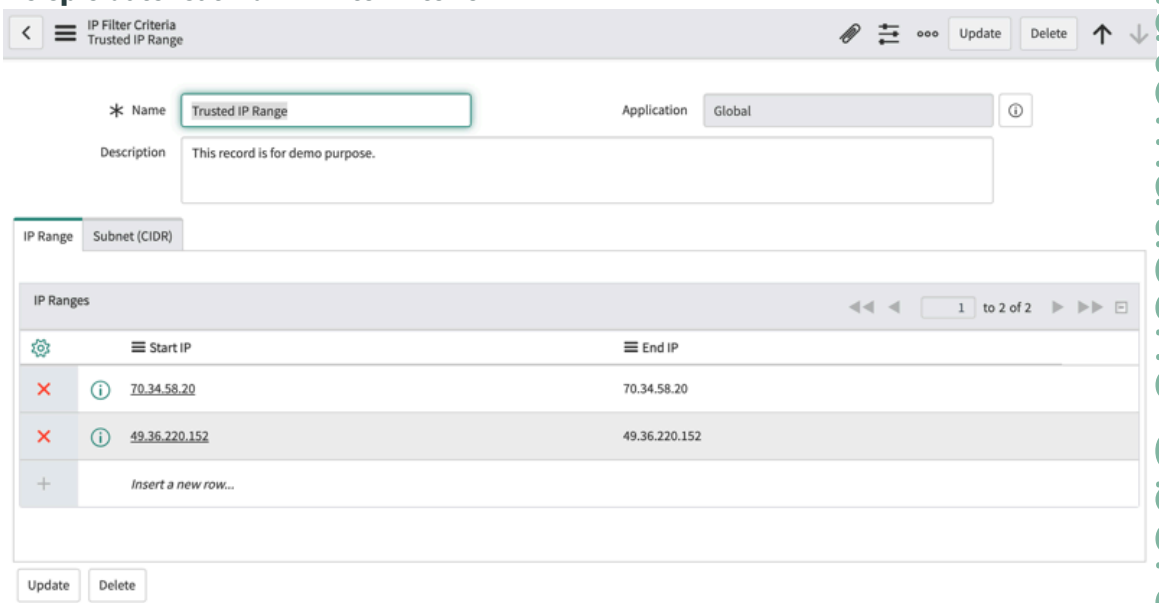
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **IP-Filterkriterien**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „IP-Filterkriterien“.

Feld	Beschreibung
Name	Name zur Identifizierung des IP-Netzwerks
Beschreibung	Kurzbeschreibung des IP-Netzwerks
Anwendung	Umfang der Anwendung.

Beispieldatensatz für IP-Filterkriterien



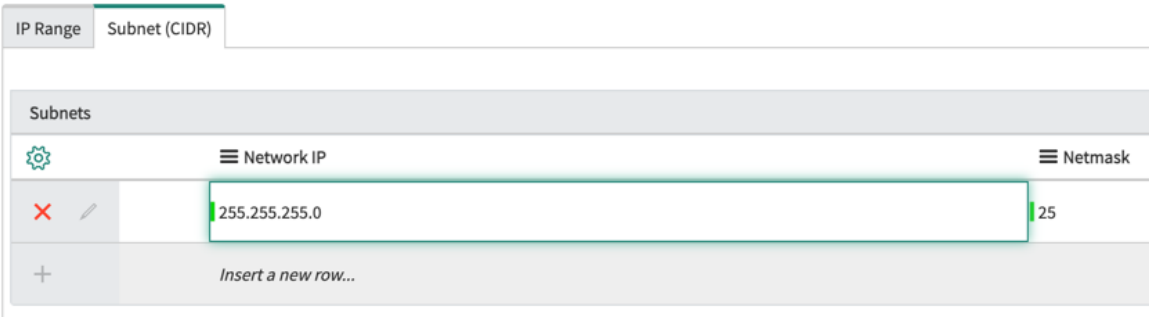
4. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
5. Doppelklicken Sie auf der Registerkarte **IP** -Bereich auf **Neue Zeile einfügen**.
   Sie können eine einzelne IP-Adresse oder mehrere IP-Adressbereiche eingeben. Geben Sie beispielsweise für einen Bereich von IP-Adressen 192.0.2.0 in die Spalte „ **Start-IP** “ und 192.0.2.255 in die Spalte „ **End-IP** “ ein.

Hinweis:
Stellen Sie für eine einzelne IP-Adresse sicher, dass Sie dieselbe IP-Adresse in die Spalten **Start-IP** -Adresse und **End-IP** eingeben. Wenn Sie eine IP-Adresse in die Spalte „ **Start-IP** “ eingeben, lassen Sie die Spalte „ **End-IP** “ leer, und speichern Sie den Datensatz. Die Spalte „ **End-IP** “ wird automatisch mit derselben **Start-IP** -Adresse ausgefüllt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Doppelklicken Sie auf der Registerkarte **Subnetz (CIDR)** auf **Neue Zeile einfügen**.
   Geben Sie die Netzwerk-IP-Adresse und die Netzmaske im CIDR-Format (Classless Inter-Domain Routing) ein. Geben Sie beispielsweise 255.255.255.0 als Netzwerk-IP und 25 als Netzmaske ein.



Rollenfilter

Verwenden Sie Rollenfilterkriterien, um Benutzer basierend auf ihren Rollen zu filtern.

Mit Rollenfilterkriterien können Sie Benutzer basierend auf den Rollen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine Liste von Benutzerrollen zuzulassen oder zu verweigern.

Erstellen Sie Rollenfilterkriterien

Mit Rollenfilterkriterien können Sie Benutzer basierend auf den Rollen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine Liste von Benutzerrollen zuzulassen oder zu verweigern.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

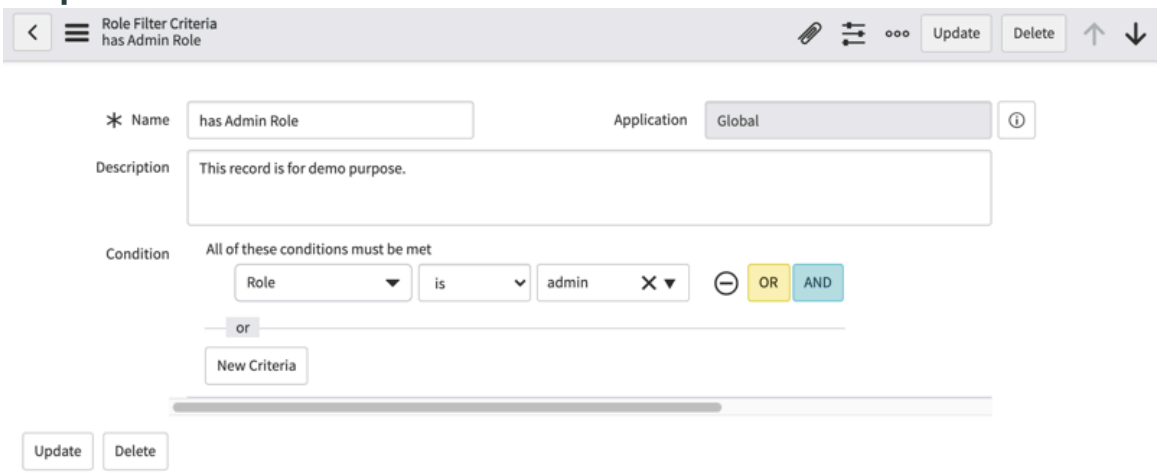
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Rollen-Filterkriterien**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „Rollenfilterkriterien“

Feld	Beschreibung
Name	Name zur Identifizierung der Rolle.
Anwendung	Umfang der Anwendung.
Beschreibung	Kurzbeschreibung der Rolle.

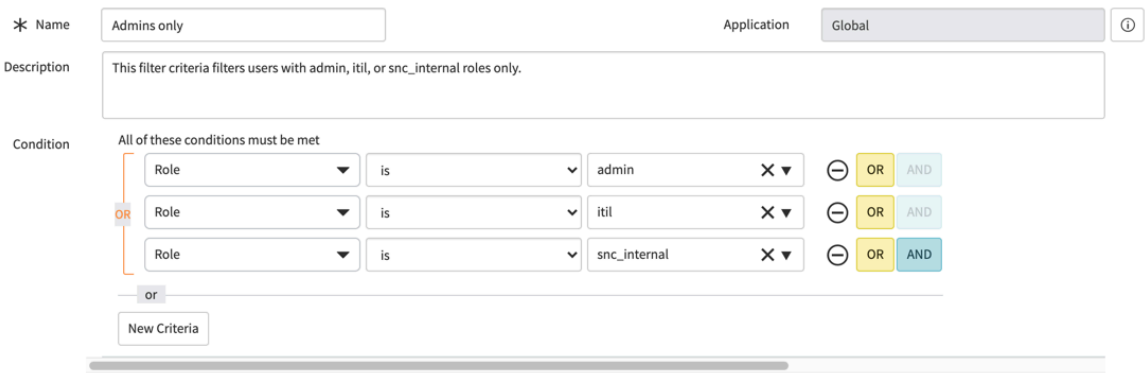
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispieldatensatz für Rollenfilterkriterien



4. Doppelklicken Sie in den **Rollen für Kriterien**auf **Neue Zeile einfügen**.
5. Erstellen Sie mit dem Bedingungsgenerator eine Bedingung für eine bestimmte Rolle.
   Sie können beispielsweise eine Bedingung erstellen, die nur Benutzer mit den Rollen „admin“, „itil“ oder „snc_internal“ zulässt. Weitere Informationen zum Bedingungsgenerator finden Sie unter Bedingungsanweisungen mit dem Bedingungsgenerator erstellen .

Hinweis:
Derzeit wird Dot-Walking in Rollenfilterkriterien nicht unterstützt.



Gruppenfilter

Verwenden Sie Gruppenfilterkriterien, um Benutzer basierend auf der Benutzergruppe zu filtern, der der Benutzer angehört.

Gruppenfilterkriterien erlauben oder verweigern den Benutzerzugriff basierend auf der Benutzergruppe, der der Benutzer angehört.

Erstellen Sie Gruppenfilterkriterien

Gruppenfilterkriterien erlauben oder verweigern den Benutzerzugriff basierend auf der Benutzergruppe, der der Benutzer angehört.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

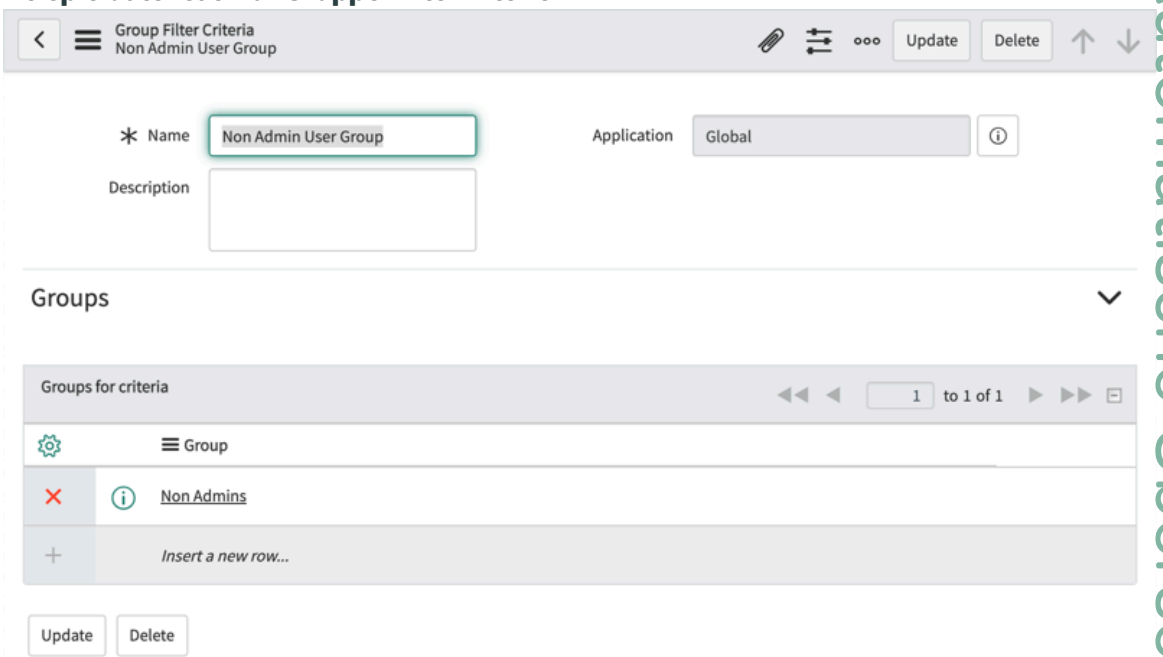
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Gruppenfilterkriterien**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Gruppenfilterkriterien

Feld	Beschreibung
Name	Name zur Identifizierung der Gruppe.
Beschreibung	Kurzbeschreibung der Gruppe.
Anwendung	Umfang der Anwendung.

Beispieldatensatz für Gruppenfilterkriterien



4. Doppelklicken Sie auf der Registerkarte **Gruppen für Kriterien** auf **Neue Zeile einfügen**.
5. Klicken Sie auf das Suchsymbol , suchen Sie nach einer Benutzergruppe und wählen Sie sie aus.
6. Klicken Sie auf das Speichern-Symbol .

Standortfilter

Standortfilterkriterien können als Filtereingabe für Benutzer basierend auf dem Benutzerstandort verwendet werden.

Der Standortfilter ist ein Filterkriterium, das die Administratoren beim Erstellen der Authentifizierungsrichtlinien basierend auf dem physischen Standort des Geräts verwenden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die Standortfilterkriterien sind ein kostenpflichtiges Plugin und erfordern eine Lizenz.
- Die Instanz muss sich auf ADCv2 befinden. Wenn sich die Instanz nicht auf ADCv2 befindet, sind keine Informationen zum Benutzerstandort verfügbar.

Mit den Standortfilterkriterien können Sie Folgendes ausführen:

- Als Richtlinieneingabe für Richtlinienbedingungen fungieren, um die Anforderungen für die Authentifizierung zu überprüfen und zu erfüllen.
- Bieten Sie die Möglichkeit, adaptive Authentifizierungsrichtlinien basierend auf dem **Land**zu erstellen.
- Instanzzugriff auf eine bestimmte Geografie zulassen oder nicht zulassen.
- Verwenden Sie die geostandortbasierte Vor- oder Nachauthentifizierungsrichtlinie für Folgendes:
  - Verhindern Sie den Zugriff aus sanktionierten Ländern außerhalb einer strikten Datenschutzregion nach Ermessen des Unternehmens.
  - Erlauben Sie den Zugriff auf Bereiche nur innerhalb der geltenden Datenschutzregion und im Ermessen des Unternehmens.
  - Konfigurieren Sie die länderbasierte Allow-Liste für die Authentifizierung.

Anwendungsfälle

Im Folgenden sind einige Anwendungsfälle für die Verwendung von Standortfilterkriterien für die adaptive Authentifizierung aufgeführt:

- Blockieren Sie den Zugriff auf die Instanz aus einem Land.
- Erlauben Sie den Zugriff auf die Instanz nur aus einem bestimmten Land.
- Erzwingen Sie die Step-up-Authentifizierung oder MFA, um sich basierend auf dem Land anzumelden.
- Reduzieren oder beschränken Sie die Rollen für den Benutzer basierend auf dem Land.
- Standortfilterkriterien können für MFA, Zero Trust Access (ZTA), Kontext vor und nach der Authentifizierung verwendet werden.

Standortidentifizierung

Die Ortungsservices zum Identifizieren des Standorts des Benutzers werden von einem Drittanbieterdienst bereitgestellt – MaxMind.

Der Standort des Benutzers wird über das VPN aus dem x-forwarded-for-Header identifiziert. Wenn keine vom Service ausgefüllte Kopfzeile vorhanden ist, wird nur die VPN-IP (Standort) als Benutzerstandort angezeigt.

Hinweis:
Wenn nach der Konfiguration des Standortfilters falsche Standorte angezeigt werden, lesen Sie den KB-Artikel zur Fehlerbehebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie den standortbasierten Zugriff

Aktivieren Sie **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access), damit Administratoren adaptive Authentifizierungsrichtlinien basierend auf dem Standort des Benutzers konfigurieren können.

Vorbereitungen

Erforderliche Rolle: admin

- Abhängiges Plugin: Adaptive Authentifizierung
- Plugin-Typ: Kostenpflichtig und erfordert Lizenz.
- Die Instanz muss sich auf ADCv2 befinden. Wenn sich die Instanz nicht auf ADCv2 befindet, sind keine Informationen zum Benutzerstandort verfügbar.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „ **Zero Trust - Location Based Access** “ (com.snc.zero_trust_location_access).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Erstellen Sie Standortfilterkriterien

Verwenden Sie Standortfilterkriterien, um Eingaben für die Benutzerauthentifizierung basierend auf dem Benutzerstandort zu filtern.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Eigenschaft: Aktivieren Sie die Eigenschaft „Adaptive Authentifizierung“.

Hinweis:
Administratoren können die Richtlinie nur basierend auf Standortfiltern erstellen, wenn der Standort für die aktuelle Benutzersitzung verfügbar ist.

Prozedur

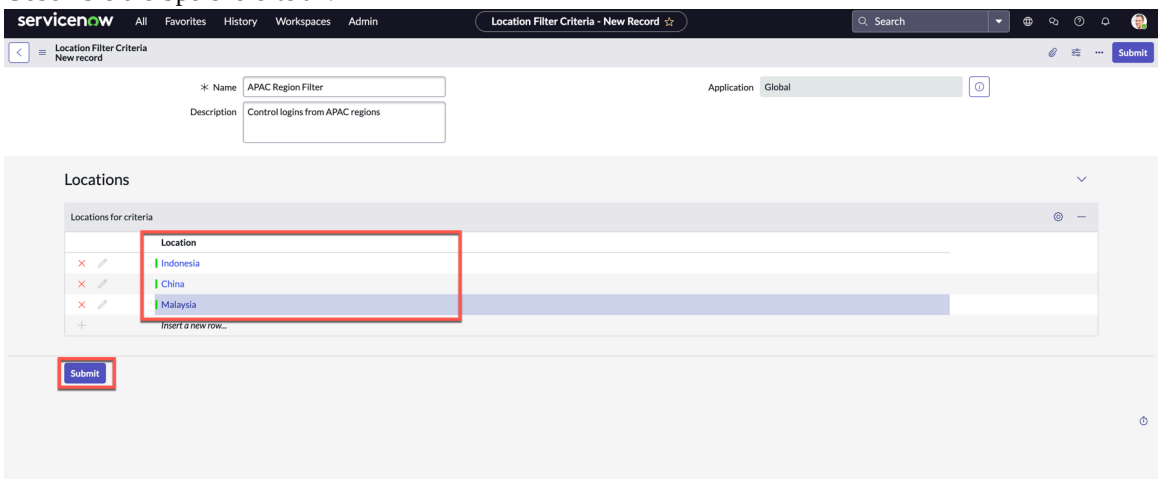
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Standortfilterkriterien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standortfilterkriterien“.

Feld	Beschreibung
Name	Name zur Identifizierung der Kriterien.
Beschreibung	Kurzbeschreibung der Kriterien.
Anwendung	Umfang der Anwendung.

4. Doppelklicken Sie in den Abschnitten „ **Standorte** “ auf der Registerkarte Standorte für Kriterien auf **Neue Zeile einfügen**.
5. Geben Sie die Speicherorte an.



6. Wählen Sie **Absenden**.

Tutorial: Standortfilterkriterien verwenden

Beschreibt Schritte zur Verwendung von Standortfilterkriterien in der Authentifizierungsrichtlinie und zur Beschränkung des Zugriffs auf die Benutzer basierend auf dem Standort.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Eigenschaft: Aktivieren Sie die Eigenschaft „Adaptive Authentifizierung“.

Hinweis:
Administratoren können die Richtlinie nur basierend auf Standortfiltern erstellen, wenn der Standort für die aktuelle Benutzersitzung verfügbar ist.

Das folgende Verfahren beschreibt, wie Sie die Standortfilterkriterien in einer Authentifizierungsrichtlinie erstellen und verwenden.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Standortfilter**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

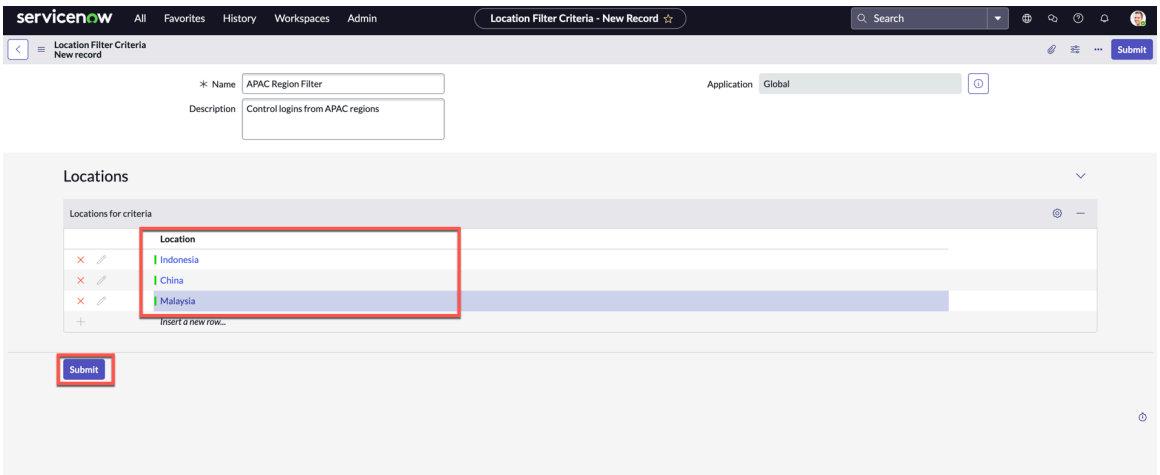
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standortfilterkriterien“.

Feld	Beschreibung
Name	Name zur Identifizierung der Kriterien.
Beschreibung	Kurzbeschreibung der Kriterien.
Anwendung	Umfang der Anwendung.

4. Doppelklicken Sie in den Abschnitten „ **Standorte** “ auf der Registerkarte Standorte für Kriterien auf **Neue Zeile einfügen**.
5. Geben Sie die Speicherorte an.

   Verwenden Sie beispielsweise einige der APAC-Regionen, um die Anmeldungen der Benutzer aus APAC zu steuern.



   Basierend auf den im Beispiel festgelegten Kriterien können Sie Anmeldungen aus Malaysia, Chinaund Malaysia für Ihre Instanz steuern.

6. Wählen Sie **Absenden**.
7. Verwenden Sie die Filterkriterien, die in einem der Authentifizierungskontexte (Pre, Post, MFA) und Sitzungszugriff erstellt wurden.

   Weitere Informationen zur Konfiguration basierend auf Authentifizierungskontext und Sitzungszugriff finden Sie unter:

   - Standortfilter im Kontext vor der Authentifizierung
   - Standortfilter im Kontext nach der Authentifizierung
   - Standortfilter im MFA-Kontext
   - Standortfilter für Sitzungszugriff

   Sie können die Eigenschaft ID – Fehlermeldung, die dem Benutzer angezeigt wird, wenn die Anmeldung aufgrund eines Fehlers bei der Authentifizierungsrichtlinie (glide.auth.policy.ui.error.message) angezeigt wird, verwenden, um die Fehlermeldung anzupassen.

Verwenden Sie den Standortfilter im Kontext vor der Authentifizierung

Verwenden Sie die im Kontext vor der Authentifizierung erstellten Standortfilterkriterien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Erstellen Sie einen Standortfilter mit den Ländern, für die Sie den Zugriff auf die Benutzer basierend auf dem Standort einschränken möchten. Weitere Informationen finden Sie unter Erstellen Sie Standortfilterkriterien.

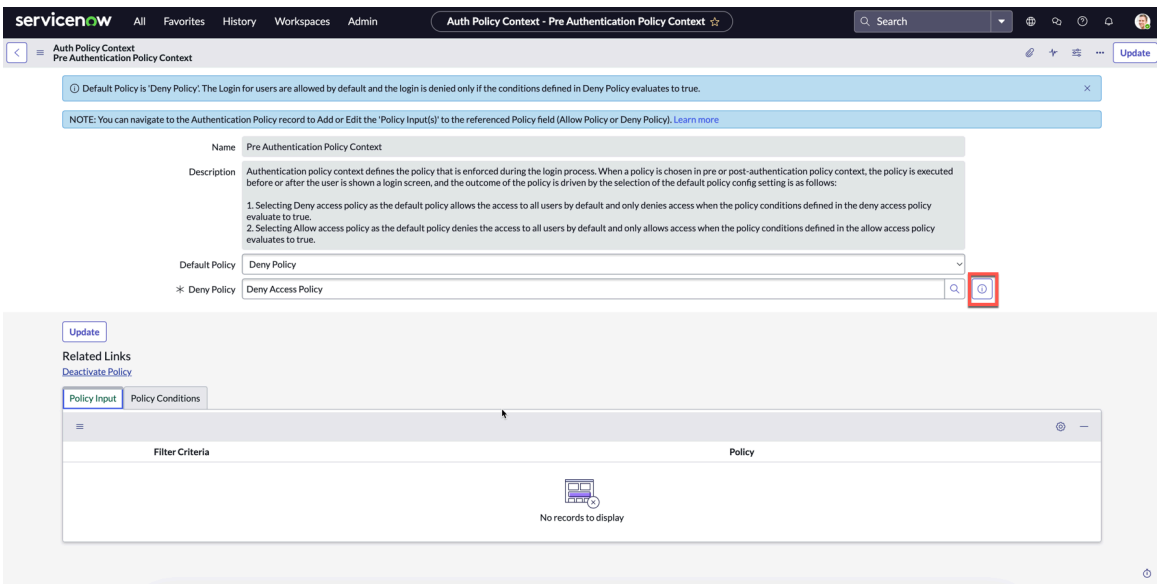
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **Kontext vor der Authentifizierung**.

   Wenn eine Richtlinie im Kontext der Vorauthentifizierungsrichtlinie ausgewählt wird:

   - Wenn Sie die Zugriffsverweigerungsrichtlinie als Standardrichtlinie auswählen, wird standardmäßig allen Benutzern der Zugriff gewährt. Der Zugriff wird nur verweigert, wenn die in der Zugriffsverweigerungsrichtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
   - Wenn Sie die Zugriffsrichtlinie zulassen als Standardrichtlinie auswählen, wird standardmäßig allen Benutzern der Zugriff verweigert und nur dann zugelassen, wenn die in der Zugriffsberechtigungsrichtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

   Das Beispiel zeigt, wie Sie die Anmeldungen an den angegebenen Standorten einschränken können. Sie können Zugriff verweigern und die zugehörige Richtlinie (Zugriff verweigern) als Vorauthentifizierungsrichtlinie auswählen und die Richtlinieneingaben und -bedingungen angeben.

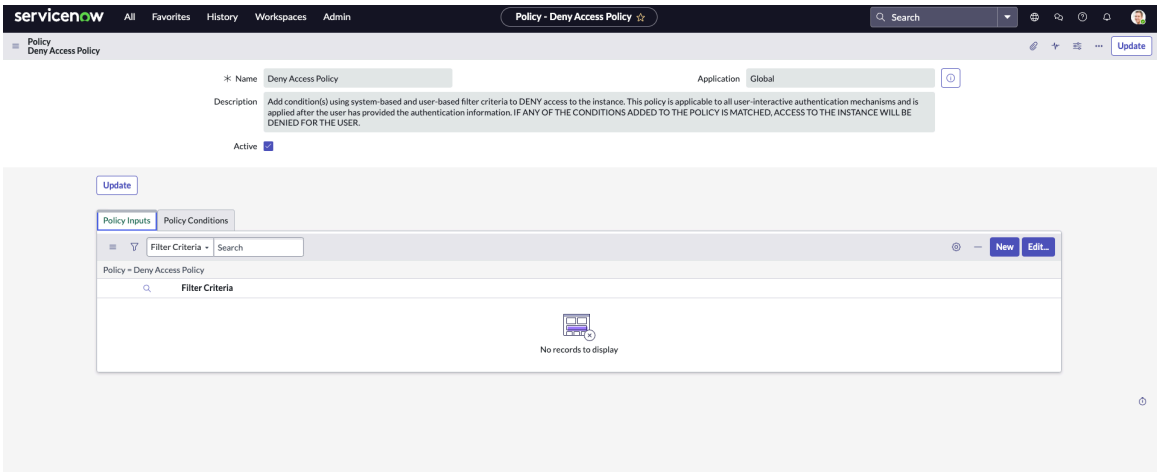


2. Klicken Sie auf das Informationssymbol, um den Datensatz der **Deny-Richtlinie** zu öffnen.

   Hinweis:
   Das in dieser Aufgabe beschriebene Beispiel ist **Deny Policy**(Verweigerungsrichtlinie). Sie können auch die **Allow-Richtlinie** verwenden und die Bedingungen entsprechend festlegen, um die Anmeldungen zu steuern.

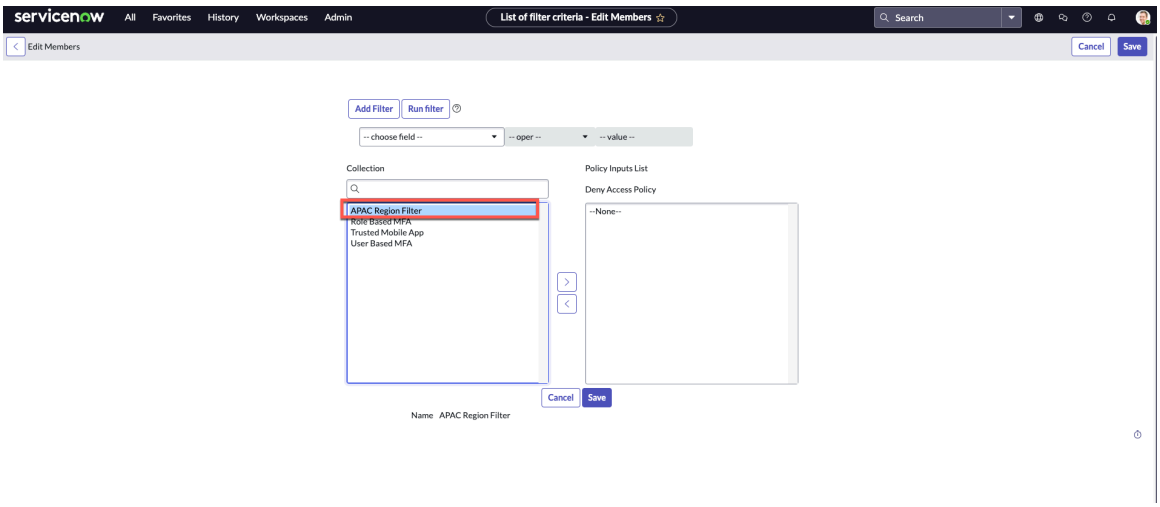
3. Wählen Sie in der Zugriffsverweigerungsrichtlinie im Abschnitt „Richtlinieneingaben“ die Option **Neu**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



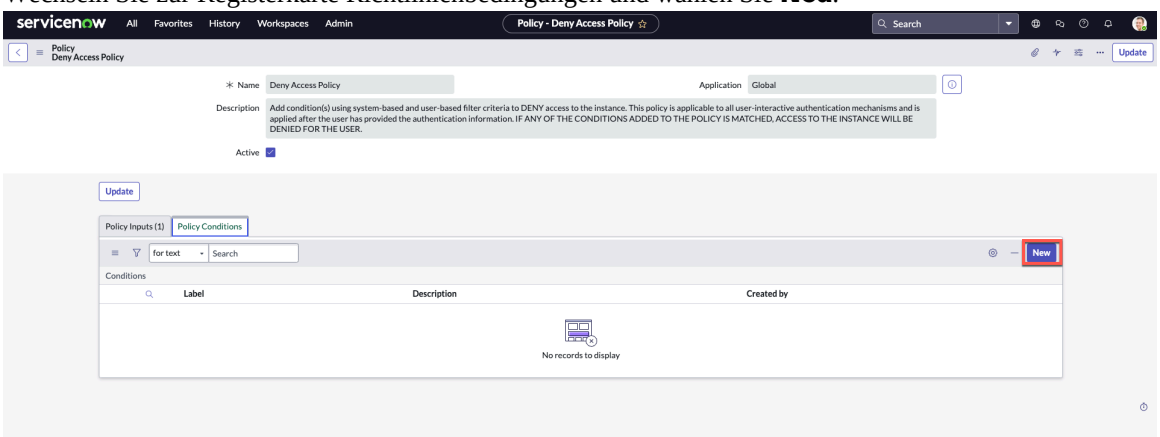
4. Fügen Sie die Eingabe Standortfilter hinzu, und klicken Sie auf **Speichern**.

Beispiel: APAC-Region.



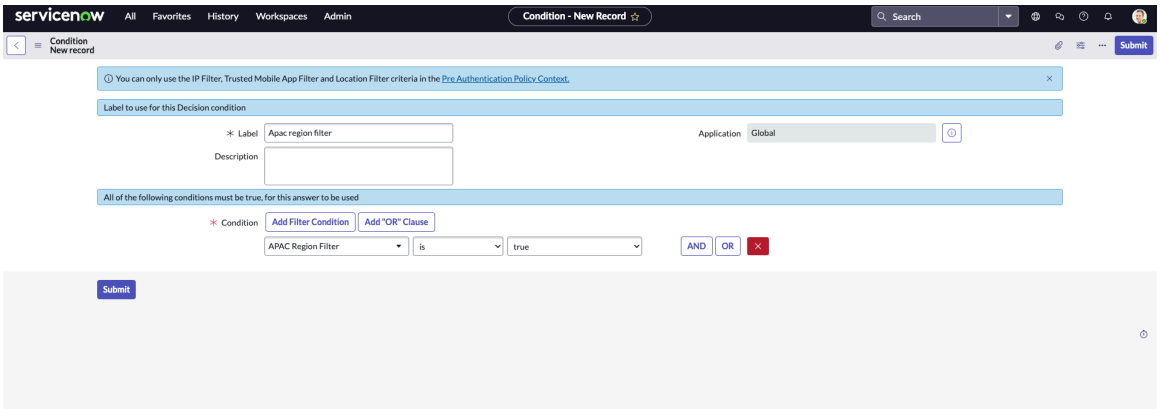
Der Filter wird als **Richtlinieneingaben**hinzugefügt.

5. Wechseln Sie zur Registerkarte Richtlinienbedingungen und wählen Sie **Neu**.



6. Geben Sie auf der Seite „Bedingungen“ die Bezeichnung und die Bedingungen an, und legen Sie sie auf „true“ fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- In diesem Beispiel bedeutet die Auswahl von true als Bedingung, dass sich der Benutzer, der sich aus den konfigurierten Regionen anmeldet, nicht bei der Instanz anmelden kann.
- Wenn die Bedingung auf „falsch“ festgelegt ist, können sich nur Benutzer aus konfigurierten Regionen bei der Instanz anmelden. Die anderen Benutzer können sich nicht bei der Instanz anmelden.

7. Wählen Sie **Absenden**.
   Benutzern, die den Instanzlink auswählen und sich in den konfigurierten Ländern protokollieren, wird eine Fehlermeldung über die Zugriffsverweigerung angezeigt (Fehlermeldung, die von ihren Administratoren auf der Seite mit den Richtlinieneigenschaften konfiguriert wurde).

Verwenden Sie den Kontext für den Standortfilter nach der Authentifizierung

Verwenden Sie die im Kontext nach der Authentifizierung erstellten Standortfilterkriterien.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Erstellen Sie einen Standortfilter mit den Ländern, für die Sie den Zugriff auf die Benutzer basierend auf dem Standort einschränken möchten. Weitere Informationen finden Sie unter Erstellen Sie Standortfilterkriterien.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **Kontext nach der Authentifizierung**.

   Wenn eine Richtlinie im Kontext der Post-Authentifizierungsrichtlinie ausgewählt wird:

   - Wenn Sie die Zugriffsverweigerungsrichtlinie als Standardrichtlinie auswählen, wird standardmäßig allen Benutzern der Zugriff gewährt. Der Zugriff wird nur verweigert, wenn die in der Zugriffsverweigerungsrichtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
   - Wenn Sie die Zugriffsrichtlinie zulassen als Standardrichtlinie auswählen, wird standardmäßig allen Benutzern der Zugriff verweigert und nur dann zugelassen, wenn die in der Zugriffsberechtigungsrichtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

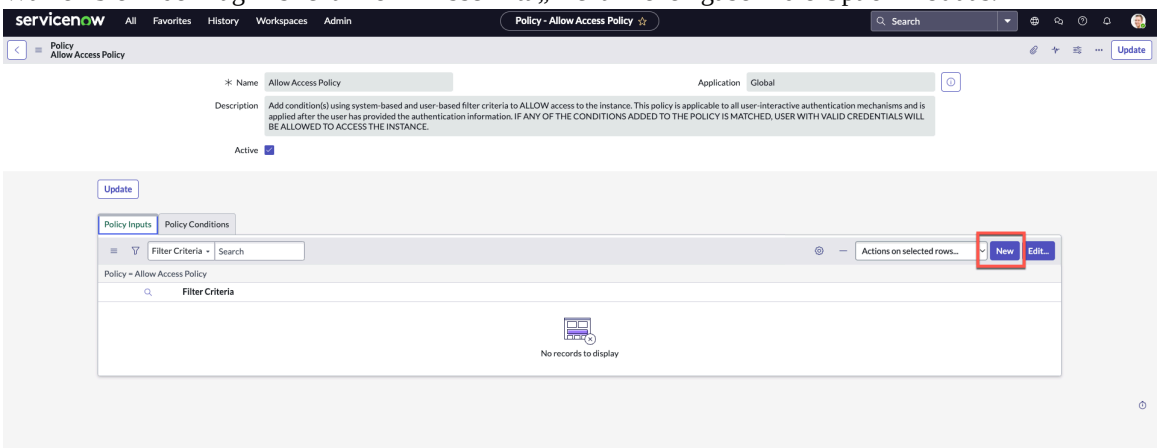
Das Beispiel zeigt, wie Sie einen ITIL- Benutzer mit einer Bedingung konfigurieren können, um nur vom angegebenen Standort (USA) aus auf die Instanz zuzugreifen. Und die ITIL-Benutzer können sich nicht aus anderen Ländern anmelden.

Nachdem Benutzer ihre Anmeldeinformationen auf der Anmeldeseite angegeben haben. Sie können Zugriff zulassen und die zugehörige Richtlinie (Zugriff zulassen) als Richtlinie nach der Authentifizierung auswählen und die Richtlinieneingaben und -bedingungen angeben.

2. Klicken Sie auf das Informationssymbol, um den Datensatz der **Allow-Richtlinie** zu öffnen.

> **Hinweis:**
> Das in dieser Aufgabe beschriebene Beispiel ist **Allow-Richtlinie**. Sie können auch die **Deny-Richtlinie** verwenden und die Bedingungen entsprechend festlegen, um die Anmeldungen zu steuern.

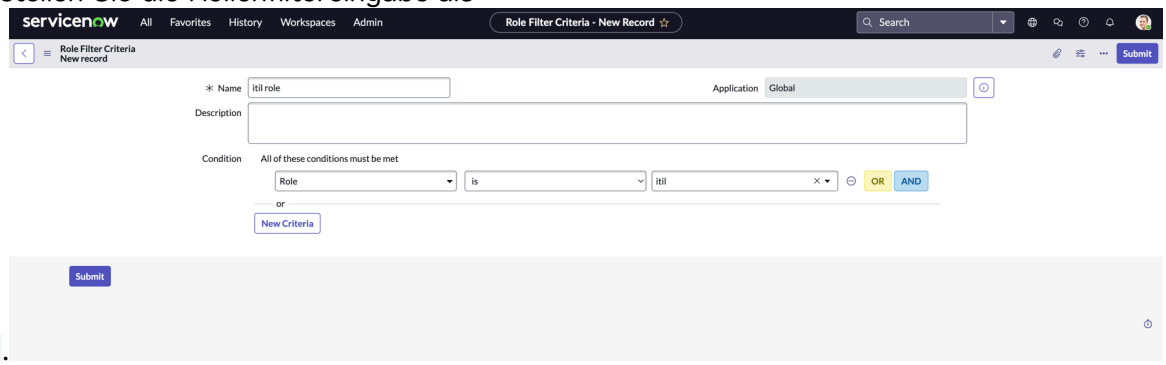
3. Wählen Sie in der Zugriffsrichtlinie im Abschnitt „Richtlinieneingaben“ die Option **Neu**aus.

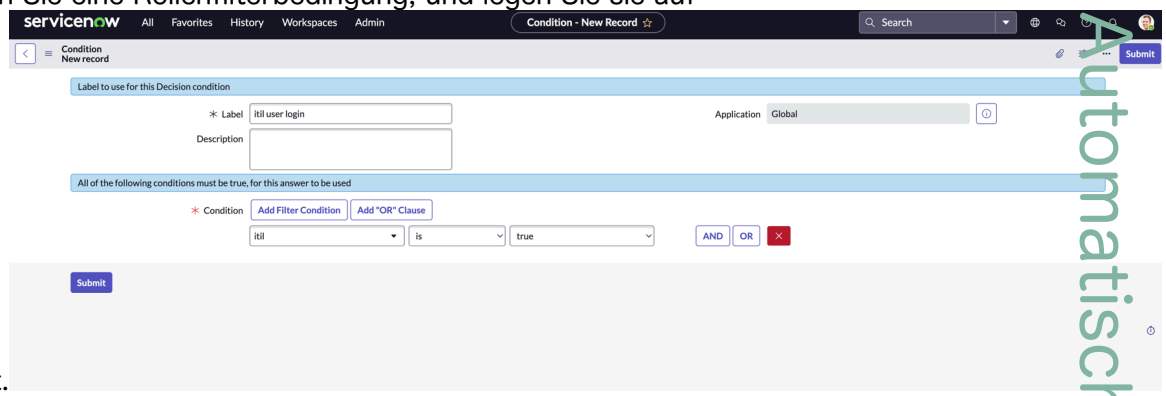


4. Fügen Sie die Rollenfilterkriterien und Standortfilterkriterien hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Hinzufügen von Rollenfilterkriterien:

- Erstellen Sie die Rollenfiltereingabe als 

itil.
- Erstellen Sie eine Rollenfilterbedingung, und legen Sie sie auf 

truefest.

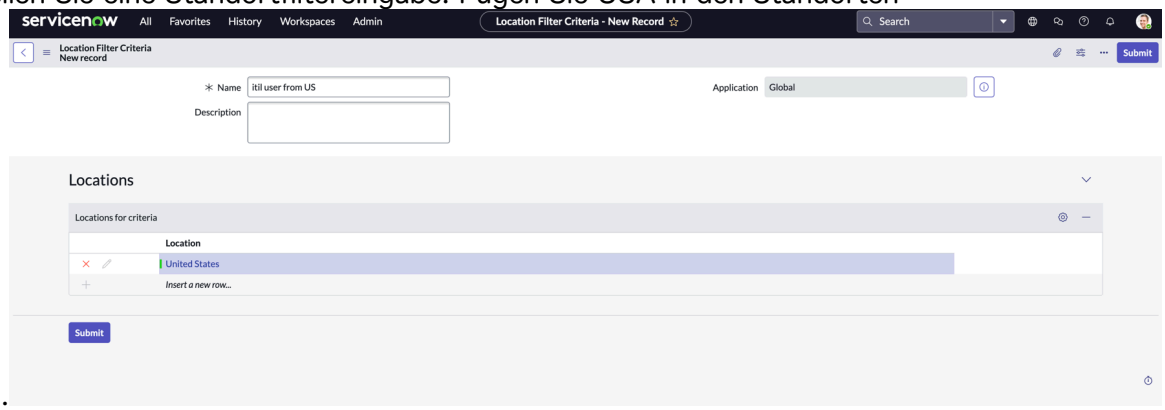
Weitere Informationen zum Erstellen von Rollenfilterkriterien finden Sie unter Erstellen Sie Rollenfilterkriterien.

b. Hinzufügen von Standortfilterkriterien:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie eine Standortfiltereingabe. Fügen Sie USA in den Standorten hinzu.



- Erstellen Sie eine Standortfilterbedingung, und legen Sie sie auf truefest.

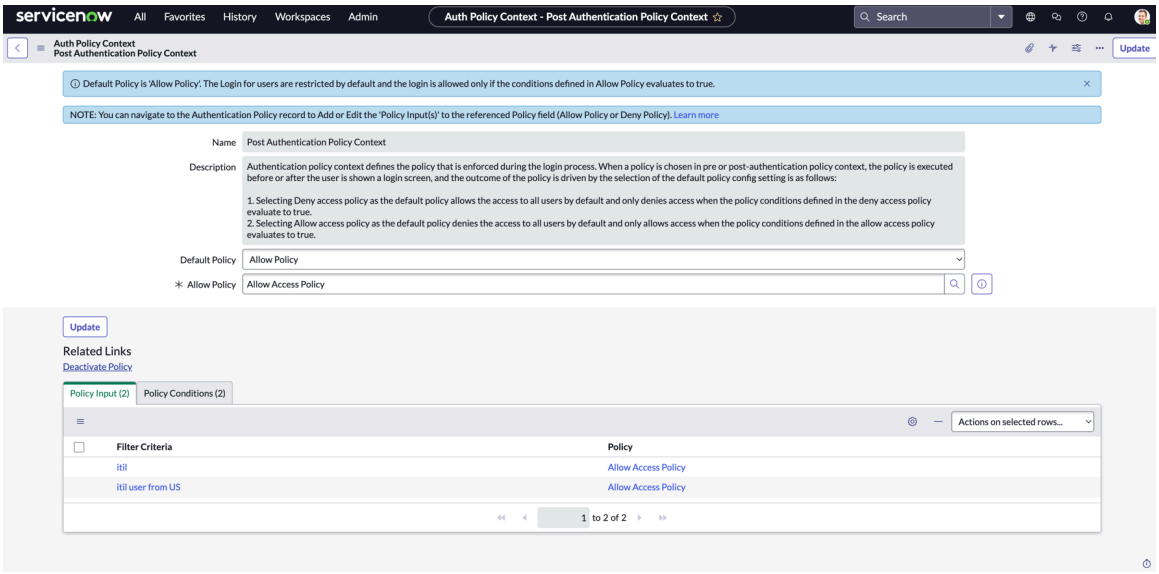
Weitere Informationen zum Erstellen von Rollenfilterkriterien finden Sie unter Erstellen Sie Standortfilterkriterien.

Die Allow-Zugriffsrichtlinie zeigt die Richtlinieneingaben und Bedingungen, die in den vorherigen Schritten erstellt wurden:

- Richtlinieneingaben: itil, itil-Benutzer aus den USA
- Richtlinienbedingungen: ITIL-Benutzeranmeldung, ITIL-Benutzer aus US-Bedingung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- In diesem Beispiel impliziert die Auswahl von true als Bedingung, dass sich die ITIL- Benutzer, die sich aus dem konfigurierten Land (USA) anmelden, bei der Instanz anmelden können.
- Wenn die Bedingung auf „false“ festgelegt ist, können sich die ITIL- Benutzer aus dem konfigurierten Land (USA) nicht bei der Instanz anmelden, und die anderen Benutzer können sich nicht bei der Instanz anmelden.

5. Wählen Sie **Absenden** oder **Aktualisieren** aus, um den Kontext nach der Authentifizierung zu aktualisieren.
   Wenn ITIL-Benutzer den Instanzlink auswählen, ihre Anmeldeinformationen angeben und sich dann außerhalb des konfigurierten Landes (USA) anmelden, wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt (Fehlermeldung, die von ihren Administratoren auf der Seite mit den Richtlinieneigenschaften konfiguriert wurde).

Verwenden Sie den Standortfilter im MFA-Kontext

Verwenden Sie die im MFA-Kontext erstellten Standortfilterkriterien.

Vorbereitungen

Erforderliche Rolle: admin

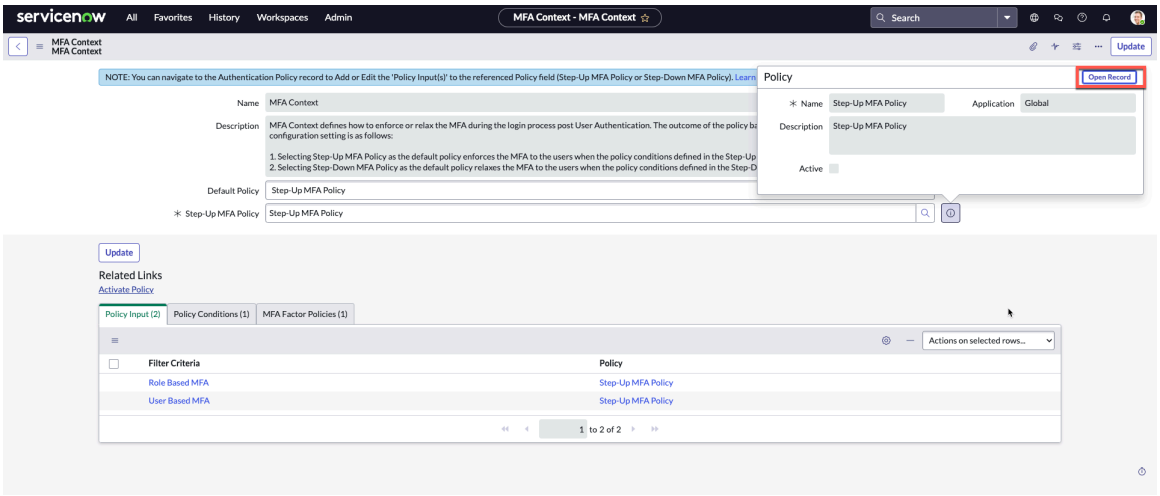
Erforderliches Plugin: **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Das folgende Verfahren beschreibt, wie Sie einen Standortfilter mit den Ländern erstellen, für die Sie MFA als zweiten Faktor für die Authentifizierung der Benutzer basierend auf dem Standort konfigurieren möchten.

Prozedur

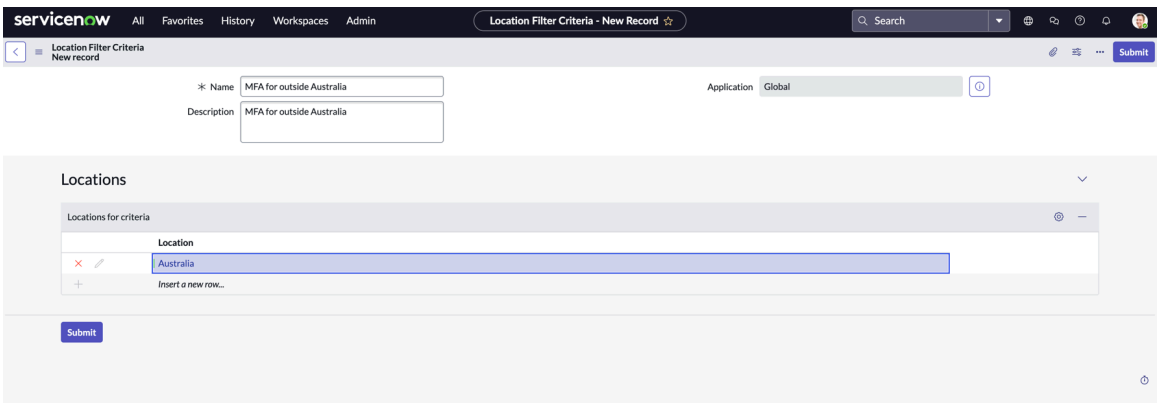
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **MFA-Kontext**.
2. Klicken Sie auf der Seite „ **MFA-Kontext** “ auf das Informationssymbol für **Step-Up-MFA-Richtlinien**, und öffnen Sie den Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

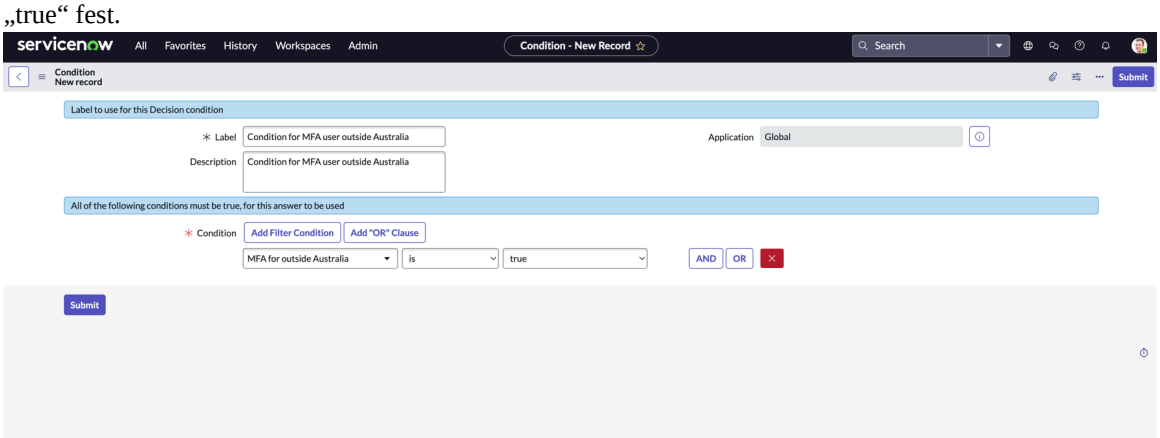


3. Wählen Sie auf der Seite „Step-Up-MFA-Richtlinie“ auf der Registerkarte Richtlinieneingaben die Option **Neu**aus.
4. Fügen Sie die Eingabe Standortfilter hinzu, und **senden**Sie.

   Beispiel: Sie möchten MFA für Benutzer anzeigen, die sich außerhalb von Australien bei der Instanz anmelden.



5. Wählen Sie auf der Seite „Step-Up-MFA-Richtlinie“ die Registerkarte Richtlinienbedingungen und dann **Neu**aus.
6. Geben Sie auf der Seite „Bedingungen“ die Bezeichnung und die Bedingungen an, und legen Sie sie auf „true“ fest.



7. Wählen Sie **Absenden**.
8. Aktivieren Sie auf der Seite „Step-Up-MFA-Richtlinie“ die MFA-Richtlinie, wenn sie **deaktiviert**ist.
9. Wählen Sie **Aktualisieren** aus, um die Konfiguration zu aktualisieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Benutzer außerhalb des konfigurierten Landes (Australien), die den Instanzlink auswählen und ihre Anmeldeinformationen angeben; wird mit dem MFA-Bildschirm angezeigt, um die Anmeldeinformationen des zweiten Faktors für die Anmeldung bei der Instanz bereitzustellen.

Verwenden Sie Standortfilter für Sitzungszugriff

Verwenden Sie die in Sitzungszugriff erstellten Standortfilterkriterien, um Rollen basierend auf dem Standort des Benutzers zu reduzieren.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Das folgende Verfahren beschreibt, wie Sie einen Standortfilter mit den Ländern erstellen, in denen Sie Rollen entfernen oder auf die Benutzer basierend auf dem Standort beschränken möchten.

Prozedur

1. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**.
2. Um eine Konfiguration für Sitzungszugriffsrollen zu erstellen, wählen Sie **Neu**.
3. Füllen Sie im Formular die folgenden Felder aus:

Konfiguration der Sitzungszugriffsrolle

Feld	Beschreibung
Name	Name der Konfiguration
Beschreibung	Kurzbeschreibung der Konfiguration.
Richtlinie	Wählen Sie die Zugriffsrichtlinie aus. Verwenden Sie das Suchsymbol, um die Liste der Richtlinien anzuzeigen. **Hinweis:** Sie müssen die Eingabe und die Bedingungen für den Standortfilter hinzufügen, indem Sie den Richtliniendatensatz öffnen.
Aktion	**Rollen entfernen** oder **auf Rollen beschränken**. ○ **Rollen entfernen**: Wenn sich der konfigurierte Benutzer angemeldet hat, wird die Liste der in der Rollen- oder Gruppenliste angegebenen Rollen für die angemeldete Sitzung entfernt. ○ **Auf Rollen beschränken**: Wenn sich der konfigurierte Benutzer anmeldet, werden ihm nur die ausgewählten Rollen zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Verfügung gestellt, und alle anderen Rollen werden für die angemeldete Sitzung entfernt.
Rollenliste	Wählen Sie die Rolle aus der Rollenliste aus.
Gruppenliste	Wählen Sie die Rolle aus der Gruppenliste aus.

4. Wählen Sie, **Absenden**.

   Die Anmeldung für Benutzer basierend auf den konfigurierten Ländern lautet wie folgt:

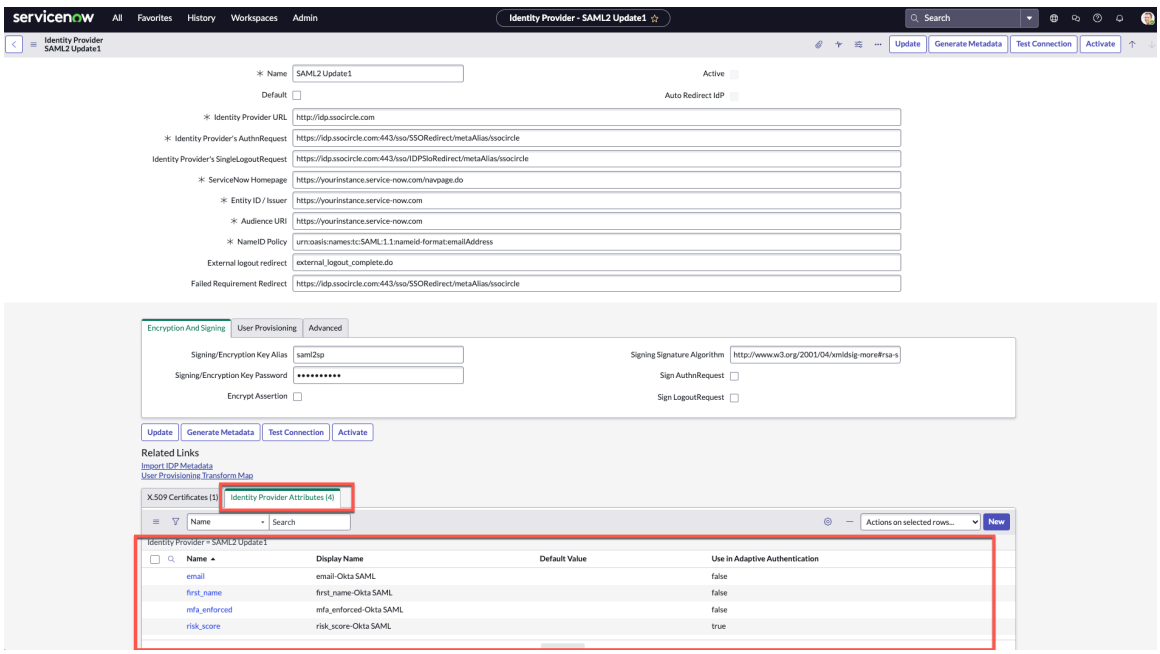
   - Wenn **Rollen entfernen ausgewählt**ist, werden die Benutzer aus den konfigurierten Ländern im Standortfilter mit den für die Sitzung konfigurierten Rollen entfernt.
   - Wenn **Auf Rollen beschränken**, haben die Benutzer aus den konfigurierten Ländern im Standortfilter nur die Rollen, die für die Sitzung konfiguriert sind.

   Weitere Informationen zum Entfernen oder Einschränken von Rollen für eine Sitzung finden Sie unter Verwenden Sie Zero Trust-Zugriff.

Filter für Identitätsanbieterattribute

Verwenden Sie die Attribute des Identitätsanbieters, die von der SAML-Antwort (Security Assertion Markup Language) des Identitätsanbieters (IdP) empfangen werden, als Filterkriterien für die Authentifizierung.

Um alle Attribute von einem IdP über die SAML-Antwort abzurufen, sollten Sie eine Testverbindung mit dem IdP herstellen. Nach einer erfolgreichen Testverbindung werden die Attribute auf einer neuen Registerkarte auf der Konfigurationsseite des Identitätsanbieters hinzugefügt.



Sie können Attribute auch hinzufügen, indem Sie im Abschnitt „Identitätsanbieterattribute“ die Option **Neu** auswählen und diese Attribute für die adaptive Authentifizierung verwenden, indem Sie sie auf `true`setzen.

Die **Attribute des Identitätsanbieters** werden mit den folgenden Details angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standortfilterkriterien“.

Feld	Beschreibung
Name	Attributname, der vom Identitätsanbieter bereitgestellt wird.
Anzeigename	Anzeigename ist der detaillierte Name, der für die Filterkriterien verwendet wird. **Hinweis:** Sie können einen lesbaren Namen als Anzeigenamen angeben. In einigen Fällen ist der vom Identitätsanbieter bereitgestellte Anzeigename lang und nicht lesbar.
Standardwert	Der Standardwert wird für die Auswertung der Filterkriterien verwendet, falls das Attribut in der SAML-Antwort fehlt.
In adaptiver Authentifizierung verwenden	Option zur Verwendung des Attributs in der adaptiven Authentifizierung.

Hinweis:
Bei Attributen, die über Azure IdP ausgefüllt werden, sind Name und Anzeigename aufgrund der Namenslänge des Attributs auf Zeichen beschränkt.

Sie können auch neue Attribute hinzufügen, indem Sie im Abschnitt **Identitätsanbieterattribute** auf **Neu** klicken.

Wenn In adaptiver Authentifizierung verwenden auf „true“ festgelegt ist, wird das ausgewählte Attribut als Filterkriterien in den generischen Filterkriterien hinzugefügt. Beispiel: **risk_score** auf truegesetzt. Auf der Seite „Generische Filterkriterien“ wurde ein neuer Filter erstellt.

Verwenden Sie das Identitätsanbieterattribut als Filterkriterien

Verwenden Sie das IDP-Attribut (Identity Provider) aus der SAML-Antwort (Security Assertion Markup Language) als Filterkriterium für die Authentifizierungsrichtlinie.

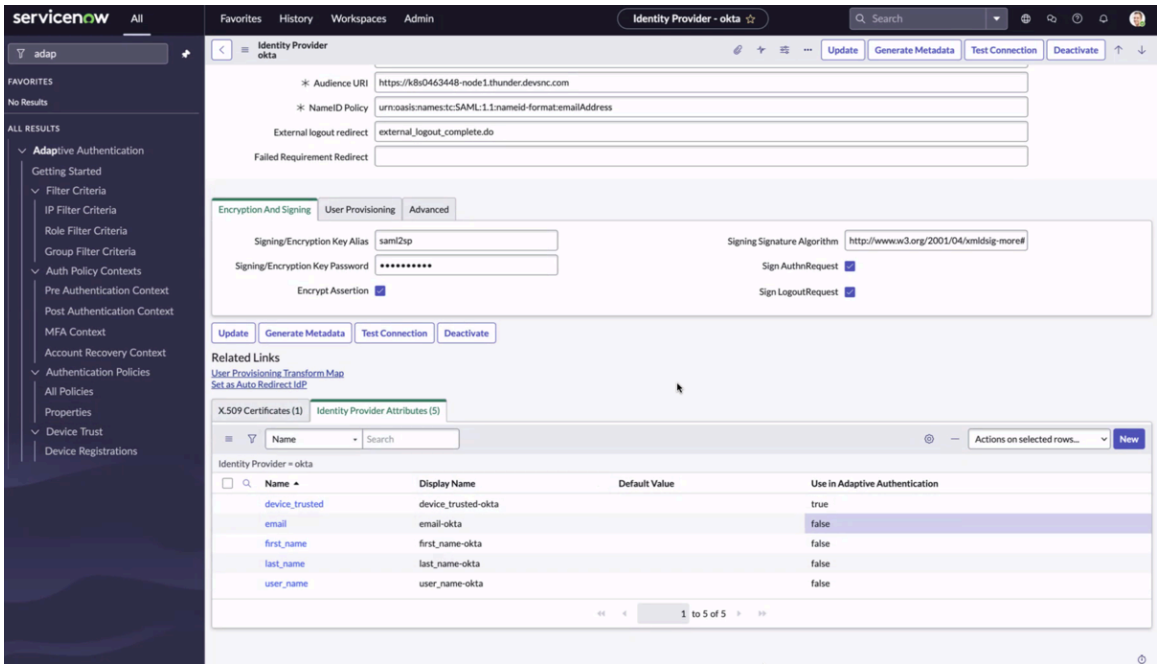
Vorbereitungen
Erforderliche Rolle: admin

Sie können eine Sitzungszugriffsrichtlinie mithilfe des Richtlinienkontexts (Vorauthentifizierung, Nachauthentifizierung, Multifaktor-Authentifizierung) und Filterkriterien (Rolle, Gruppe, IP, Standort) mit Richtlinieneingaben und -bedingungen erstellen.

Das folgende Verfahren zeigt Schritte zum Konfigurieren des IdP-Attributs aus der SAML-Antwort als Richtlinieneingabe zur Steuerung der Authentifizierung im Kontext nach der Authentifizierung, im **Kontext**der **Multifaktor-Authentifizierung (MFA)**und in **Zero Trust – richtlinienbasierter Sitzungszugriff**.

Die Okta-IDP-Attribute werden im folgenden Screenshot angezeigt. Legen Sie die Option In adaptiver Authentifizierung verwenden auf true fest, um sie in den Richtlinien für **Post Authentication Context**, **Multi-Factor Authentication (MFA) Context**und **Zero Trust – Policy-basierte Sitzungszugriffsrichtlinien** zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Richtlinien in der Nachautorisierung, MFA, Zero Trust – Richtlinienbasierter Sitzungszugriff werden ausgeführt, nachdem die Benutzer die Anmeldeinformationen oder die SSO-Antwort eingegeben haben.

Prozedur

1. Verwendung des IdP-Attributs im Kontext der Post-Authentifizierungsrichtlinie.
   Beispiel: Konfiguration, um Anmeldungen über die Okta-IDP-Attribute zu ermöglichen, wenn das Gerät vertrauenswürdig ist

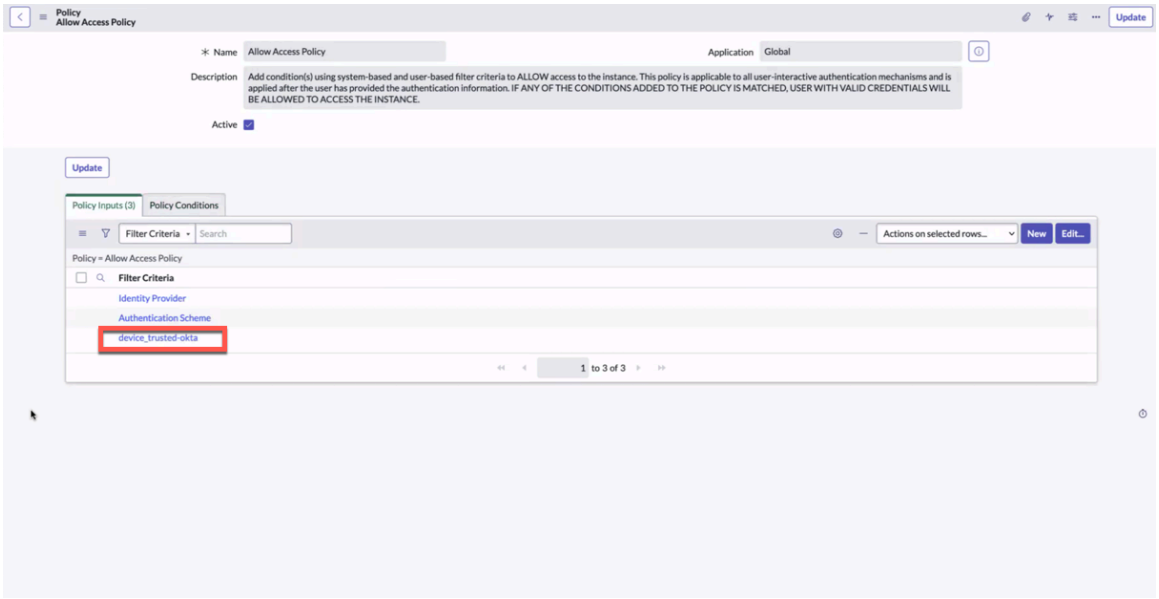
   a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Richtlinienkontext nach der Authentifizierung.**.

   b. Wählen **Sie Allow Policy** (Richtlinie zulassen) aus, und öffnen Sie den Richtliniendatensatz.

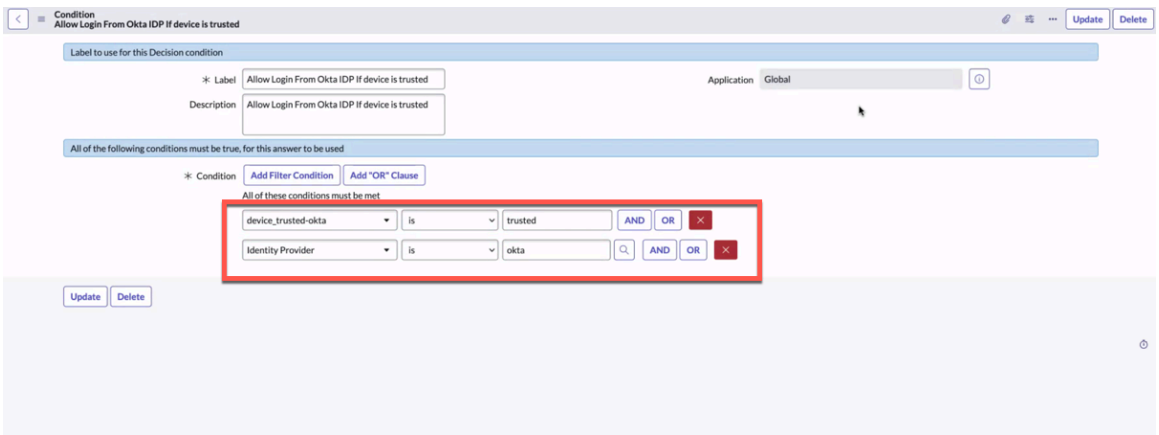
   c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe**: Fügen Sie **device_trusted-okta hinzu**.



- **Richtlinienbedingungen**: **device_trusted-okta** ist vertrauenswürdig und **Identitätsanbieter** ist okta.



Basierend auf dieser Konfiguration wird der Benutzer bei der Instanz authentifiziert, wenn dem Gerät vom Okta (IdP) vertraut wird.

Weitere Informationen zum Erstellen eines Kontexts nach der Authentifizierung mit Richtlinie und Bedingung finden Sie unter Kontext nach der Authentifizierung.

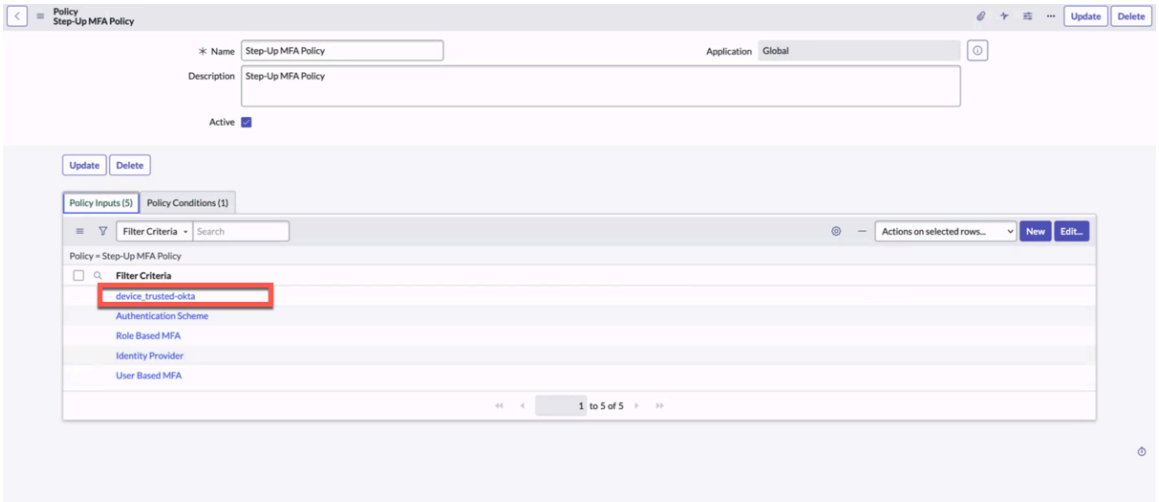
2. Verwendung des IDP-Attributs im MFA-Richtlinienkontext.
Beispiel: Konfigurieren, um MFA über die Okta-IDP-Attribute zu aktivieren, wenn das Gerät nicht vertrauenswürdig ist

a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext der MFA-Authentifizierungsrichtlinie**.

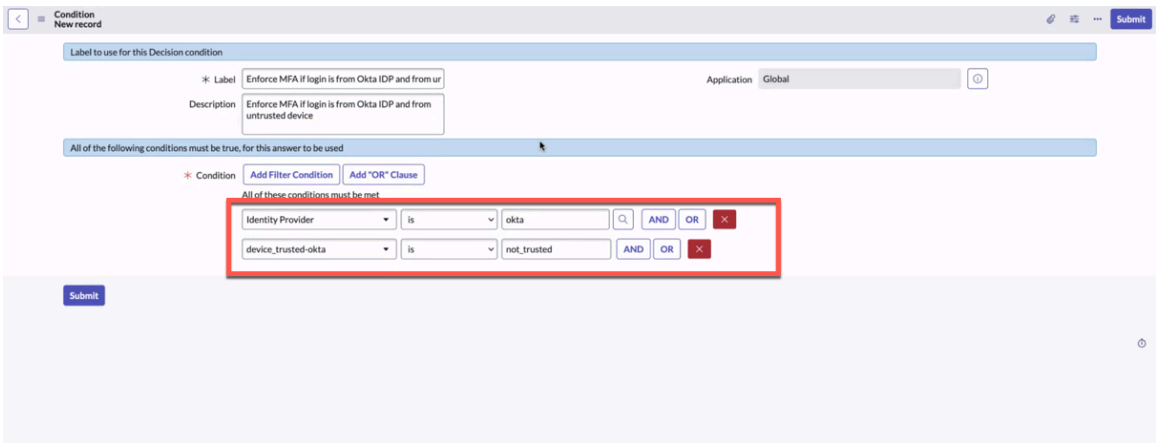
b. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe**: Fügen Sie **device_trusted-okta hinzu**.



- **Richtlinienbedingungen**: **device_trusted-okta** ist `not_trusted` und **Identitätsanbieter** ist `okta`.



Basierend auf dieser Konfiguration hat der Benutzer, wenn dem Gerät vom Okta (IdP) nicht vertraut wird, eine zweite Faktorauthentifizierung angezeigt, um sich bei der Instanz anzumelden.

Weitere Informationen zum Erstellen eines MFA-Kontexts mit Richtlinie und Bedingung finden Sie unter MFA-Kontext (Multifaktor-Authentifizierung)..

3. Verwendung des IDP-Attributs in Zero Trust – Richtlinienbasierter Sitzungszugriff.
   Beispiel: Konfiguration, um die Berechtigung der `ITIL` -Rolle aus Okta-IDP-Attributen zu reduzieren, wenn das Gerät nicht vertrauenswürdig ist.

   a. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**.

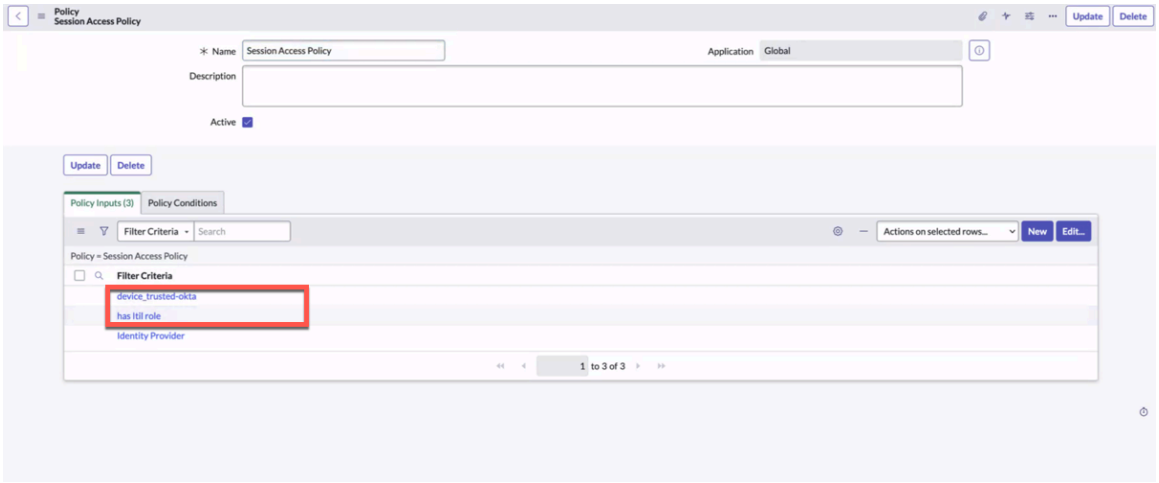
   b. Erstellen Sie eine Rollenkonfiguration für den Sitzungszugriff.

   c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.

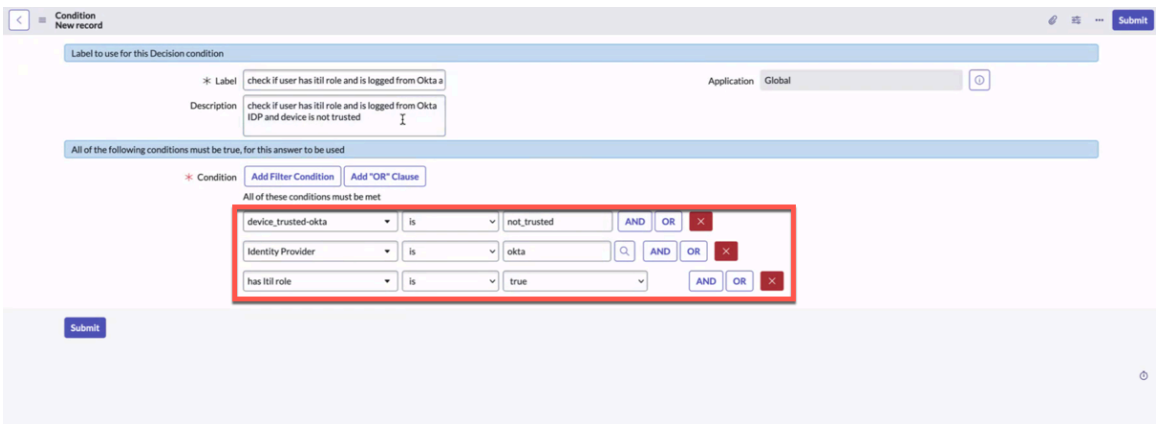
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe**: **„device_trusted-okta** “ hinzufügen und **itil-Rolle übernehmen**.



- **Richtlinienbedingungen**: **„device_trusted-okta“** ist „not_trusted“, „ **Identitätsanbieter** “ ist „ okta“ und **„itil“-Rolle** ist „ true“.



Basierend auf dieser Konfiguration werden die Berechtigungen des Benutzers für die angemeldete Sitzung reduziert, wenn der itil -Benutzer ein Gerät verwendet, dem vom Okta-IdP nicht vertraut wird.

Weitere Informationen zum Erstellen von richtlinienbasiertem Zero Trust-Sitzungszugriff mit Richtlinie und Bedingung finden Sie unter Zero Trust-Zugriff.

Kontexte der Authentifizierungsrichtlinie

Verwenden Sie Authentifizierungsrichtlinienkontexte, um zu bestimmen, wie und wann Ihre Instanz Authentifizierungsrichtlinien durchsetzt.

Authentifizierungskontexte definieren, wie und wann eine Richtlinie während des Anmeldevorgangs erzwungen wird. Weisen Sie eine Richtlinie einem Richtlinienkontext zu, um Eingaben und Bedingungen dafür zu definieren, wie Ihre Instanz die Authentifizierung behandelt.

Kontext vor der Authentifizierung

Richtlinien im Vorautorisierungskontext werden ausgeführt, wenn ein Benutzer zum ersten Mal auf die Instanz zugreift, bevor ihm ein Anmeldebildschirm angezeigt wird. Sie können den Vorautorisierungskontext verwenden, um den Zugriff zuzulassen oder zu verweigern, bevor die Benutzer basierend auf der ausgewählten Richtlinie zur Eingabe von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen aufgefordert werden. Da diese Richtlinien ausgewertet werden, bevor ein Benutzer Informationen eingibt, können diese Richtlinien keine Kriterien wie die Rollen oder Gruppen eines Benutzers berücksichtigen.

Weitere Informationen zu diesem Kontext finden Sie unter Kontext vor der Authentifizierung.

Kontext nach der Authentifizierung

Richtlinien im Kontext nach der Autorisierung werden ausgeführt, nachdem Benutzer ihre Anmeldeinformationen oder SSO-Antwort eingegeben haben. Ihre Instanz erlaubt oder verweigert den Zugriff basierend auf der von Ihnen ausgewählten Richtlinie. Da sich Ihre Benutzer über ihre Anmeldeinformationen identifiziert haben, kann die Richtlinie Benutzerinformationen verwenden, um zu bestimmen, ob Zugriff gewährt wird.

Weitere Informationen zu diesem Kontext finden Sie unter Kontext nach der Authentifizierung.

MFA-Kontext (Multifaktor-Authentifizierung).

Dem MFA-Kontext zugewiesene Richtlinien definieren, ob MFA während des Anmeldevorgangs erzwungen werden soll. Ob Ihre Instanz MFA erzwingt, wird durch die Konfiguration der Richtlinien in diesem Kontext bestimmt. Weitere Informationen zu diesem Kontext finden Sie unter MFA-Kontext (Multifaktor-Authentifizierung)..

Account-Wiederherstellungskontext

Administratoren können die Accountwiederherstellung (ACR) konfigurieren, um Wiederherstellungsaktivitäten durchzuführen, z. B. um SSO-Fehlkonfigurationen oder abgelaufene Zertifikate zu beheben. Um die Accountwiederherstellung zu verwenden, müssen Sie mindestens einen Administratoraccount als Accountwiederherstellungsbenutzer registrieren. Single Sign-on kann in Ihrer Instanz erst aktiviert werden, wenn mindestens ein Konto konfiguriert ist. Weitere Informationen zum Kontext, der festgelegt werden kann, finden Sie unter Account-Wiederherstellungskontext.

Kontext der Sitzungsvalidierung

Der Kontext „Sitzungsvalidierung“ kann mit dem Framework für adaptive Authentifizierungsrichtlinien verwendet werden. Das Framework verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen (Sitzung) auszuwerten und dann den Zugriff basierend auf Richtlinienbedingungen entweder zu verweigern oder zuzulassen. Weitere Informationen finden Sie unter Sitzungsvalidierungskontext.

Standardrichtlinie

Innerhalb des Richtlinienkontexts können Sie im Feld **Standardrichtlinie** eine Standardrichtlinie definieren. Dieser Standard definiert, wie Ihre Instanz auf das Ergebnis Ihrer Richtlinie reagiert. Die verfügbaren Standardrichtlinienoptionen hängen davon ab, welchen Kontext Sie verwenden. Details zu diesen Optionen finden Sie in den Dokumenten, die diese einzelnen Kontexte beschreiben.

Kontext vor der Authentifizierung

Der Kontext der Vorauthentifizierungsrichtlinie definiert, wie und wann eine Richtlinie während des Anmeldevorgangs erzwungen wird. Die in diesem Kontext verwendete Richtlinie wird ausgeführt, bevor die Benutzer einen Anmeldebildschirm sehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontextdatensatz der Vorauthentifizierung

Richtlinien im Vorautorisierungskontext werden ausgeführt, wenn ein Benutzer zum ersten Mal auf die Instanz zugreift, bevor ein Anmeldebildschirm angezeigt wird.

Sie können den Vorauthentifizierungskontext verwenden, um den Zugriff zuzulassen oder zu verweigern, bevor die Benutzer basierend auf der ausgewählten Richtlinie zur Eingabe von Anmeldeinformationen aufgefordert werden. Da diese Richtlinien ausgewertet werden, bevor ein Benutzer Informationen eingibt, können diese Richtlinien keine Kriterien wie die Rollen oder Gruppen eines Benutzers berücksichtigen.

Verwenden Sie die Felder im Kontextdatensatz der Vorauthentifizierungsrichtlinie, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Formular für Vorauthentifizierungskontext

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts beim Auswerten der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Zulassungsrichtlinie** Verweigert standardmäßig allen Benutzern den Zugriff und lässt den Zugriff nur zu, wenn die Bedingungen der im Feld **Allow Policy** (Zulassungsrichtlinie) ausgewählten Richtlinie als „true“ ausgewertet werden. **Verweigerungsrichtlinie** Ermöglicht standardmäßig den Zugriff für alle Benutzer und verweigert den Zugriff nur, wenn die Bedingungen der im Feld **Deny Policy** (Verweigerungsrichtlinie) ausgewählten Richtlinie als „true“ ausgewertet werden.
Zulassungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Allow Policy**(Richtlinie zulassen) festgelegt ist.
Verweigerungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Deny Policy**(Richtlinie verweigern) festgelegt ist.

Hinweis:

Sie können die Kriterien IP-Filter, Trusted Mobile App-Filter und Standortfilter nur im Kontext der Vorauthentifizierungsrichtlinie verwenden.

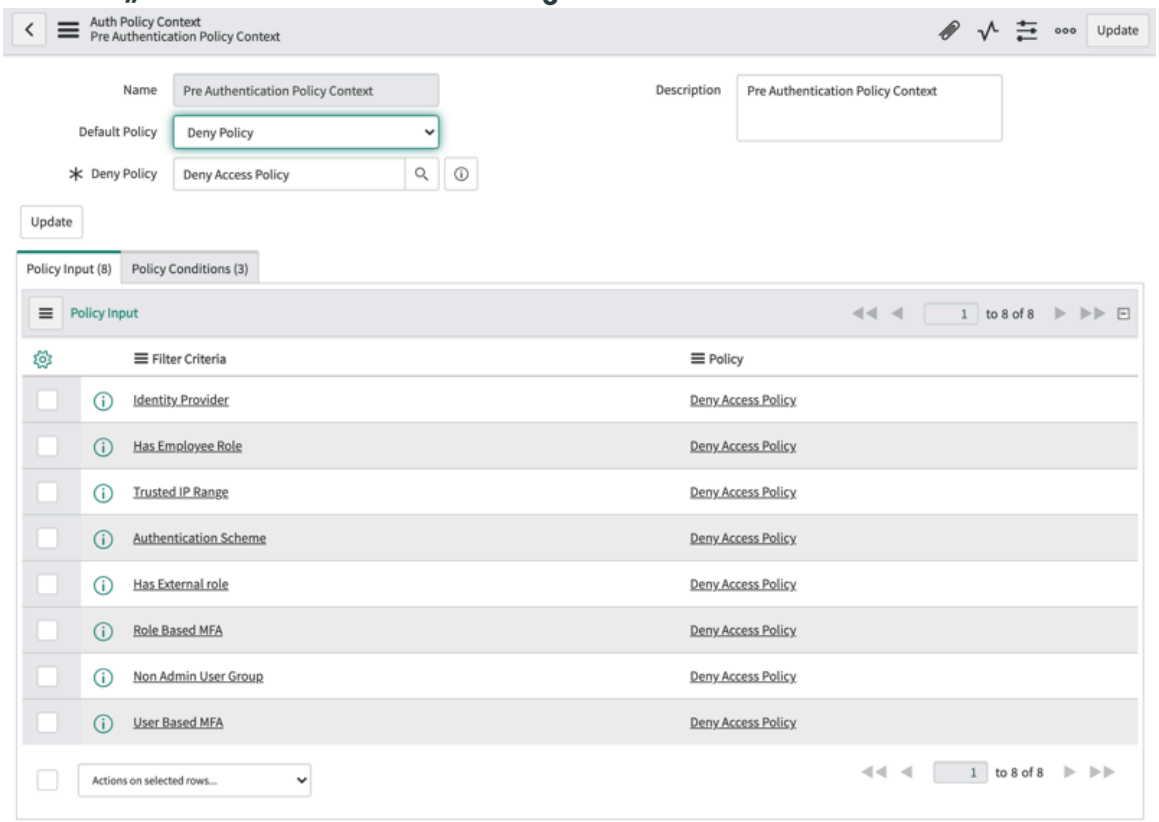
Richtlinieneingaben und -bedingungen

Auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** werden die Eingaben und Bedingungen der Richtlinie angezeigt, die im Feld **Allow-Richtlinie** oder **Deny-Richtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinie zu ändern, navigieren Sie mithilfe des Referenzsymbols (ⓘ) neben dem Feld **Allow-Richtlinie** oder **Deny-Richtlinie zur Richtlinie**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Beispiel zeigt einen Kontextdatensatz einer Vorauthentifizierungsrichtlinie, der so konfiguriert ist, dass er den Zugriff standardmäßig verweigert. Der Kontext verwendet eine Richtlinie mit der Bezeichnung **Zugriffsverweigerungsrichtlinie**. Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingung** angezeigt werden.

Formular „Kontext der Vorauthentifizierungsrichtlinie“.



Kontext nach der Authentifizierung

Der Richtlinienkontext nach der Authentifizierung definiert, wie und wann eine Richtlinie während des Anmeldevorgangs erzwungen wird. Die in diesem Kontext verwendete Richtlinie wird ausgeführt, nachdem die Benutzer einen Anmeldebildschirm sehen.

Kontextdatensatz nach der Authentifizierung

Richtlinien im Kontext nach der Autorisierung werden ausgeführt, nachdem Benutzer ihre Anmeldeinformationen oder SSO-Antwort eingegeben haben. Ihre Instanz erlaubt oder verweigert den Zugriff basierend auf der von Ihnen ausgewählten Richtlinie. Da sich Ihre Benutzer über ihre Anmeldeinformationen identifiziert haben, kann die Richtlinie Benutzerinformationen wie Rolle oder Gruppe verwenden, um zu bestimmen, ob Zugriff gewährt wird.

Verwenden Sie die Felder im Kontextdatensatz der Richtlinie nach der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Formular „Kontext nach Authentifizierung“

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Kontext nach Authentifizierung“ (Fortsetzung)

Feld	Beschreibung
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts beim Auswerten der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Zulassungsrichtlinie** Verweigert standardmäßig allen Benutzern den Zugriff und lässt den Zugriff nur zu, wenn die Bedingungen der im Feld **Allow Policy** (Zulassungsrichtlinie) ausgewählten Richtlinie als „true“ ausgewertet werden. **Verweigerungsrichtlinie** Ermöglicht standardmäßig den Zugriff für alle Benutzer und verweigert den Zugriff nur, wenn die Bedingungen der im Feld **Deny Policy** (Verweigerungsrichtlinie) ausgewählten Richtlinie als „true“ ausgewertet werden.
Zulassungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Allow Policy**(Richtlinie zulassen) festgelegt ist.
Verweigerungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Deny Policy**(Richtlinie verweigern) festgelegt ist.

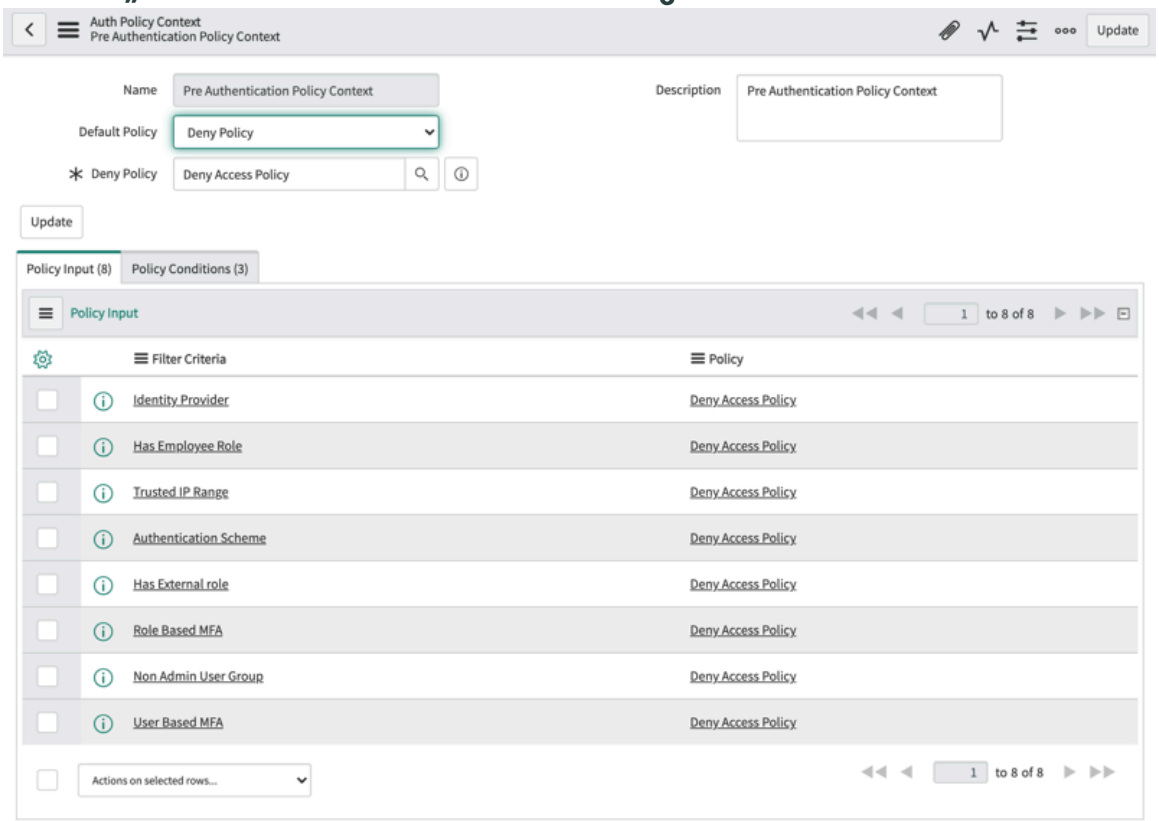
Richtlinieneingaben und -bedingungen

Auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** werden die Eingaben und Bedingungen der Richtlinie angezeigt, die im Feld **Allow-Richtlinie** oder **Deny-Richtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie mithilfe des Referenzsymbols (ⓘ) neben dem Feld **Allow-Richtlinie** oder **Deny-Richtlinie zur Richtlinie**.

Dieses Beispiel zeigt einen Kontextdatensatz einer Richtlinie nach der Authentifizierung, der so konfiguriert ist, dass er den Zugriff standardmäßig verweigert. Der Kontext verwendet eine Richtlinie mit der Bezeichnung **Zugriffsverweigerungsrichtlinie**. Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingung** angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Richtlinienkontext nach Authentifizierung“



MFA-Kontext (Multifaktor-Authentifizierung).

Der MFA-Richtlinienkontext (Multifaktor-Authentifizierung) verwendet eine Richtlinie, um zu definieren, wie und wann MFA während des Anmeldevorgangs erzwungen wird.

MFA-Kontextdatensatz

Der Kontext der MFA-Richtlinie (Multifaktor-Authentifizierung) definiert, ob Benutzer bei der Anmeldung eine zweite Form der Authentifizierung angeben müssen. Dieser Kontext verweigert nicht den Zugriff auf Ihre Instanz, da die Richtlinien nach und vor der Authentifizierung gelten. Die Richtlinie, die Sie in diesem Kontext auswählen, hat Vorrang vor benutzer- oder rollenbasierten Konfigurationen für die Multifaktor-Authentifizierung.

Um auf den MFA-Kontext zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**.

Verwenden Sie die Felder im Kontextdatensatz der Richtlinie nach der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Hinweis:

- Wenn die Standardrichtlinie **Step-Up-MFA-Richtlinie**ist, werden Anwender mit Multifaktor-Authentifizierung angezeigt, wenn die in der **Step-Up-MFA-** Richtlinie konfigurierte Richtlinie als „wahr“ ausgewertet wird. Die Richtlinie hat Vorrang vor der anwender- oder rollenbasierten Konfiguration.
- MFA mit SSO-Anmeldung ist nur verfügbar, wenn die Eigenschaft „ glide.authenticate.mfa.with.multisso.enabled“ auf „wahr“ festgelegt ist.
- Sie können zum Datensatz „Authentifizierungsrichtlinie“ navigieren, um die Richtlinieneingabe(n) im referenzierten Richtlinienfeld (**Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie**) hinzuzufügen oder zu bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA-Kontextformular

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts beim Auswerten der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Step-Up-MFA-Richtlinie** Erzwingt MFA für Benutzer, wenn die im Feld **Step-Up-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden. **Step-Down-MFA-Richtlinie** Erzwingt MFA standardmäßig. MFA wird nur dann nicht erzwungen, wenn die im Feld **Step-Down-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
Step-Up-MFA-Richtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Step-Up-MFA-Richtlinie**festgelegt ist.
Step-Down-MFA-Richtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Step-Down-MFA-Richtlinie**festgelegt ist.

Richtlinieneingaben und -bedingungen

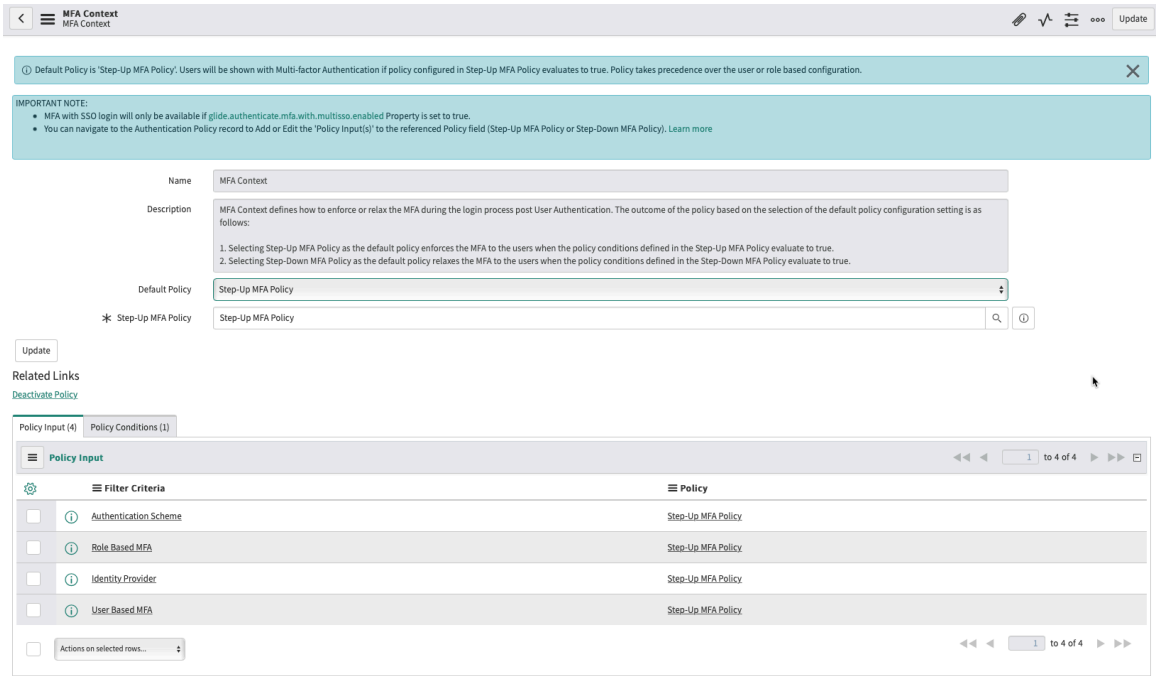
Auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** werden die Eingaben und Bedingungen der Richtlinie angezeigt, die im Feld **Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie mithilfe des Referenzsymbols (ⓘ) neben dem Feld **Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie zur Richtlinie**.

Hinweis:
Richtlinienbedingungen können hier erstellt werden. Es wird jedoch empfohlen, neue Richtlinienbedingungen über die Richtlinienseite hinzuzufügen.

Dieses Beispiel zeigt einen MFA-Kontextdatensatz, der mit einer Step-up-MFA-Richtlinie konfiguriert wurde. Diese Standardrichtlinie bedeutet, dass MFA nur erzwungen wird, wenn die in der Richtlinie definierten Bedingungen als „wahr“ ausgewertet werden. Der Kontext verwendet eine Richtlinie mit der Bezeichnung **Step-Up-MFA-Richtlinie**. Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingung** angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MFA-Richtlinienkontext“



Account-Wiederherstellungskontext

Der Accountwiederherstellungskontext verwendet eine Richtlinie, um zu definieren, wie und wann die Accountwiederherstellung eingerichtet werden kann.

Administratoren können diesen Kontext und die zugehörige Richtlinie anzeigen und ändern, indem sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Kontext der Accountwiederherstellung**.

Hinweis:
Standardmäßig lautet die Richtlinie **Allow-Richtlinie**. Die Anmeldung für -Benutzer ist standardmäßig eingeschränkt, und die Anmeldung ist nur zulässig, wenn die in der Zulassungsrichtlinie definierten Bedingungen als „wahr **"** ausgewertet werden.

Verwenden Sie die Felder im Kontextdatensatz der Kontowiederherstellung, um zu definieren, wie Ihre Instanz die Richtlinie verwendet.

Formular „Account-Wiederherstellungskontext“

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts beim Auswerten der Richtlinie. Wählen Sie unter den folgenden Optionen aus: • Zulassungsrichtlinie • Verweigerungsrichtlinie
Zulassungsrichtlinie	Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Allow Policy**(Richtlinie zulassen) festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

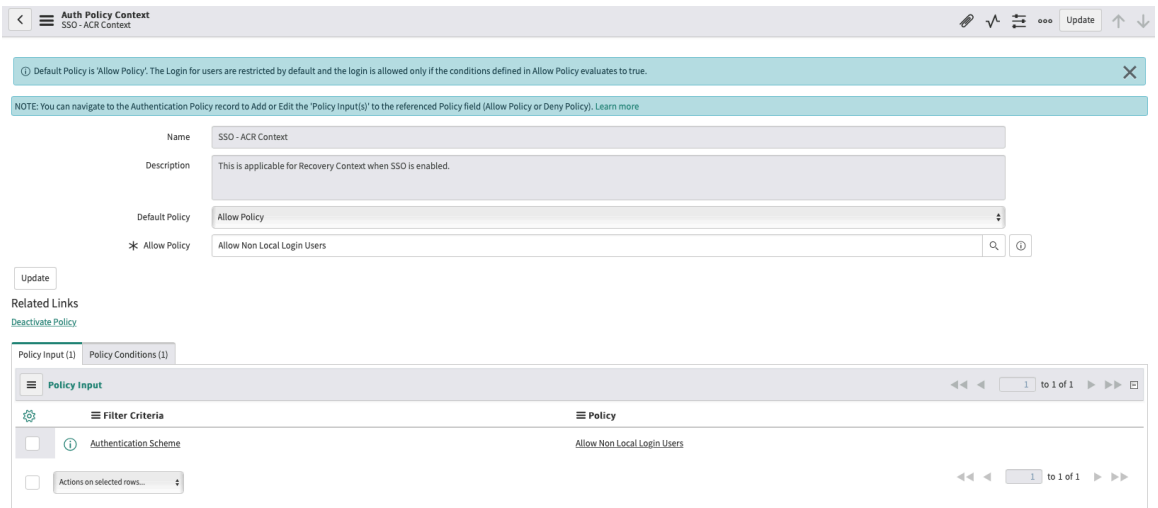
Formular „Account-Wiederherstellungskontext“ (Fortsetzung)

Feld	Beschreibung
Verweigerungsrichtlinie	Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Deny Policy**(Richtlinie verweigern) festgelegt ist.

Richtlinieneingaben und -bedingungen

Auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** werden die Eingaben und Bedingungen der Richtlinie angezeigt, die im Feld **Allow-Richtlinie** oder **Deny-Richtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie mithilfe des Symbols „ **Vorschau auf diesen Datensatz** anzeigen“ neben dem Feld **„Zulassungsrichtlinie“** oder **„Verweigerungsrichtlinie“ zur Richtlinie**.

Hinweis:
Richtlinienbedingungen können hier erstellt werden. Es wird jedoch empfohlen, neue Richtlinienbedingungen über die Richtlinienseite hinzuzufügen.



Sitzungsvalidierungskontext

Verwenden Sie den Sitzungsvalidierungskontext als zusätzliche Schutzebene gegen Sitzungs- oder Cookie-Hijacking.

Sie können den Sitzungsvalidierungskontext mit dem Richtlinien-Framework Adaptive Authentifizierung verwenden. Das Framework verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten, und verweigert oder erlaubt dann den Zugriff basierend auf Richtlinieneingaben und -bedingungen.

Die Richtlinie „Sitzungsvalidierungskontext“ kann in Verbindung mit der Richtlinie nach der Authentifizierung verwendet werden, in der ein Administrator während der angemeldeten Sitzung IP-Beschränkungen für bestimmte oder alle Benutzer erzwingen kann.

Die Funktion „Sitzungsvalidierungskontext“ wertet die IP-Adressen basierend auf den von Ihnen festgelegten Bedingungen aus und ermöglicht den Zugriff auf die Instanz innerhalb einer Sitzung. Die Ergebnisse des Sitzungsvalidierungskontexts lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verweigerungsrichtlinie: Wenn Sie die Zugriffsverweigerungsrichtlinie als Standardrichtlinie auswählen, können Benutzer die Sitzung standardmäßig fortsetzen. Die Sitzung wird nur beendet, wenn eine der in der Zugriffsverweigerungsrichtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet wird.
- Allow-Richtlinie: Wenn Sie die Zugriffsrichtlinie als Standardrichtlinie auswählen, wird die Benutzersitzung sofort beendet, es sei denn, eine der in der Allow-Zugriffsrichtlinie definierten Richtlinienbedingungen wird als „wahr“ ausgewertet.

Hinweis:

- Der Sitzungsvalidierungskontext für eine Authentifizierungsrichtlinie ist standardmäßig auf **Allow-Richtlinie** festgelegt.
- Der Sitzungsvalidierungskontext wird über die Allow-Richtlinie implementiert. Es wird nicht empfohlen, den Kontext so festzulegen, dass die Richtlinie verweigert wird.

Der Sitzungsvalidierungskontext funktioniert basierend auf dem folgenden Mechanismus:

- Erfasst die IP-Adresse des Benutzers bei Erstellung der Sitzung aus Benutzeranforderung und speichert sie in der Sitzung und Datenbank.
- Lehnt eine Anforderung ab, wenn sich ihre IP-Adresse von der in der Sitzung unterscheidet oder außerhalb der vom Kunden definierten gültigen IP-Bereiche liegt, die Sie definiert haben.

Hinweis:

Der Sitzungsvalidierungskontext lautet:

- Nur für authentifizierte Benutzer verfügbar.
- Gilt nicht für Gastbenutzersitzungen oder native Mobile-Apps.
- Optional und basierend auf der Anforderung, dass sie konfiguriert werden kann.
- Wird nur für Post-Login-Anforderungen ausgeführt.

Vorteile der Sitzungsvalidierung

Der Sitzungsvalidierungskontext bietet die folgenden Vorteile:

- Schränkt den Zugriff auf ServiceNow® ein, wenn Hijacking-Anwender Sitzungscookies eines Benutzers von einem Gerät auf ein anderes kopieren, um die Identität der Sitzung anzunehmen.
- Schränkt den Sitzungszugriff des Benutzers ein, wenn er ein unsicheres Netzwerk verwendet.
- Konfiguriert die verschiedenen Regeln und IP-Bereiche nach Benutzergruppe oder Rolle für Benutzeranmeldungen.

Kontextdatensatz für Sitzungsvalidierung

Richtlinien im Sitzungsvalidierungskontext führen Post-Login-Anforderungen aus.

Verwenden Sie die Felder im Kontextdatensatz der Sitzungsvalidierungsrichtlinie, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontextformular für Sitzungsvalidierung

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts.
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts beim Auswerten der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Zulassungsrichtlinie** Verweigert standardmäßig allen Benutzern den Zugriff und lässt den Zugriff nur zu, wenn die Bedingungen im **Feld** Zulassungsrichtlinie als „wahr“ ausgewertet werden. **Verweigerungsrichtlinie** Ermöglicht standardmäßig den Zugriff für alle Benutzer und verweigert den Zugriff nur, wenn die Bedingungen im Feld **Deny Policy** (Verweigerungsrichtlinie) als „true“ ausgewertet werden.
Zulassungsrichtlinie	Die für diesen Kontext verwendete Richtlinie. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Allow Policy**(Richtlinie zulassen) festgelegt ist.
Verweigerungsrichtlinie	Die für diesen Kontext verwendete Richtlinie. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Deny Policy**(Richtlinie verweigern) festgelegt ist.

Sie können die **Sitzungsvalidierungsrichtlinie basierend auf der Richtlinieneingabe und den Richtlinienbedingungen** als Allow-Richtlinie oder Deny-Richtlinie auswählen.

Hinweis:

Sie können nur die Filterkriterien IP, Rolle und Gruppe für die Richtlinie „Sitzungsvalidierung“ verwenden.

Richtlinieneingaben und -bedingungen

Auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** werden die Eingaben und Bedingungen der Richtlinie angezeigt, die im Feld **Allow-Richtlinie** oder **Deny-Richtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz. Sie können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinie zu ändern, navigieren Sie mithilfe des Referenzsymbols (ⓘ) neben dem Feld **Allow-Richtlinie** oder **Deny-Richtlinie zur Richtlinie**.

Aktivieren Sie den Sitzungsvalidierungskontext

Verwenden Sie den Sitzungsvalidierungskontext, um den Zugriff auf ServiceNow® einzuschränken, wenn Hijacking-Anwender Sitzungscookies eines Benutzers von einem Gerät auf ein anderes kopieren, um die Identität der Sitzung anzunehmen, oder den Sitzungszugriff des Benutzers einschränken, wenn er ein unsicheres Netzwerk verwendet.

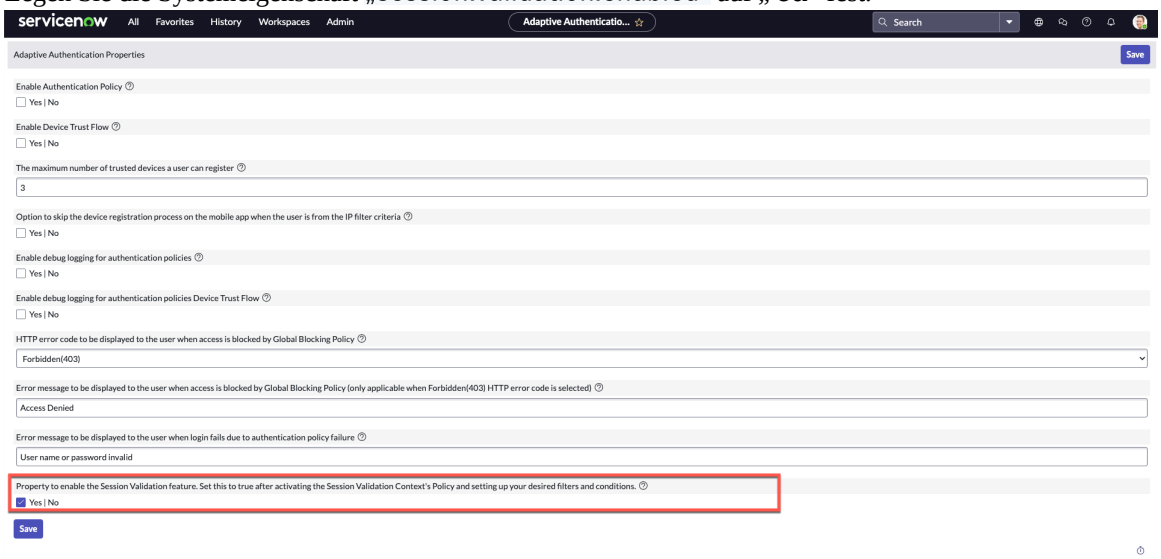
Vorbereitungen
Erforderliche Rolle: admin

Um die Sitzungsvalidierung zu verwenden, müssen Sie die folgenden Schritte ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**.
2. Wählen Sie auf der Seite Richtlinien (sys_authentication_policy_list.do) die **Sitzungsvalidierungsrichtlinie**aus.
3. Geben Sie die **Richtlinieneingaben** und **Richtlinienbedingungen an**.
4. Legen Sie die Bedingungen für die hinzugefügten Filter auf **true** oder **false** fest.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Richtlinie zu aktivieren, nachdem die Sitzungsvalidierungsrichtlinie mit Richtlinieneingaben und -bedingungen eingerichtet wurde.
6. Aktivieren Sie das Kontrollkästchen **AuthnRequest erzwingen** für den Standardidentitätsanbieter in der Tabelle „sso_properties“, wenn für die Instanz SSO konfiguriert ist.
7. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**.
8. Legen Sie die Systemeigenschaft „session.validation.enabled“ auf „ **Ja**“ fest.



Ergebnisse

Die Funktion „Sitzungsvalidierung“ ist aktiviert. Sie können die Richtlinieneingaben und -bedingungen für die Richtlinie konfigurieren, um die Funktion zu verwenden. Weitere Informationen finden Sie unter Tutorial: Sitzungsvalidierung konfigurieren.

Tutorial: Sitzungsvalidierung konfigurieren

Konfigurieren Sie die Sitzungsvalidierung innerhalb des Frameworks der adaptiven Authentifizierung, um eine zusätzliche Schutzebene für Sitzungs- oder Cookie-Hijacking bereitzustellen.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Adaptive Authentication** (com.snc.adaptive_authentication)

Um die Sitzungsvalidierung zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

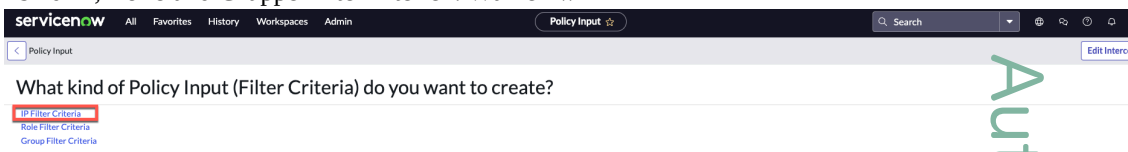
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

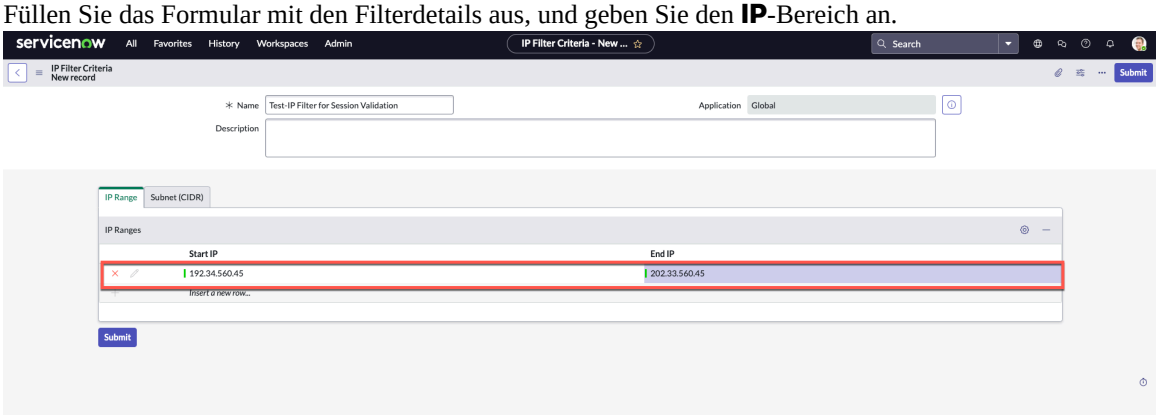
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**.
2. Wählen Sie auf der Seite Richtlinien (`sys_authentication_policy_list.do`) die **Sitzungsvalidierungsrichtlinie**aus.
3. Wählen Sie **Richtlinieneingaben aus**.

   a. Wählen Sie **Neu** oder **Bearbeiten**.

   b. Wählen Sie die Art der Richtlinieneingabe (Filterkriterien) aus, die Sie erstellen möchten. Verfügbare Optionen sind IP, Rolle und Gruppenfilterkriterien. Wählen wir **IP-Filterkriterien**aus.



   c. Füllen Sie das Formular mit den Filterdetails aus, und geben Sie den **IP**-Bereich an.



   Weitere Informationen zum Erstellen eines IP-Filters finden Sie unter Erstellen Sie IP-Filterkriterien.

   d. Wählen Sie **Absenden**.

4. Wählen Sie **Richtlinienbedingungen** auf der Seite „Sitzungsvalidierungsrichtlinie“ aus.

   a. Wählen Sie **Neu**.

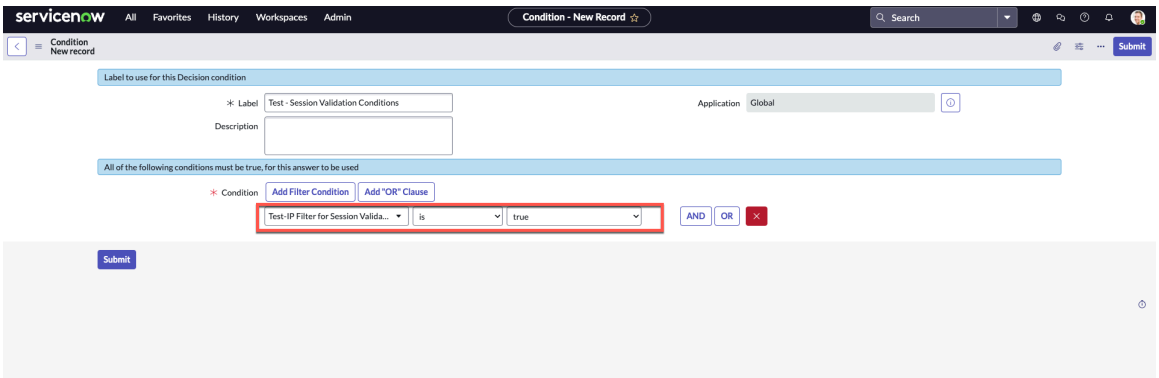
   b. Füllen Sie das Formular aus, und legen Sie die Bedingung für die Richtlinieneingabe fest.

Automatische Übersetzung

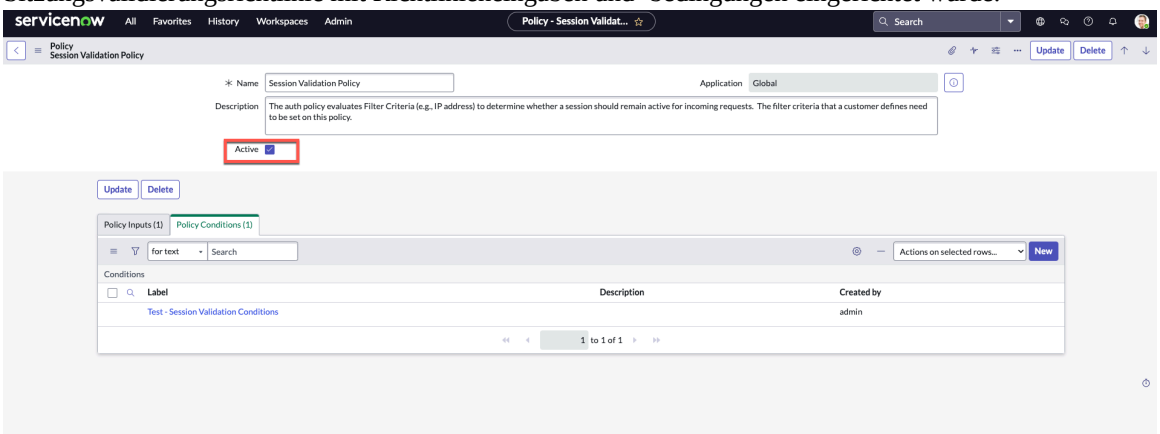
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

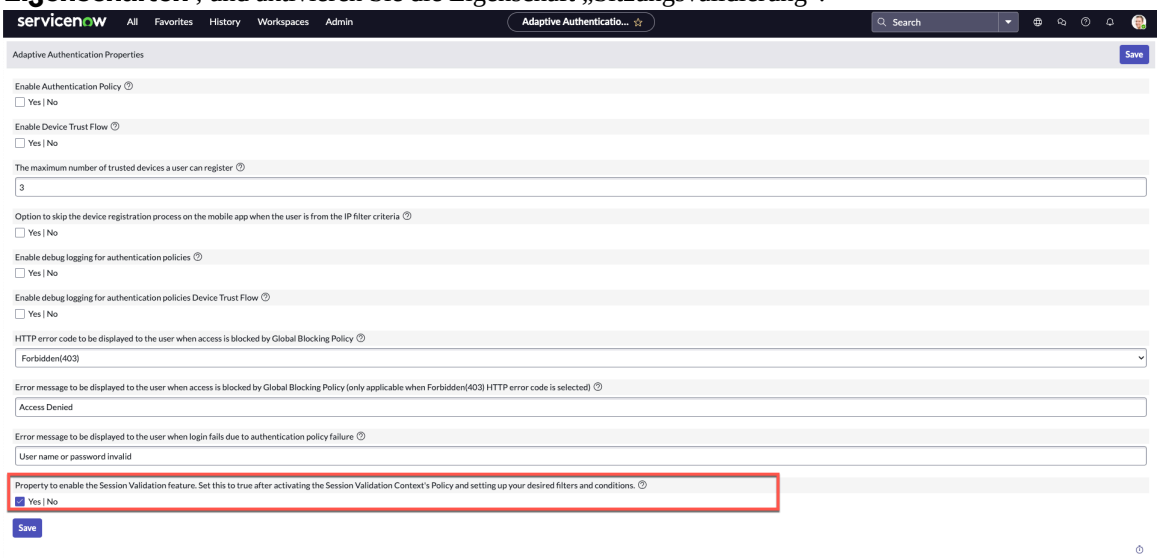
Sie können die Bedingungen basierend auf der Konfiguration der Richtlinieneingabe auf „ true “ oder „ false “ festlegen. In diesem Beispiel ist er auf truefestgelegt. Wenn Sie die Bedingung in diesem Fall auf „true“ setzen, kann sich nur der Benutzer mit der konfigurierten IP-Adresse anmelden.



5. Aktivieren Sie das Kontrollkästchen Aktiv, um die Richtlinie zu aktivieren, nachdem die Sitzungsvalidierungsrichtlinie mit Richtlinieneingaben und -bedingungen eingerichtet wurde.



6. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften** , und aktivieren Sie die Eigenschaft „Sitzungsvalidierung“.

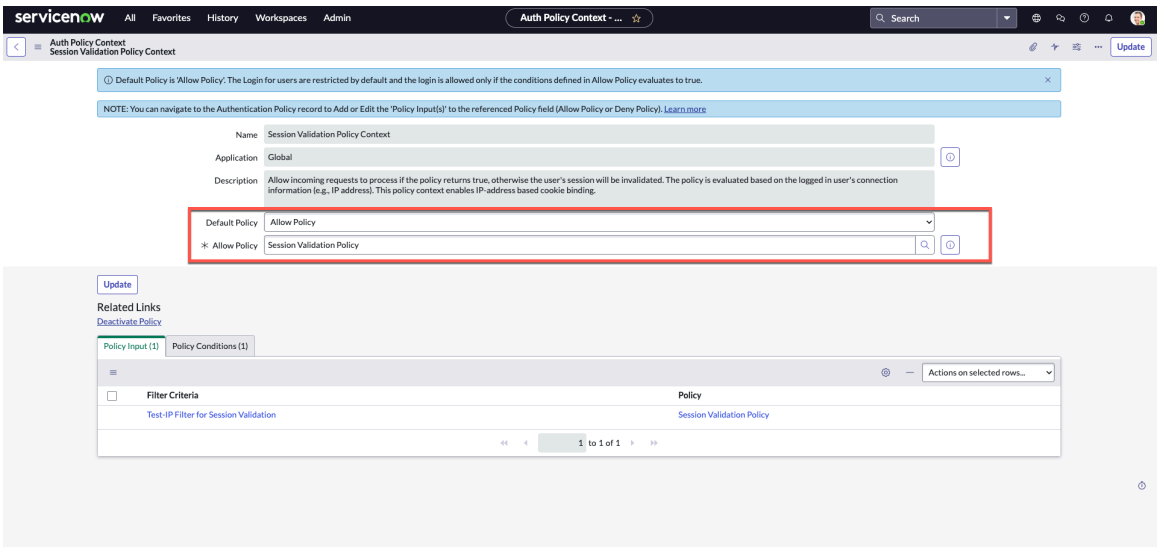


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Sitzungsvalidierungskontext**.
8. Legen Sie die Standardrichtlinie auf **Allow Policy** (Zulassungsrichtlinie) oder **Deny Policy** (Verweigerungsrichtlinie) fest, um den Sitzungsvalidierungskontext gemäß der Richtlinieneingabe und den Richtlinienbedingungen festzulegen.

Hinweis:
Standardmäßig gilt:

- Der Kontext der Sitzungsvalidierung ist auf **Allow Policy**festgelegt.
- Zulassungsrichtlinie ist als **Sitzungsvalidierungsrichtlinie**ausgewählt.



Ergebnisse

Die Konfiguration wertet die Anmeldesitzung basierend auf Folgendem aus:

- Beschränkt den Zugriff auf die Instanz ServiceNow®, wenn Hijacking-Anwender Sitzungscookies eines Benutzers von einem Gerät auf ein anderes kopieren, um die Identität einer Sitzung anzunehmen.
- Schränkt den Sitzungszugriff des Benutzers ein, wenn er ein unsicheres Netzwerk verwendet.

Authentifizierungsrichtlinien

Authentifizierungsrichtlinien werten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen aus und erlauben oder verweigern den Zugriff abhängig von der Ausgabe der Auswertung der Richtlinienbedingungen. Beispielsweise ist der Zugriff nur zulässig, wenn alle in der **Zugriffsrichtlinie angegebenen Richtlinienbedingungen** als „wahr“ ausgewertet werden.

Verwenden Sie die integrierten Authentifizierungsrichtlinien, oder erstellen Sie eine Authentifizierungsrichtlinie gemäß Ihren Sicherheitsanforderungen. Sie finden die Richtlinien in Ihrer Instanz, indem Sie zu navigieren **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**.

Hinweis:
Zu jedem Zeitpunkt kann entweder eine Zugriffsrichtlinie oder eine Zugriffsverweigerungsrichtlinie ausgeführt werden, aber nicht beides.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie	Beschreibung
Zugriffsrichtlinie zulassen	Lehnt standardmäßig alle Authentifizierungsanforderungen ab. Erlaubt nur die Authentifizierungsanforderungen, die den angegebenen Richtlinienbedingungen entsprechen.
Vorauthentifizierungsrichtlinie für Zugriffsgenehmigung	Vorauthentifizierungsrichtlinie für Zugriff zulassen.
Nicht lokal angemeldete Benutzer zulassen	Wählen Sie diese Richtlinie aus, um Benutzer mit nicht lokaler Anmeldung zuzulassen. Wird im Kontext von SSO-Wiederherstellungs-Flows verwendet.
Zugriffsverweigerungsrichtlinie	Ermöglicht standardmäßig die Authentifizierungsanforderungen. Verweigert nur die Authentifizierungsanforderungen, die den angegebenen Richtlinienbedingungen entsprechen.
Globale Blockierungsrichtlinie	Verweigert die Zugriffsanforderungen von Benutzern und APIs vor der Authentifizierung. Diese Richtlinie kann als Alternative zur IP-Adresszugriffssteuerungverwendet werden.
Richtlinie zur Sitzungsvalidierung	Die Authentifizierungsrichtlinie wertet Filterkriterien (z. B. IP-Adresse) aus, um zu bestimmen, ob eine Sitzung für eingehende Anforderungen aktiv bleiben soll. Sie müssen die Filterkriterien für diese Richtlinie festlegen.
Richtlinie zum Verweigern der lokalen Anmeldung	Wählen Sie diese Richtlinie aus, um alle lokalen Anmeldungen zu blockieren. Wird im Kontext von SSO-Wiederherstellungs-Flows verwendet.
Step-Down-MFA-Richtlinie	Wählen Sie die **Step-Down-MFA-Richtlinie** als Standardrichtlinie in Situationen aus, in denen Benutzer keine MFA-Authentifizierung benötigen. Wenn die in der Step-Up-MFA-Richtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden, müssen sich Benutzer nicht mit MFA anmelden.
Step-up-MFA-Richtlinie	Wählen Sie **Step-Up-MFA-Richtlinie** als Standardrichtlinie aus, um die MFA-Authentifizierung zu erfordern, wenn die in der Step-Up-MFA-Richtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

Konfigurieren Sie eine Authentifizierungsrichtlinie

Konfigurieren Sie eine Authentifizierungsrichtlinie, um Eingaben und Bedingungen zu definieren, die verwendet werden, um Zugriff auf eine Instanz zu gewähren oder die Multifaktor-Authentifizierung zu erzwingen.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**.

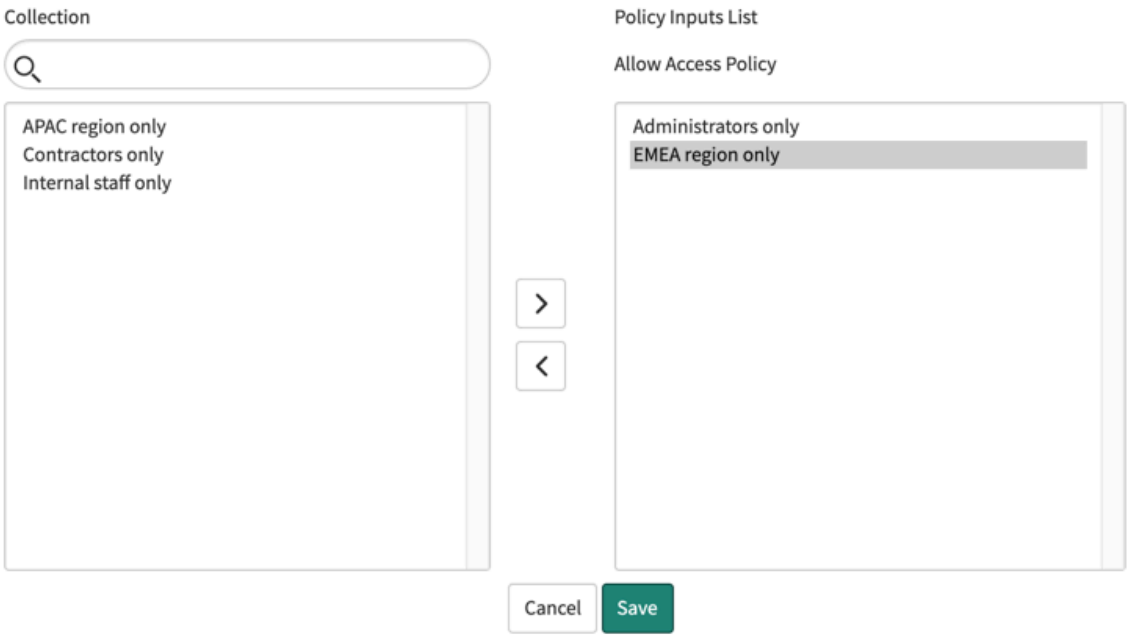
   Hinweis:
   Beispiele für abgeschlossene Richtlinien finden Sie in den folgenden Richtlinien in Ihrer Instanz:
   - DEMO-RICHTLINIE: Lokale Anmeldung für Administratoren nur aus dem vertrauenswürdigen IP-Bereich zulassen
   - DEMO-RICHTLINIE: Lokale Anmeldung nur für Administratoren zulassen
   - DEMO-RICHTLINIE – Benutzername- und passwortbasierte Authentifizierung für bestimmte Anwender einschränken

2. Klicken Sie auf die Schaltfläche **Neu**, um einen neuen Richtliniendatensatz zu erstellen.
3. Füllen Sie die Felder im Formular **„Richtlinie“** aus.

Richtlinienformular

Feld	Beschreibung
Name	Name der Richtlinie.
Anwendung	Die bereichsbezogene Anwendung für die Richtlinie. Dieses Feld wird automatisch mit der aktuellen Anwendung ausgefüllt.
Beschreibung	Beschreibung der Richtlinie
Aktiv	Gibt an, ob die Richtlinie aktiv ist.

4. Klicken Sie auf der Registerkarte **Richtlinieneingaben** auf **Bearbeiten**.
5. Wählen Sie ein oder mehrere Filterkriterien aus der Liste „ **Sammlung“** aus, und verschieben Sie sie in die Liste „ **Richtlinieneingaben** “ der Liste **„Zugriffsrichtlinie zulassen“**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Informationen zum Erstellen eigener Filterkriterien zur Verwendung in diesem Abschnitt finden Sie unter .

6. Klicken Sie auf der Registerkarte **Richtlinienbedingungen** auf **Neu**.
7. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination mehrerer Richtlinieneingaben (Filterkriterien), die zum Auswerten von Authentifizierungsanforderungen verwendet wird. Sie können beispielsweise Bedingungen erstellen, die nur Auftragnehmer aus einer Liste vertrauenswürdiger IP-Adressen zulassen.

8. **Wahlweise:** Wiederholen Sie Schritt 7, um zusätzliche Richtlinienbedingungen zu erstellen.

Hinweis:
Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen OR-Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „wahr“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

9. Klicken Sie auf **Speichern**.

Fügen Sie einem Authentifizierungsrichtlinienkontext eine Authentifizierungsrichtlinie hinzu

Fügen Sie einem der Authentifizierungsrichtlinienkontexte eine Authentifizierungsrichtlinie hinzu. Der Authentifizierungskontext verwendet die Richtlinieneingaben und -bedingungen, um zu bestimmen, ob Benutzern Zugriff auf die Instanz gewährt wird oder ob MFA für Benutzer erzwungen wird.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie**, und wählen Sie je nach Bedarf einen der Einträge aus.

Kontext vor der Authentifizierung

Verwenden Sie den Vorautorisierungskontext, um Ihre Richtlinie auszuwerten, bevor der Benutzer den Anmeldebildschirm sieht. Basierend auf dieser Auswertung wird Benutzern der Zugriff gewährt oder verweigert.

Kontext nach der Authentifizierung

Verwenden Sie den Kontext nach der Autorisierung, um Ihre Richtlinie auszuwerten, nachdem der Benutzer seine Anmeldeinformationen eingegeben hat. Basierend auf dieser Auswertung wird Benutzern der Zugriff gewährt oder verweigert. Da diese Auswertung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erfolgt, nachdem die Instanz den Benutzer identifiziert hat, können Richtlinien in diesem Kontext ihre Bewertung basierend auf Benutzerdaten wie Rolle oder Gruppe vornehmen.

MFA-Kontext

Verwenden Sie den MFA-Kontext, um zu bestimmen, ob ein Benutzer bei der Anmeldung die Multifaktor-Authentifizierung verwenden muss.

Sitzungsvalidierungskontext

Verwenden Sie den Sitzungsvalidierungskontext, um die IP-Adresse auszuwerten, die basierend auf den als Filter definierten Bedingungen festgelegt wird und den Zugriff auf die Instanz innerhalb einer Sitzung ermöglicht.

2. **Wählen Sie im Feld Standardrichtlinie** einen Wert aus.
   Der Wert in diesem Feld bestimmt, wie der Kontext das Ergebnis der Bedingungen Ihrer Richtlinie verwendet.

   Die verfügbaren Optionen in diesem Feld hängen vom ausgewählten Kontext ab. Weitere Informationen zu diesen Kontexten finden Sie unter Kontexte der Authentifizierungsrichtlinie.

3. Weisen Sie dem Kontext eine Richtlinie zu.
   Der Name des Felds hängt davon ab, welchen Kontext Sie ausgewählt haben.

   Kontext vor und nach der Authentifizierung

   Diese Kontexte verfügen über ein Feld **Verweigerungsrichtlinie** oder **Zulassungsrichtlinie**, abhängig von der Auswahl im Feld **Standardrichtlinie**.

   MFA-Kontext

   Dieser Kontext verfügt über ein Feld **Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie**, abhängig von der Auswahl im Feld **Standardrichtlinie**.

   Sitzungsvalidierungskontext

   Dieser Kontext verfügt über ein Feld **Allow-Richtlinie** oder **Deny-Richtlinie**, abhängig von der Auswahl im Feld **Standardrichtlinie**.

4. Klicken Sie auf **Aktualisieren**.
   Nach der Aktualisierung des Datensatzes können Sie die Eingaben und Bedingungen Ihrer Richtlinie auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** anzeigen.

Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung

Konfigurieren Sie nach der Aktivierung der adaptiven Authentifizierung die Eigenschaften der adaptiven Authentifizierung entsprechend Ihren Sicherheitsanforderungen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**.
2. Konfigurieren Sie die folgenden Eigenschaften:

Adaptive Authentifizierung – Eigenschaften

Eigenschaft	Beschreibung	Wert
Authentifizierungsrichtlinie aktivieren (glide.authenticate.auth.policy.enabled)	Option zum Aktivieren der Authentifizierungsrichtlinie.	Ja | Nein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Wert
Debug-Protokollierung für Authentifizierungsrichtlinien aktivieren (glide.authenticate.policy.debug)	Option zum Aktivieren der Debug-Protokollierung für die Authentifizierungsrichtlinien.	Ja | Nein
HTTP-Fehlercode, der dem Anwender angezeigt werden soll, wenn der Zugriff durch die globale Sperrrichtlinie blockiert wird (glide.authenticate.global.blocking_policy.error_code)	HTTP-Fehlercode, der während der Anmeldung angezeigt wird, wenn die globale Blockierungsrichtlinie eine Benutzeranmeldung blockiert.	Wählen Sie aus: ○ Unzulässig (403) ○ Nicht gefunden (404)
Fehlermeldung, die dem Anwender angezeigt werden soll, wenn der Zugriff durch die globale Sperrrichtlinie blockiert wird (nur anwendbar, wenn HTTP-Fehlercode „Forbidden(403)“ ausgewählt ist) (glide.authenticate.global.blocking_policy.error_message)	Fehlermeldung, die angezeigt wird, wenn die globale Sperrrichtlinie den Zugriff blockiert	Textfeld
Gerätevertrauens-Flow aktivieren (glide.authenticate.preauth.allow.trusted.device)	Option zum Aktivieren des vertrauenswürdigen Geräte-Flows.	Ja | Nein
Maximale Anzahl der vertrauenswürdigen Geräte, die ein Benutzer registrieren kann (glide.trusted.device.max.count)	Dies ist die maximale Anzahl vertrauenswürdiger Geräte, die ein Benutzer registrieren kann.	Textfeld
Geräteregistrierung für Gerätevertrauens-Flow überspringen, wenn der Benutzer aus dem vertrauenswürdigen Netzwerk stammt (glide.authenticate.preauth.skip.user.registration)	Option zum Überspringen der Registrierung, wenn der Benutzer versucht, sich über das vertrauenswürdige Netzwerk zu registrieren	Ja | Nein
Eigenschaft zum Aktivieren der Sitzungsvalidierungsfunktion. Legen Sie diese Option auf „wahr“ fest, nachdem Sie die Richtlinie des Sitzungsvalidierungskontexts aktiviert und die gewünschten Filter und Bedingungen eingerichtet haben (session.validation.enabled).	Option zum Aktivieren der Sitzungsvalidierungsfunktion. Legen Sie diese Option auf „true“ fest, nachdem Sie die Richtlinie des Sitzungsvalidierungskontexts aktiviert und die gewünschten Filter und Bedingungen eingerichtet haben.	Ja | Nein

Tutorial: Konfigurieren der adaptiven Authentifizierung

Verwenden Sie diese Beispielschritte, um die adaptive Authentifizierung für eine Instanz zu konfigurieren.

Um dieses Tutorial zu verwenden, benötigen Sie eine Instanz mit aktivierter adaptiver Authentifizierung. Details zu diesem Vorgang finden Sie unter Aktivieren Sie die adaptive Authentifizierung.

Das Beispiel führt Sie durch die Erstellung einer neuen Richtlinie und deren Anwendung auf eine Instanz. In diesem Tutorial werden Sie:

Erstellen Sie einen Filterkriteriendatensatz

Erstellen Sie einen Datensatz für Gruppenfilterkriterien, der als Eingabe für Ihre Richtlinie verwendet werden soll. Mit diesem Datensatz kann Ihre Richtlinie den Zugriff basierend auf der Gruppe eines Benutzers bestimmen. In diesen Schritten der Anleitung definieren Sie die Gruppe oder Gruppen, anhand derer die Richtlinie den Zugriff bestimmt.

Erstellen Sie eine Richtlinie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Richtlinie, die bestimmt, ob ein Benutzer auf die Instanz zugreifen kann. Diese Richtlinie verwendet den von Ihnen erstellten Datensatz für Gruppenfilterkriterien als Eingabe. In diesen Schritten definieren Sie auch Richtlinienbedingungen, die definieren, wie die Richtlinie die Richtlinieneingabe verwendet, um den Benutzerzugriff zu bestimmen.

Konfigurieren Sie einen Richtlinienkontext

Konfigurieren Sie den **Post Authentication-Richtlinienkontext** so, dass Ihre neue Richtlinie verwendet wird. Nach der Konfiguration verweigert Ihre Instanz Benutzern innerhalb der im Filterkriteriendatensatz definierten Gruppe den Zugriff.

Erstellen Sie einen Filterkriteriendatensatz

Erfahren Sie, wie Sie einen Kriteriendatensatz erstellen, der als Richtlinieneingabe für Ihre Richtlinie für die adaptive Authentifizierung verwendet werden soll.

Vorbereitungen

Erforderliche Rolle: admin

Um den Zugriff auf Ihre Instanz basierend auf Benutzergruppen zu verweigern, müssen Sie einen Datensatz für Gruppenfilterkriterien erstellen. Dieser Datensatz definiert eine Benutzergruppe oder eine Reihe von Benutzergruppen, denen Ihre Richtlinie den Zugriff gewähren oder verweigern kann. In diesem Beispiel erstellen Sie einen Datensatz mit Gruppenfilterkriterien für eine einzelne Benutzergruppe.

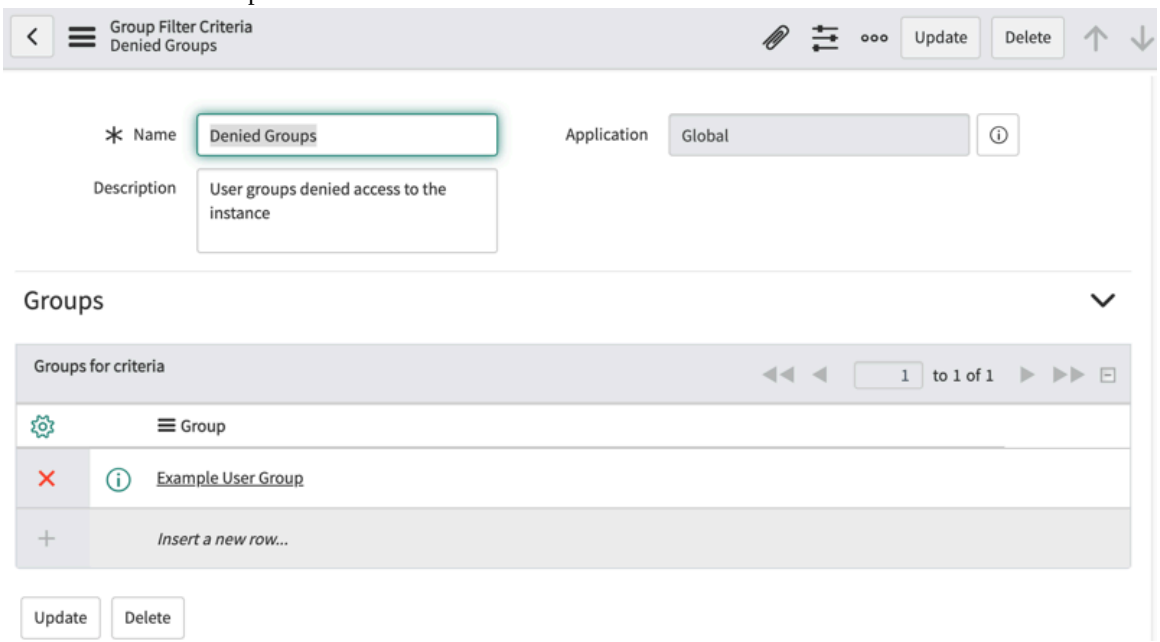
Weitere Informationen zu Benutzergruppen und ihrer Verwendung in Ihrer Instanz finden Sie unter Exploring user administration .

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Gruppenkriterien**.
2. Klicken Sie auf **Neu**, um einen neuen Datensatz zu erstellen.
3. Geben Sie im Feld **Name** einen Namen für Ihren Datensatz ein.
   Beispiel: Ausgelehnte Gruppen.
4. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung ein.
   Beispiel: Benutzergruppen haben Zugriff auf die Instanz verweigert.
5. Doppelklicken Sie in der Liste **Gruppen für Kriterien** auf **Neue Zeile einfügen...**
6. Geben Sie den Namen einer Benutzergruppe ein, oder klicken Sie auf das Referenzsymbol ( ), um eine Gruppe aus einer Liste auszuwählen.
   Wenn Sie eine neue Benutzergruppe für Ihre Filterkriterien erstellen möchten, klicken Sie auf das Referenzsymbol ( ) und dann auf die Schaltfläche **Neu**. Weitere Informationen zum Erstellen von Benutzergruppen finden Sie unter Benutzergruppen erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Nachdem Sie Ihre Benutzergruppe hinzugefügt haben, klicken Sie auf **Absenden**, um den Kriteriendatensatz zu speichern.



Erstellen Sie eine Richtlinie

Erfahren Sie, wie Sie eine Richtlinie erstellen, um den Zugriff auf Benutzergruppen zu verweigern, die in Ihren Gruppenfilterkriterien definiert sind.

Vorbereitungen

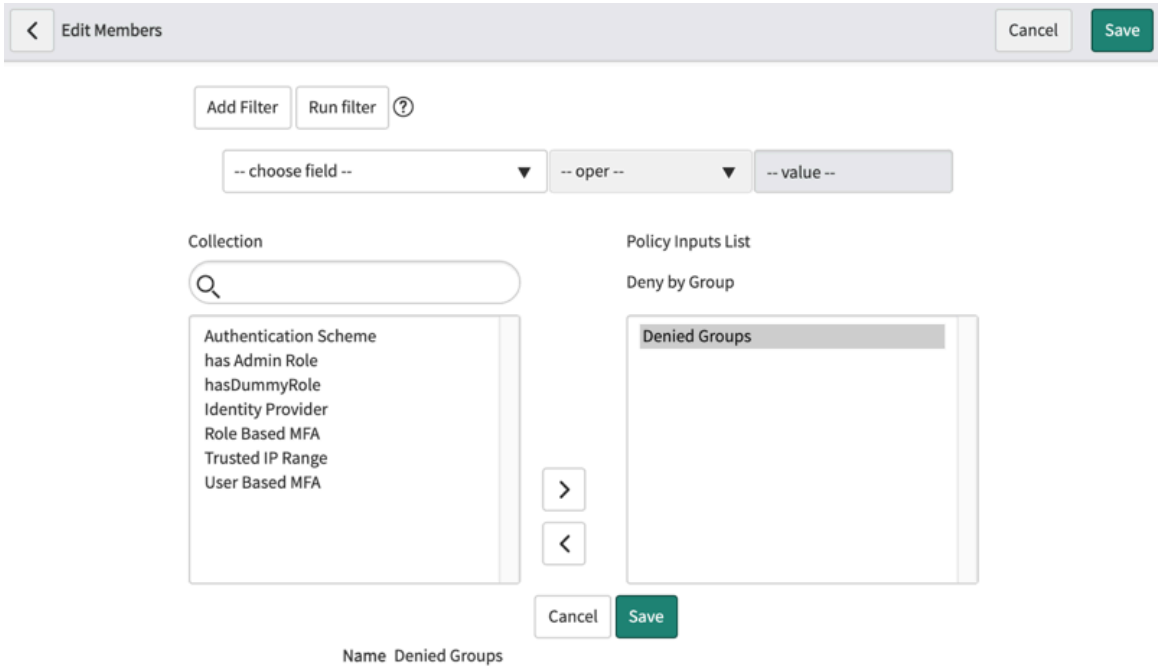
Erforderliche Rolle: admin

Prozedur

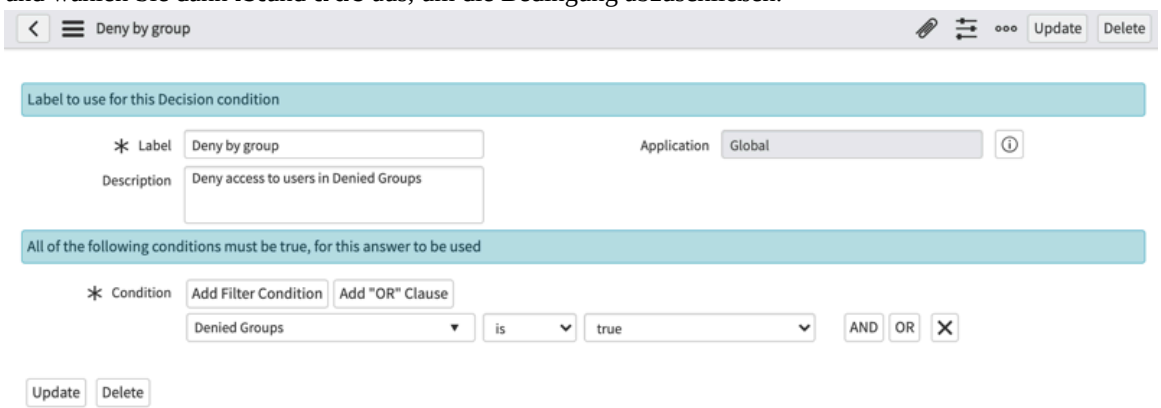
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**.
2. Klicken Sie in der Liste „ **Richtlinien** “ auf **Neu**.
3. Geben Sie im Feld **Name** einen Namen für Ihren Datensatz ein.
   Beispiel: Deny nach Gruppe.
4. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung ein.
   Beispiel: Benutzergruppen haben Zugriff auf die Instanz verweigert.
5. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
   Nach dem Speichern werden die Listen **Richtlinieneingaben** und **Richtlinienbedingungen** im Formular angezeigt.
6. Klicken Sie in der Liste **„Richtlinieneingaben“** auf **Bearbeiten**.
7. Fügen Sie im Listensammler die in den vorherigen Schritten erstellten Filterkriterien zu Ihrer Richtlinie hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Klicken Sie auf **Speichern**.
   Die Instanz speichert die Richtlinieneingabe und zeigt den Richtliniendatensatz erneut an.
9. Klicken Sie in der Liste **Richtlinienbedingungen** auf **Neu**.
10. **Erstellen Sie** im Feld Bezeichnung eine Bezeichnung für diese Bedingung, z. B. `Deny by group`(Nach Gruppe verweigern).
11. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung ein.
    Beispiel: `Zugriff für Benutzer in verweigerten Gruppen verweigern`.
12. Wählen Sie im Feld **Bedingung** die Filterkriterien aus, die Sie in den vorherigen Schritten erstellt haben, und wählen Sie dann **ist**und **true** aus, um die Bedingung abzuschließen.



13. Klicken Sie auf **Speichern**.

Konfigurieren Sie einen Richtlinienkontext

Konfigurieren Sie den Post Authentication-Richtlinienkontext so, dass Ihre neue Richtlinie verwendet wird. Nach der Konfiguration verweigert Ihre Instanz Benutzern innerhalb der im Filterkriteriendatensatz definierten Gruppe den Zugriff.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext nach der Authentifizierung**.
   Sie müssen den **Kontext nach der Authentifizierung** verwenden, da die in diesem Tutorial verwendete Richtlinie auswerten muss, zu welcher Gruppe ein Benutzer gehört. Diese Informationen sind nur verfügbar, nachdem die Anmeldeinformationen eingegeben wurden.
2. Wählen Sie im Feld **Standardrichtlinie** die Option Verweigerungsrichtlinieaus.
   Diese Auswahl gewährt Benutzern standardmäßig Zugriff und verweigert den Zugriff nur, wenn die Richtlinienbedingungen als „wahr“ ausgewertet werden.
3. Wählen Sie im Feld **Deny Policy** (Verweigerungsrichtlinie) die Richtlinie aus, die Sie in den vorherigen Schritten erstellt haben.
4. Klicken Sie auf **Aktualisieren**, um den Richtlinienkontextdatensatz zu speichern.

Adaptive Authentifizierung für vertrauenswürdige Mobile-Apps

Greifen Sie über den ServiceNow aus nicht vertrauenswürdigen Netzwerken auf Now Mobile-Appzu.

Adaptive Authentifizierung für vertrauenswürdige Mobile-Apps

Mit der adaptiven Authentifizierung für vertrauenswürdige Mobile-Apps können Benutzer über ServiceNow auf die Instanz Now Mobile-Appzugreifen. Die Instanz ist hinter einer vertrauenswürdigen IP-Netzwerkgrenze geschützt.

Im Folgenden sind einige der Szenarien aufgeführt, in denen Sie Zugriff auf die Instanz benötigen, während Sie sich außerhalb Ihres Netzwerks befinden.

Als Mitarbeiter müssen Sie von außerhalb des Netzwerks auf Now Mobile-App und das Employee Service Center (Portal) zugreifen. Mit dem Filter für vertrauenswürdige Mobile-Apps können Sie die eingehende Anforderung identifizieren, die von einem vertrauenswürdigen Now Mobile-App stammt, der mit einem Benutzerkonto verknüpft ist.

Als Administrator können Sie die Richtlinie konfigurieren. Mit der Richtlinie können Benutzer ihre Mobilgeräte registrieren und in einem vertrauenswürdigen Netzwerk auf die Instanz zugreifen.

Als Benutzer können Sie Ihr Mobilgerät registrieren, indem Sie den in der Instanz angezeigten QR scannen. Nach der Registrierung können Sie sich über Now Mobile-Appmit Ihren -Anmeldeinformationen bei Ihrer Instanz anmelden.

Hinweis:
Um das Mobilgerät registrieren zu können, müssen Sie sich in einem vertrauenswürdigen Netzwerk befinden. Nach der Registrierung können Sie sich auch aus anderen Netzwerken bei der Instanz anmelden.

Funktionen

Als Administrator können Sie die folgenden Funktionen verwenden:

- Konfigurieren Sie Richtlinien mithilfe von Filterkriterien für vertrauenswürdige Apps.
- Erstellen Sie Richtlinienbedingungen mit neuen Filterkriterien für vertrauenswürdige Mobile-Apps.
- Unterstützen Sie alle Anmeldemethoden in der vertrauenswürdigen mobilen App für die Benutzer (lokale Anmeldung, SAML, OIDC und MFA).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Widerrufen Sie ein vertrauenswürdiges Gerät.
- Fügen Sie Sicherheitsereignisse für alle Aktionen zur Geräteregistrierung oder -widerrufung hinzu. Die Events können verwendet werden, um den Benutzer zu benachrichtigen.
- Unterstützen Sie Sicherheits-Events für Signaturfehler, Fehler bei der Cookie-Validierung, ungültige Token, ungültige Header oder Abfrageparameter.
- Steuern Sie die maximale Anzahl registrierter Geräte.
- Verhindern Sie eine neue Geräteregistrierung, es sei denn, der Benutzer entfernt ein vorhandenes gekoppeltes Gerät.
- Erfassen Sie den Zeitpunkt, zu dem ein Gerät zuletzt verwendet wurde.

Aktivieren Sie Trusted Mobile App

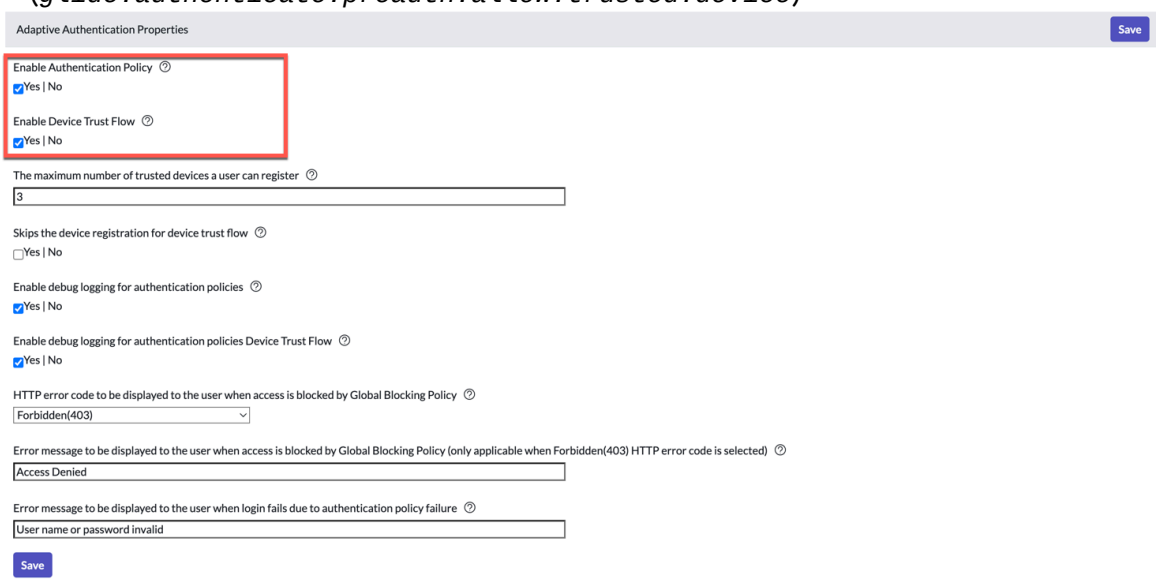
Aktivieren Sie die adaptive Authentifizierung mit der Trusted Mobile-App mithilfe der Authentifizierungsrichtlinie und der Filterbedingungen.

Vorbereitungen
Stellen Sie sicher, dass das Plugin „Adaptive Authentifizierung“ (`com.snc.adaptive_authentication`) installiert ist.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**.
2. Aktivieren Sie auf der Seite „Eigenschaften der adaptiven Authentifizierung“ die folgenden Eigenschaften:
   - Authentifizierungsrichtlinie aktivieren (`glide.authenticate.auth.policy.enabled`)
   - Gerätevertrauens-Flow aktivieren (`glide.authenticate.preauth.allow.trusted.device`)



Hinweis:
Um die Gerätevertrauens-Flow-Eigenschaft zu deaktivieren, müssen Sie die Bedingungen mit dem Filter für vertrauenswürdige Mobilgeräte entfernen. Andernfalls wird eine Fehlermeldung angezeigt, um die Bedingungen zu entfernen.

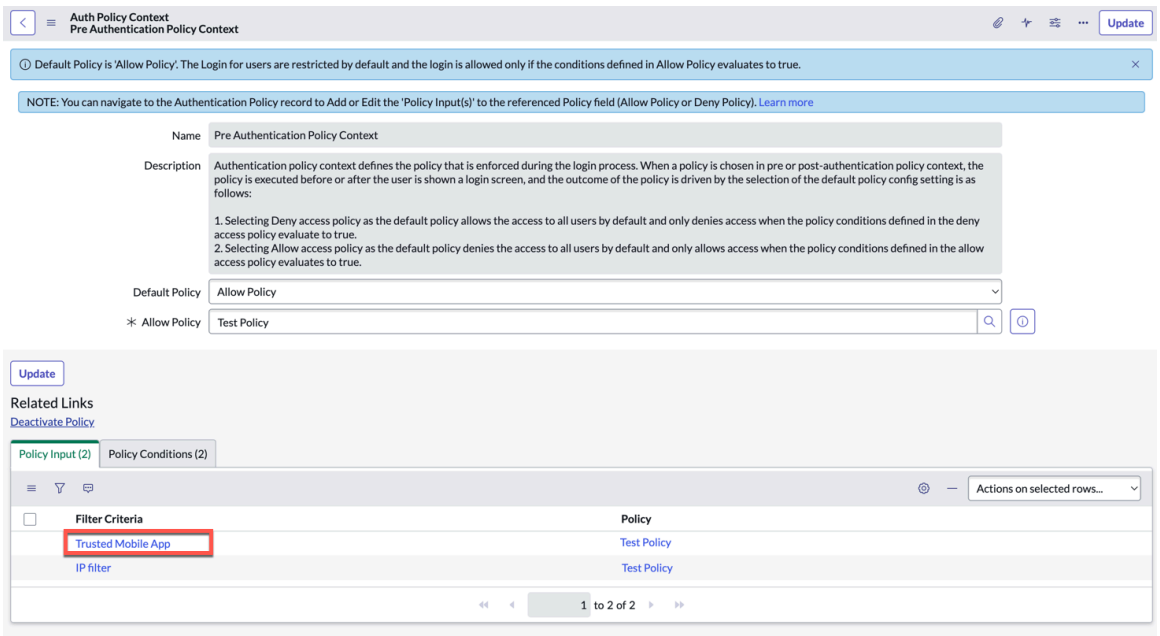
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext vor der Authentifizierung**.
4. Definieren Sie die Bedingungen im Kontext der Vorauthentifizierung.
   Für weitere Informationen Kontext vor der Authentifizierung.

Hinweis:
Standardmäßig lautet die Richtlinienbedingung **Deny Policy**(Verweigerungsrichtlinie). Sie können in **Allow-Richtlinie**ändern. Diese Richtlinien sind direkte Gegensätze.

- Mit der **Allow-Richtlinie**wird allen Benutzern standardmäßig der Zugriff verweigert. Der Zugriff wird nur zugelassen, wenn die Bedingungen der Zugriffsberechtigungsrichtlinie erfüllt sind.
- Mit der **Deny-Richtlinie**wird standardmäßig allen Benutzern der Zugriff gewährt. Der Zugriff wird nur verweigert, wenn die Bedingungen der Zugriffsverweigerungsrichtlinie erfüllt sind.

In der Richtlinieneingabe ist die Richtlinieneingabe **Trusted Mobile App** eine Richtlinieneingabe für die vertrauenswürdige Mobile-App.

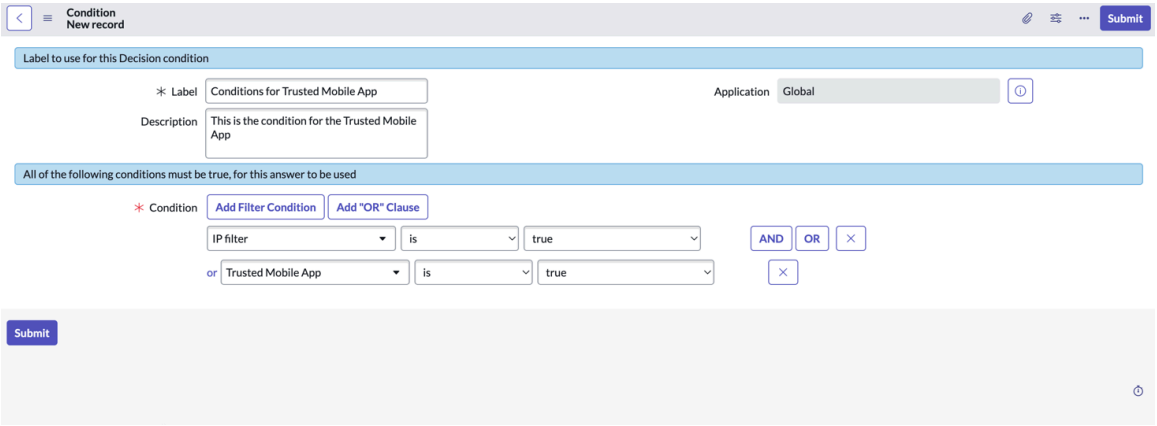


5. Erstellen Sie in den Richtlinienbedingungen die Bedingung, indem Sie auf **Neu**klicken.
6. Füllen Sie die Felder im Formular aus.

Formular „Filterbedingung“

Feld	Beschreibung
Bezeichnung	Name der Bedingung
Beschreibung	Beschreibung der Bedingung
Anwendung	Anwendungsbereich für diesen Datensatz
Bedingung	Bedingungen basierend auf AND und OR. Da die Auth-Richtlinie auf **Allow Policy**festgelegt ist, wird die Bedingung für Trusted Mobile App im Beispiel der Abbildung auf „true“ gesetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.

Ergebnisse

Die Richtlinieneingabe und die Filterbedingungen werden für die Funktion „Vertrauenswürdiges Gerät“ erstellt. Benutzer können mit der Funktion „Vertrauenswürdiges Gerät“ fortfahren, um über den Now Mobile-App] aus nicht vertrauenswürdigen Netzwerken auf die Instanz ServiceNow zuzugreifen. Weitere Informationen finden Sie unter Registrieren Sie ein vertrauenswürdiges Gerät.

Registrieren Sie ein vertrauenswürdiges Gerät

Registrieren Sie ein vertrauenswürdiges Gerät, um außerhalb des Netzwerks auf die Instanz ServiceNow zuzugreifen.

Vorbereitungen

Sie müssen sich im vertrauenswürdigen Netzwerk befinden, um die Registrierung des vertrauenswürdigen Geräts durchzuführen.

Erforderliche Rolle: keine

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:

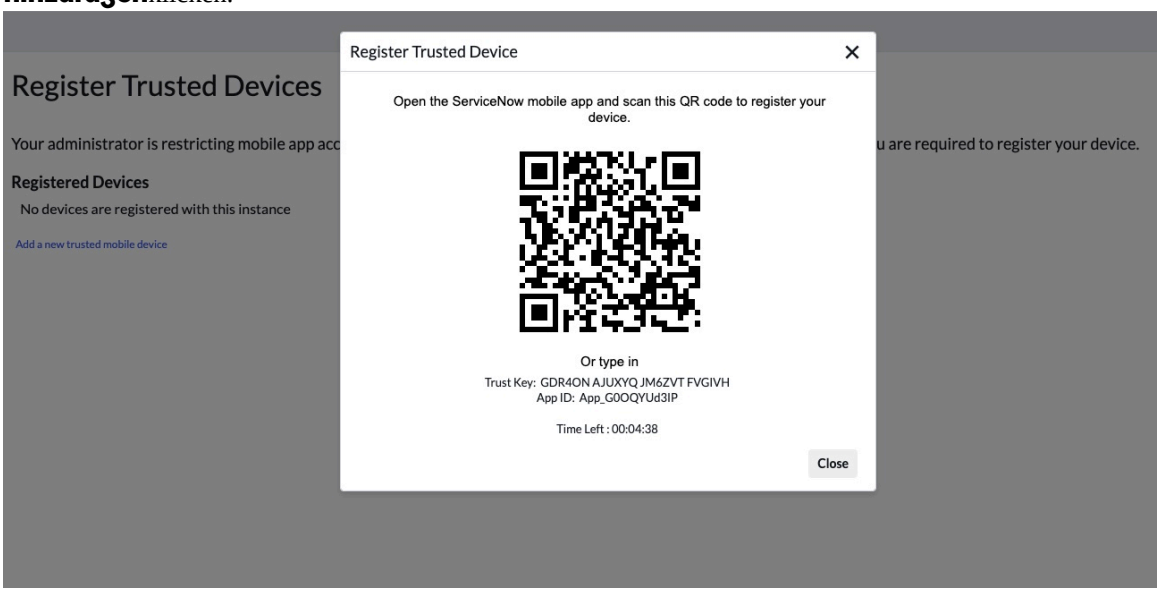
- Navigieren Sie auf Now Platformzu **Alle** > **Selfservice** > **Mein Profil**.

  Hinweis:
  Sie können Ihr Profil auch aufrufen, indem Sie im Instanz-Header auf Ihren Benutzernamen klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

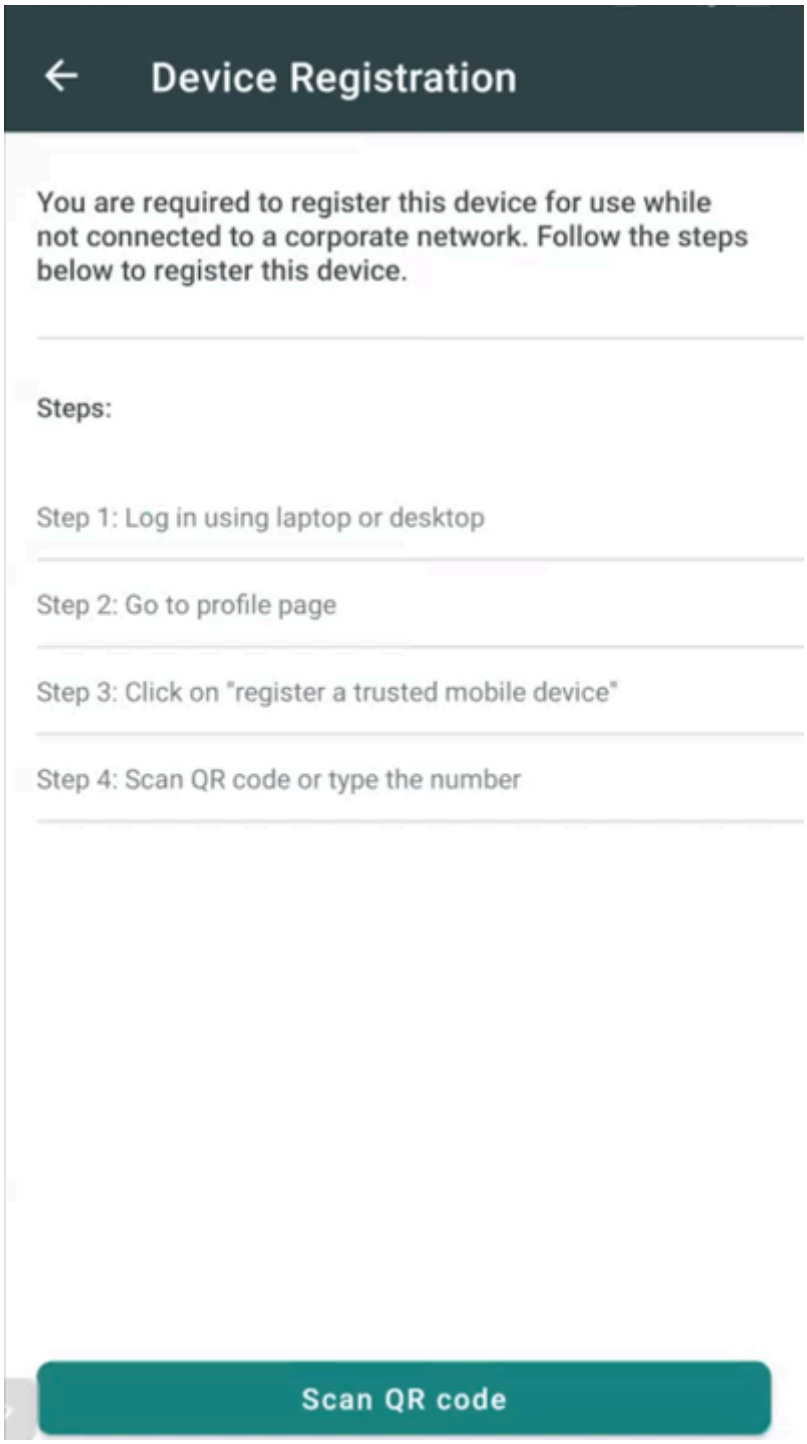
- Klicken Sie unter Now Supportauf das Profil, und wählen Sie **Trusted Device**(Vertrauenswürdiges Gerät) aus.

2. Klicken Sie in Ihrem Benutzerprofil im Abschnitt Zugehörige Links **auf Ein vertrauenswürdiges Mobilgerät registrieren**.
   Die Seite Register Trusted Devices (Vertrauenswürdige Geräte registrieren) wird angezeigt.
3. Registrieren Sie ein neues Gerät, indem Sie auf **Neues vertrauenswürdiges Mobilgerät hinzufügen**klicken.



4. Tippen Sie im Bildschirm „Geräteregistrierung“ in Ihrer Mobile-App ServiceNow auf die Schaltfläche **QR-Code** scannen, und scannen Sie den QR-Code, der auf Ihrem Laptop oder Desktop-Computer angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

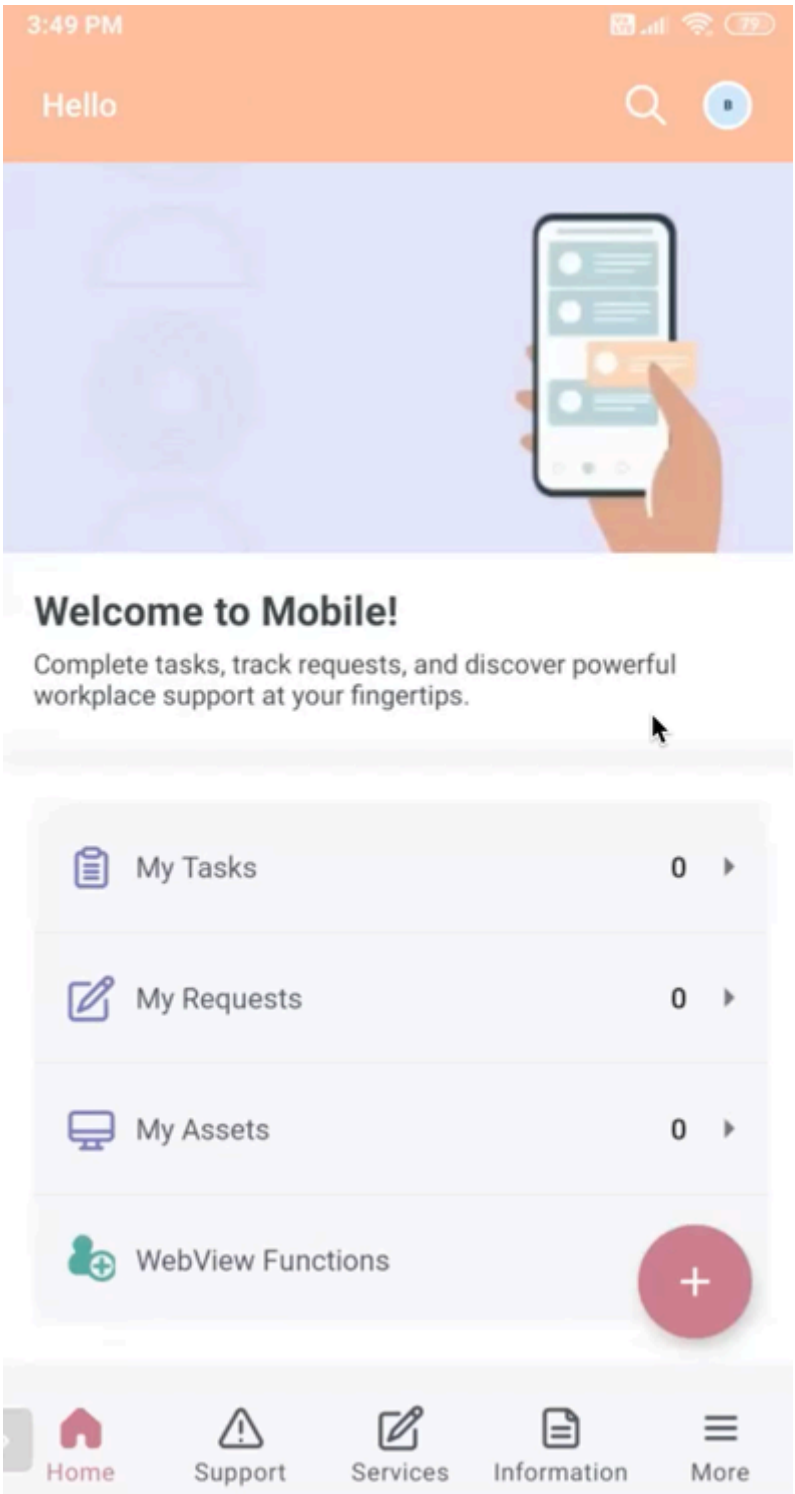


Der Registrierungsprozess wird abgeschlossen, und Sie werden zu Ihrer Anmeldeseite aufgefordert, um Ihre Authentifizierung abzuschließen.

5. Geben Sie Ihre -Anmeldeinformationen an, und melden Sie sich bei Now Mobile-Appan.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Mobile-Startbildschirm wird angezeigt.



Ergebnisse

Auf der Seite „Vertrauenswürdige Geräte registrieren“ auf Ihrem Laptop oder Desktop-Computer wird das registrierte Gerät angezeigt. Sie können das verwenden, wenn Sie das registrierte Gerät von der Seite entfernen möchten.

Nächste Maßnahme

Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Gerätevertrauen** > **Geräteregistrierung** , um alle Details des registrierten Geräts anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Ihr vertrauenswürdiges Gerät

Verwalten Sie Ihr vertrauenswürdiges Gerät über die Registrierungsseite für vertrauenswürdige Geräte.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - Navigieren Sie auf Now Platformzu **Alle** > **Selfservice** > **Mein Profil**.

     Hinweis:
     Sie können Ihr Profil auch aufrufen, indem Sie im Instanz-Header auf Ihren Benutzernamen klicken.

   - Klicken Sie unter Now Supportauf das Profil, und wählen Sie **Trusted Device**(Vertrauenswürdiges Gerät) aus.
2. Klicken Sie in Ihrem Benutzerprofil im Abschnitt Zugehörige Links auf **Register Trusted Device** (Vertrauenswürdiges Gerät registrieren).
   Die Seite Register Trusted Devices (Vertrauenswürdige Geräte registrieren) wird angezeigt.
3. Entfernen Sie das Gerät auf der Seite „Register Trusted Devices“ (Vertrauenswürdige Geräte registrieren), indem Sie auf das “ klicken.

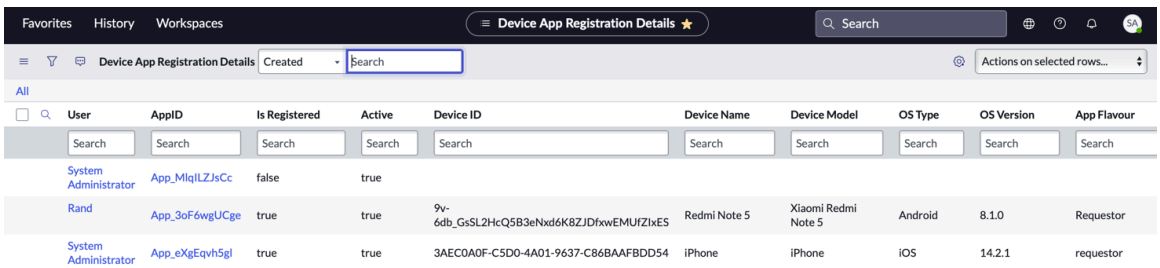
Hinweis:
Das gelöschte Mobilgerät muss erneut registriert werden, um auf die Instanz zugreifen zu können.

Registrierungsdetails der registrierten Geräte

Zeigen Sie die Details der Geräte an, die bei Ihrer ServiceNow -Instanz registriert sind.

Um alle Details des bei der Instanz registrierten Geräts anzuzeigen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Gerätevertrauen** > **Geräteregistrierung**.

Verwenden Sie den Filter, um das Gerät zu identifizieren. Klicken Sie auf das Feld **AppID**, um mehr über das registrierte Gerät zu erfahren.

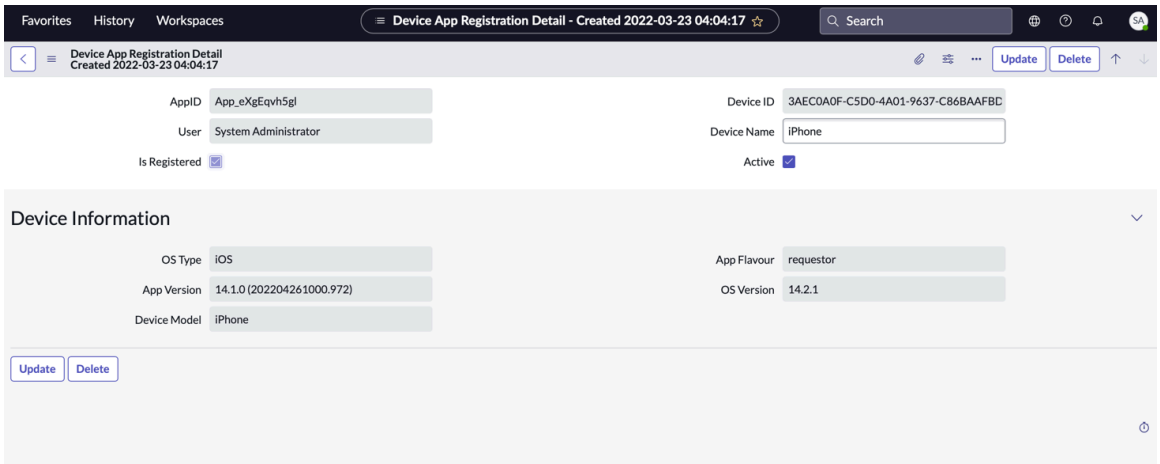


Die folgenden Details werden für das Gerät angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- AppID
- Geräte-ID
- Benutzer
- Gerätename
- Geräteinformationen wie:
  - BS-Typ
  - App-Variante
  - App-Version
  - BS-Version
  - Gerätemodell



Fehlerbehebung bei vertrauenswürdigen Mobile-Apps

Überprüfen Sie diese Problembehandlungsszenarien, um Probleme mit der vertrauenswürdigen Mobile-App zu beheben.

In den folgenden Abschnitten werden einige Problembehandlungsszenarien und Möglichkeiten zur Problembehandlung beschrieben.

Zeitunterschied zwischen Instanz und Mobilgerät (Taktabweichung)

Bei einer Taktabweichung können Sie die Uhr auf Ihrem Mobilgerät für die Verwendung des vertrauenswürdigen Geräts anpassen oder zurücksetzen.

QR-Code läuft innerhalb von fünf Minuten ab

Der QR-Code für die Funktion „Vertrauenswürdiges Gerät“ läuft innerhalb von fünf Minuten ab. In einem solchen Fall können Sie auf klicken, um einen neuen QR-Code zu erhalten.

Hinweis:
Der Ablauf des QR-Codes kann verlängert werden. Wenden Sie sich an Ihren Administrator, um den Codeablauf zu verlängern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaft hat sich geändert

Wenn sich die Systemeigenschaft geändert hat, überprüfen Sie die Registrierung basierend auf der Systemeigenschaft für die gültigen Anmeldeinformationen, die für die Anmeldung verwendet werden können.

Maximale Anzahl registrierter Geräte

Wenn die maximale Anzahl von Geräteregistrierungen erreicht ist, entfernen Sie das vorhandene Gerät, oder wenden Sie sich an Ihren Administrator, um die maximale Geräteanzahl zu ändern.

API-Authentifizierung

Authentifizierungskonfigurationen für -API.

Die API-basierte Authentifizierung in ServiceNow® validiert die Identität eines Benutzers, der auf eine Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Auftragsfunktion des Benutzers entsprechen, während ein API-Aufruf an die Instanz ServiceNow® durchgeführt wird.

Im Folgenden sind die Typen der API-Authentifizierung in ServiceNow® aufgeführt:

- Zertifikatsbasierte Authentifizierung
- OAuth
- Tokenbasierte Authentifizierung

Zertifikatsbasierte Authentifizierung

Mit der zertifikatsbasierten Authentifizierung können Sie eingehende API-Anforderungen gegenseitig mit Zertifikaten einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) authentifizieren.

Zertifikatsbasierte Authentifizierung für eingehende Webservices

Authentifizieren Sie eingehende Anforderungen bei ServiceNow SOAP- und REST-APIs. Informationen zum Einrichten der gegenseitigen Authentifizierung für eingehende Webservices finden Sie unter Richten Sie die zertifikatsbasierte Authentifizierung ein.

OAuth

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensstellung im System herzustellen.

OAuth 2.0 - Open Authorization ist das Branchenstandardprotokoll für Autorisierung, das auf Client-Entwickler-Einfachheit setzt und gleichzeitig spezifische Autorisierungs-Flows für Webanwendungen, Desktop-Anwendungen und Mobilgeräte bereitstellt.

Eingang

Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch werden ein OAuth-Client-Anwendungsdatensatz sowie eine Client-ID und ein Client-Secret erstellt, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt. Weitere Informationen finden Sie unter OAuth eingehend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tokenbasierte Authentifizierung

Tokenbasierte Authentifizierung für die Konfiguration eingehender REST-APIs mit API-Schlüssel oder HMAC.

Support-API-Token für REST-API-Endpunkte, sodass ServiceNow® für die Benutzerauthentifizierung.

Die tokenbasierte Authentifizierung für die Konfiguration eingehender REST-APIs kann in der Instanz ServiceNow® mit dem API-Schlüssel oder dem HMAC-Tokendurchgeführt werden.

API-Schlüssel und HMAC-Authentifizierung für eingehende REST-APIs

Support-API-Token für REST-API-Endpunkte, sodass der Benutzername und das Passwort ServiceNow® in der Webhook-URL nicht sichtbar sind.

Aktivieren Sie die auf API-Schlüsseln basierende Authentifizierung, um die eingehende Webhook-URL sicher zu authentifizieren.

Um den API-Schlüssel und die HMAC-Authentifizierung zu verwenden, müssen Sie (Plugin: `com.glide.tokenbased_auth`) in der Instanz ServiceNow® installieren.

> **⚠ Warnung:**
> Verwenden Sie die **POST** -Anforderung, wenn Sie vertrauliche Informationen an den Server senden.

Die Installation von API-Schlüssel und HMAC-Authentifizierung hat Abhängigkeiten von den folgenden Plugins:

- REST API Auth Scope Plugin (`com.glide.rest.auth.scope`)
- Plugin „REST API Access Policy“ (`com.glide.rest.policy`)
- Authentifizierungsbereich (`com.glide.auth.scope`)

Vorteile

API-Schlüssel und HMAC-Authentifizierung für eingehende REST-APIs ermöglichen Folgendes:

- Möglichkeit zur Angabe des API-Schlüssels oder HMAC-Tokens für die REST-API-Authentifizierung.
- Möglichkeit, ein Benutzerkonto mit dem API-Schlüssel oder HMAC-Token zu verknüpfen.
- Möglichkeit, ein Token als Abfrageparameter oder Header im REST-API-Aufruf anzugeben.
- Möglichkeit, den Authentifizierungsbereich mit API-Schlüssel- oder HMAC-Token-Konfigurationen zu verknüpfen, sodass API-Schlüssel nur zum Aufrufen von APIs verwendet werden können, die bestimmten Bereichen zugeordnet sind.
- Möglichkeit, eine API-Schlüssel- oder HMAC-Token-Konfiguration einem Authentifizierungsprofil zuzuordnen, das in API-Zugriffsrichtlinien verwendet werden kann.

Aktivieren Sie API-Schlüssel und HMAC-Authentifizierung

Sie können den Plugin-API-Schlüssel und die HMAC-Authentifizierung (`com.glide.tokenbased_auth`) in Ihrer ServiceNow® -Instanz aktivieren.

Vorbereitungen
Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „ API Key“ und „HMAC Authentication “ (com.glide.tokenbased_auth).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

API-Schlüssel konfigurieren – Tokenbasierte Authentifizierung

Konfigurieren Sie einen API-Schlüssel, um die Authentifizierung für REST-API-Endpunkte zu unterstützen.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: API-Schlüssel und HMAC-Authentifizierung (com.glide.tokenbased_auth)

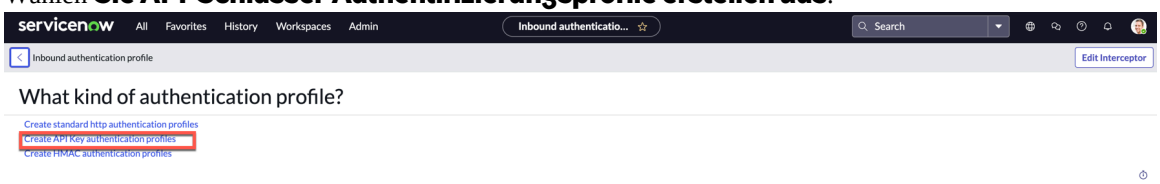
Prozedur

1. Erstellen Sie ein eingehendes Authentifizierungsprofil.

   a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**.

   b. Wählen Sie **Neu**.
   Die Meldung Welche Art von Authentifizierungsprofil?wird angezeigt.

   c. Wählen **Sie API-Schlüssel-Authentifizierungsprofile erstellen aus**.



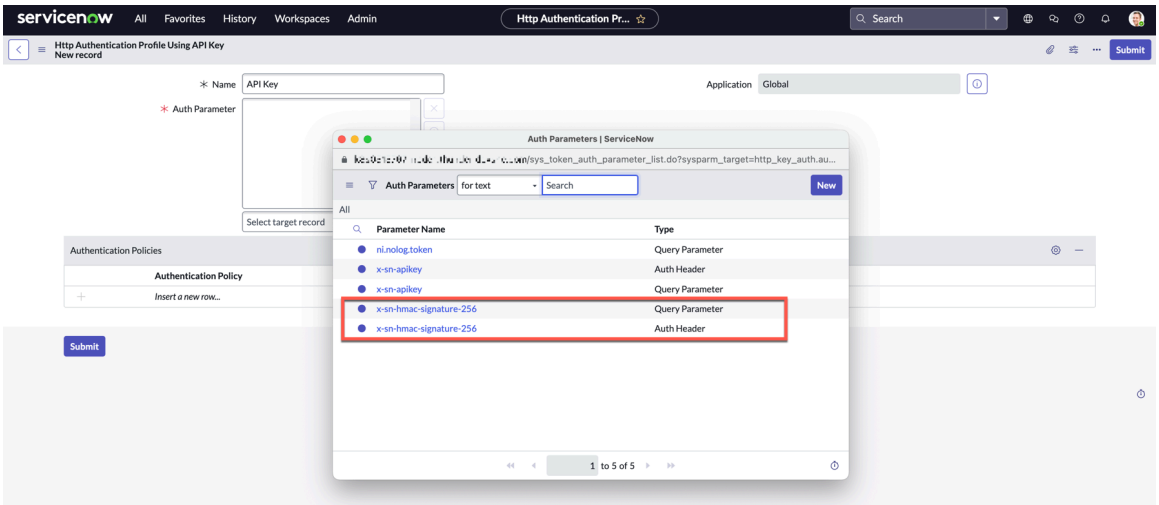
   d. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Schlüsselauthentifizierungsprofile

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Auth-Parameter	Wählen Sie den Auth-Parameter für die Authentifizierungsanforderung aus. Sie können die Standardoptionen auswählen oder einen neuen Authentifizierungsparameter erstellen: ▪ x-sn-apkey: Auth-Header ▪ x-sn-apkey: Abfrageparameter-Header

Hinweis:
Die ausgewählte Option muss im REST-Aufruf als Teil der Auth-Kopfzeile oder des Abfrageparameters definiert werden.



e. Bestätigen Sie das Formular.

2. Erstellen Sie einen REST-API-Schlüssel.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die folgenden Felder aus:

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST-API-Schlüssels
Beschreibung	Beschreibung für den REST-API-Schlüssel.

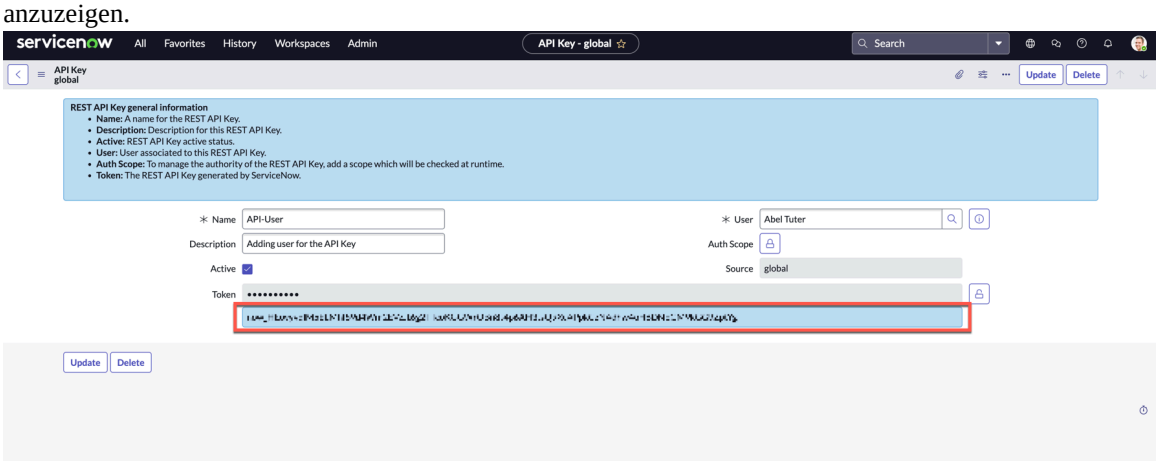
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Status des REST-API-Schlüssels.
Benutzer	Benutzer, der dem REST-API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Benutzer auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen eines Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.
Token	Der von Now Platformgenerierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.

d. Bestätigen Sie das Formular.

e. Öffnen Sie den Datensatz, der erstellt wurde, um das von Now Platform für den Benutzer generierte Token anzuzeigen.



3. Erstellen Sie eine REST-API-Zugriffsrichtlinie.

a. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

API-Zugriffsrichtlinien

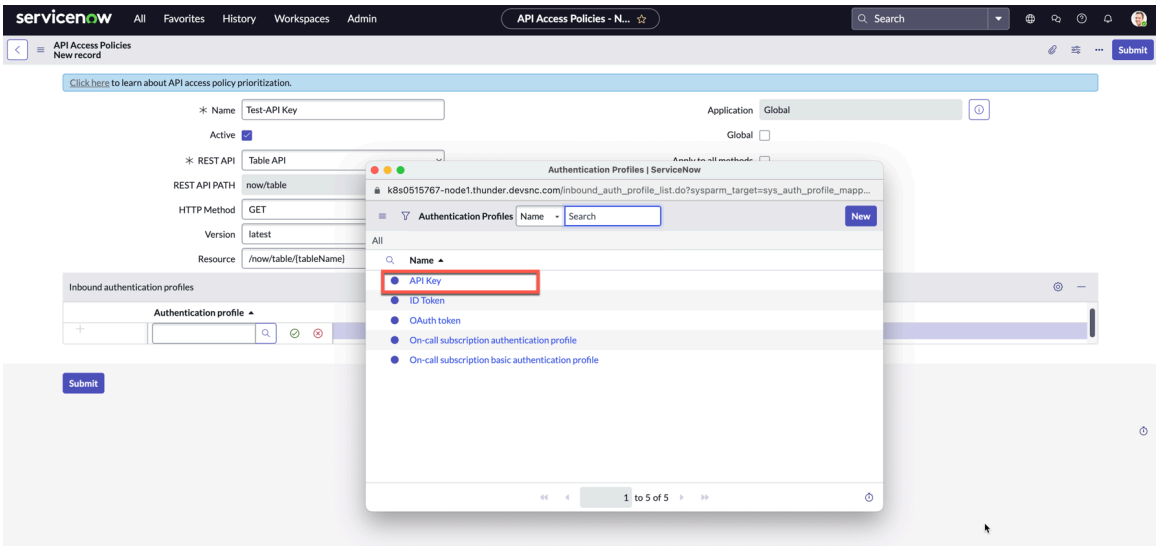
Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API**.
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	automatisch ausgefüllt. Beispiel: **now/attachment**.
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1**. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST-API erstellen möchten, müssen Sie für jede Version eine eigene Richtlinie erstellen.
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **/now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen für die API anzuwenden. **Hinweis:** Tokenbasierte Authentifizierung ist in der globalen REST-API-Richtlinie nicht zulässig.
Auf alle Methoden anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Fügen Sie das erstellte API-Authentifizierungsprofil hinzu.

e. Bestätigen Sie das Formular.

Sie können den REST-API-Aufruf mit dem x-sn-apikey (Token) senden, der von Now Platform während der API-Schlüsselerstellung innerhalb des Header- oder Abfrageparameters basierend auf der Konfiguration für die Authentifizierung generiert wurde.

> **Warnung:**
> Verwenden Sie die **POST** -Anforderung, wenn Sie vertrauliche Informationen an den Server senden.

Konfigurieren Sie die tokenbasierte HMAC-Authentifizierung

Konfigurieren Sie HMAC so, dass die Authentifizierung für REST-API-Endpunkte unterstützt wird.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: API-Schlüssel und HMAC-Authentifizierung (com.glide.tokenbased_auth)

Prozedur

1. Erstellen Sie eine HMAC-Konfiguration.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **HMAC-Konfiguration**.

b. Wählen Sie **Neu**.

> **Hinweis:**
> Sie können auch die **standardmäßige HMAC SHA256 Base64-Codierung** verwenden, die bei der Installation des Plugins erstellt wird.

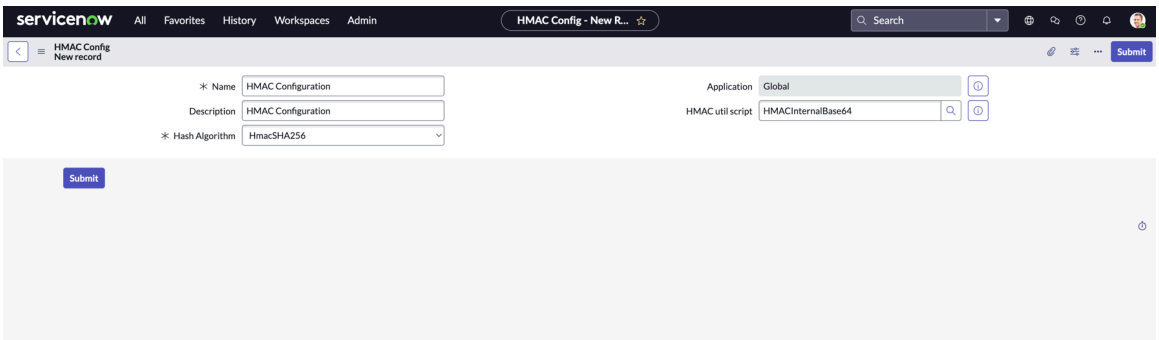
c. Füllen Sie im Formular die folgenden Felder aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HMAC-Konfiguration

Feld	Beschreibung
Name	Name für die HMAC-Konfiguration.
Anwendung	Umfang der Konfiguration.
Beschreibung	Detaillierte Beschreibung der Konfiguration.
Hash-Algorithmus	Wählen Sie den Hash-Algorithmus aus. Verfügbare Optionen: ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
HMAC-Hilfsskript	Hilfsskript für HMAC.



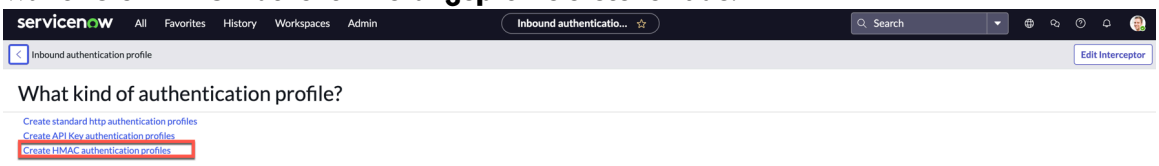
d. Senden Sie den Datensatz ab.

2. Erstellen Sie ein eingehendes Authentifizierungsprofil.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**.

b. Wählen Sie **Neu**.
Die Meldung Welche Art von Authentifizierungsprofil?wird angezeigt.

c. Wählen **Sie HMAC-Authentifizierungsprofile erstellen aus**.



d. Füllen Sie die Felder des Formulars aus.

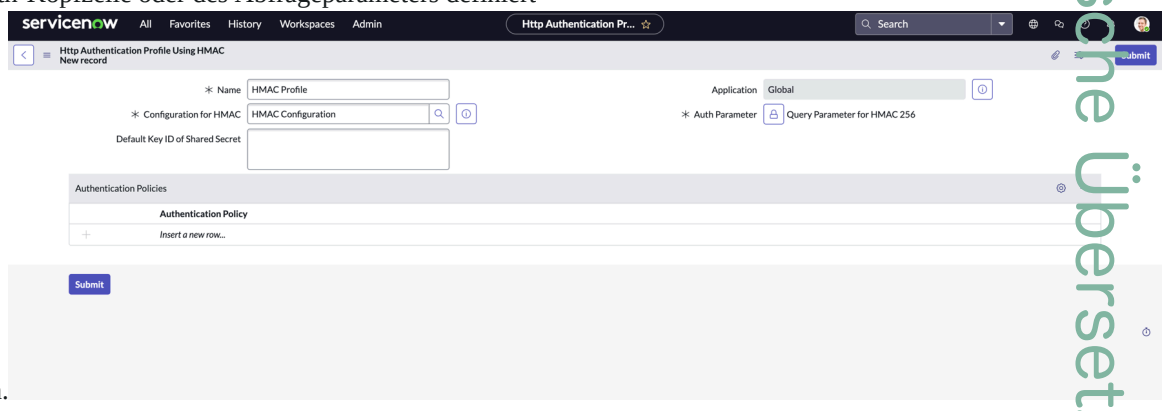
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HMAC-Authentifizierungsprofile

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Konfiguration für HMAC	Wählen Sie die erstellte HMAC-Konfiguration aus.
Auth-Parameter	Wählen Sie den Auth-Parameter für die Authentifizierungsanforderung aus. Sie können die Standardoptionen auswählen oder einen neuen Authentifizierungsparameter erstellen: ▪ x-sn-hmac-signature-256: Auth-Header ▪ x-sn-hmac-signature-256: Abfrageparameter-Header
Standardschlüssel-ID des gemeinsamen Geheimnisses	Die Token-Informationen, die in diesem Feld für die Verwendung von HMAC aktualisiert werden können.

Hinweis:
Die ausgewählte Option muss im REST-Aufruf als Teil der Auth-Kopfzeile oder des Abfrageparameters definiert werden.



e. Bestätigen Sie das Formular.

3. Erstellen Sie einen HMAC-Geheimschlüssel.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-HMAC-Geheimnis**.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die folgenden Felder aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

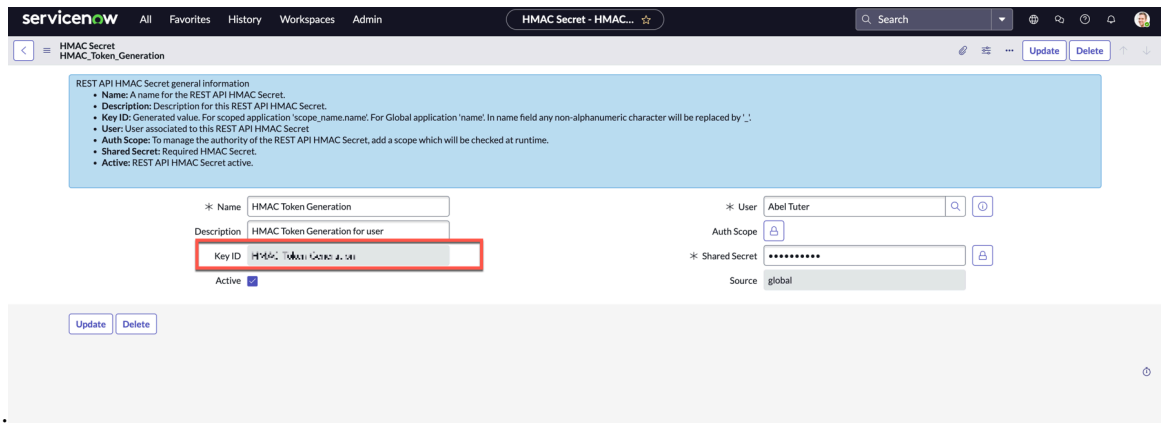
REST-API-HMAC-Geheimnis

Feld	Beschreibung
Name	Name zur Identifizierung des REST-API-HMAC-Geheimnisses.
Beschreibung	Beschreibung für den REST-API-HMAC-Geheimschlüssel.
Aktiv	Status des REST-API-HMAC-Geheimnisses.
Benutzer	Benutzer, der dem REST-API-HMAC-Geheimnis zugeordnet ist. Verwenden Sie das Suchsymbol, um den Benutzer auszuwählen.
Schlüssel-ID	Schlüssel-ID, die als Teil des REST-Aufrufs gesendet werden muss. Schlüssel-ID wird nach dem Absenden des Formulars generiert.
Gemeinsames Geheimnis	Gemeinsame geheime Schlüssel des Benutzers. Zum Beispiel das Passwort.
Quelle	Quelle des Datensatzes.

d. Bestätigen Sie das Formular.

e. Öffnen Sie den erstellten Datensatz.

Suchen Sie die Schlüssel-ID, die von Now Platform für den Benutzer generiert wurde



Hinweis:
Sie können die Schlüssel-ID hinzufügen, die während der Schlüssel-ID im für HMAC erstellten Authentifizierungsprofil generiert wurde, wenn Sie den Parameter Auth oder Query für den API-Aufruf nicht angeben möchten.

4. Erstellen Sie eine REST-API-Zugriffsrichtlinie.

a. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

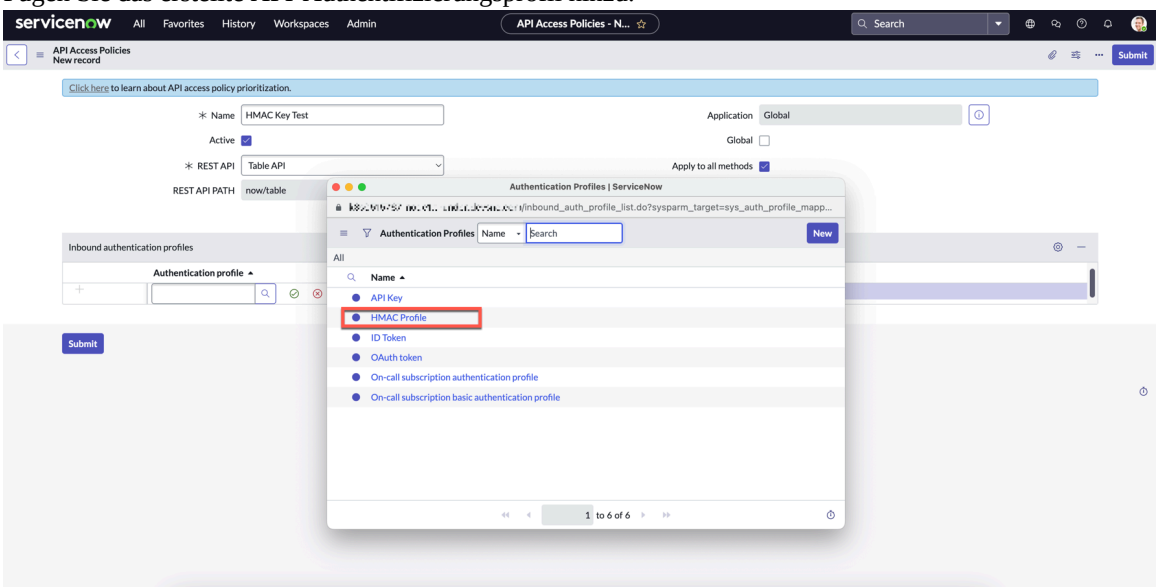
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Zugriffsrichtlinien

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API**.
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **now/attachment**.
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1**. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST-API erstellen möchten, müssen Sie für jede Version eine eigene Richtlinie erstellen.
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **/now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen für die API anzuwenden. **Hinweis:** Tokenbasierte Authentifizierung ist in der globalen REST-API-Richtlinie nicht zulässig.
Auf alle Methoden anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Fügen Sie das erstellte API-Authentifizierungsprofil hinzu.



e. Bestätigen Sie das Formular.
Sie können den REST-API-Aufruf senden:

- Mit der x-sn-hmac-signature-256, die von ServiceNow® während der API-Schlüsselerstellung im Header- oder Abfrageparameter basierend auf der Konfiguration für die Authentifizierung generiert wurde.
- Mit Vorab-Anforderungsskript, bei dem das gemeinsame Geheimnis als Teil der Anforderung angegeben ist.

> **⚠ Warnung:**
> Verwenden Sie die **POST** -Anforderung, wenn Sie vertrauliche Informationen an den Server senden.

API-Zugriffsrichtlinie

Die API-Zugriffsrichtlinie definiert die Berechtigungen und die Dauer des Zugriffs auf eine API.

Mit der API-Zugriffsrichtlinie können Sie den Zugriff auf eingehende ServiceNow® APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie einschränken.

Im Folgenden finden Sie die Unterstützung der dreistufigen Authentifizierungsrichtlinie für nicht interaktive Sitzungen:

- **REST-API**: Der Administrator kann eine globale API-Authentifizierungsrichtlinie oder eine API-spezifische Authentifizierungsrichtlinie definieren.
- **SOAP-API**: Der Administrator kann eine globale API-Authentifizierungsrichtlinie oder eine API-spezifische Authentifizierungsrichtlinie definieren.
- **System-/Exportprozessor**: Der Administrator kann fünf Basissystem-Authentifizierungsprofile definieren, die verwendet werden können, um das Authentifizierungsprofil auf die API-Authentifizierungsrichtlinie oder die prozessorspezifische Authentifizierungsrichtlinie von Prozessoren anzuwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie eine globale Authentifizierungsrichtlinie hinzufügen, gilt die Richtlinie für alle REST APIs, SOAP APIs oder System-/Exportprozessoren.

Im Folgenden sind die Plugins aufgeführt, die für API-Richtlinien und den Authentifizierungsbereich automatisch installiert werden:

- com.glide.rest.policy
- com.glide.soap.policy
- com.glide.prozessor.policy
- com.glide.rest.auth.scope

Sie können die standardmäßige globale Sperrrichtlinie konfigurieren oder eine benutzerdefinierte API-Zugriffsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Und wenden Filterkriterien an, die Filterbedingungen oder Abfragen enthalten, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden.

Die folgenden API-Zugriffsrichtlinien werden in ServiceNow®unterstützt:

- REST API-Zugriffsrichtlinien
- SOAP-API-Zugriffsrichtlinien

Weitere Informationen zu Richtlinien im Zusammenhang mit Exportprozessoren finden Sie unter Zugriffsrichtlinie für System-/Exportprozessoren.

REST API-Zugriffsrichtlinien

Mit REST-API-Zugriffsrichtlinien können Sie den Zugriff auf eingehende REST-APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie einschränken.

Eine REST-API, auch bekannt als RESTful-API, ist eine Art von Anwendungsprogrammierschnittstelle (API), die den Richtlinien des REST-Architekturstils entspricht. REST APIs bieten ein hohes Maß an Flexibilität und sind daher im Web weit verbreitet.

Filterkriterien enthalten Filterbedingungen oder Abfragen, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden.

Sie können die standardmäßige globale Sperrrichtlinie konfigurieren oder eine benutzerdefinierte API-Zugriffsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Sie können beispielsweise eine benutzerdefinierte API-Zugriffsrichtlinie erstellen, die nur den Authentifizierungstyp OAuth 2.0 aus einem bestimmten Bereich von IP-Adressen zulässt. Authentifizierungsanforderungen anderer Authentifizierungstypen und Zugriffsanforderungen von anderen IP-Adressen als den angegebenen IP-Adressen werden abgelehnt.

Aktivieren Sie die REST API-Zugriffsrichtlinie

Sie können das Plugin „ REST API Access Policy“ (com.glide.rest.policy) aktivieren, wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und installiert zugehörige ServiceNow® Store-Anwendungen und Plugins, sofern sie nicht bereits installiert sind.

Vorbereitungen
Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit der REST-API-Zugriffsrichtlinieinstalliert:

- Plugins: com.gilde.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- Tabellen: sys_api_access_policy, sys_auth_profile_mapping, auth_policy_mapping, inbound_auth_profile, std_http_auth.

Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „ REST API Access Policy“ (com.glide.rest.policy).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Erstellen Sie ein Authentifizierungsprofil

Erstellen Sie ein Authentifizierungsprofil, und fügen Sie dem Profil eine oder mehrere Authentifizierungsrichtlinien hinzu. Sie können auch die standardmäßig verfügbaren Authentifizierungsprofile **ID-Token** und **OAuth-Token** konfigurieren.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis:
Sie können Authentifizierungsrichtlinien, IP-Bereiche, rollenbasierte, benutzerbasierte usw. mit gegenseitiger Authentifizierung und benutzerdefinierter Authentifizierung anwenden.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**.
2. Wählen Sie **Neu**.
   Das System zeigt die Nachricht an. Welche Art von Authentifizierungsprofil?
3. Wählen **Sie Standard-HTTP-Authentifizierungsprofile erstellen aus**.
4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standard Authentication Profile“ (Standardauthentifizierungsprofil)

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Beschreibung	Beschreibung der Authentifizierungsrichtlinie.
Aktiv	Option zum Aktivieren der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Typ	Typ der verfügbaren Authentifizierung. Sie können **Basisauthentifizierung**, **ID-Token**, **Zertifikatbasierte Authentifizierung**oder **OAuth**auswählen.
OAuth-Entität	OAuth-Entitätsprofil. Dieses Feld wird nur angezeigt, wenn **ID-Token** oder **OAuth** unter **Typ**ausgewählt wird.

5. Doppelklicken Sie auf **Neue Zeile einfügen**.
6. Wählen Sie eine Authentifizierungsrichtlinie aus der Liste aus und klicken Sie auf das Speichern-Symbol .

Hinweis:
Wählen Sie keine Zugriffsrichtlinie zulassen oder Zugriffsverweigerungsrichtlinie aus. Diese Richtlinien sind nur für Benutzeranmeldungen gedacht.

Sie können eine oder mehrere Authentifizierungsrichtlinien für ein Authentifizierungsprofil hinzufügen.

Hinweis:

Header authentifizieren [WWW-Authenticate].

Wenn das Authentifizierungsprofil geändert wird, gibt die Autorisierungskopfzeile einen Wert zurück, der für die zu diesem Zeitpunkt vorgenommenen Änderungen spezifisch ist. Um alle im Header „WWW-Authenticate“ zurückgegebenen Authentifizierungsschemas abzurufen, müssen Sie `glide.security.response.authenticate.header.auth_profile.first_scheme_only` auf **false**aktivieren. Die Antwort wird mit mehreren Headern zurückgegeben. Beispiel:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Erstellen Sie eine REST-API-Zugriffsrichtlinie

Erstellen Sie eine API-Zugriffsrichtlinie, und ordnen Sie ein Authentifizierungsprofil zu, um den Authentifizierungstyp für eine REST-API einzuschränken. Sie können beispielsweise eine API-Zugriffsrichtlinie erstellen, die nur die ID-Token-Authentifizierung für eine REST-API zulässt.

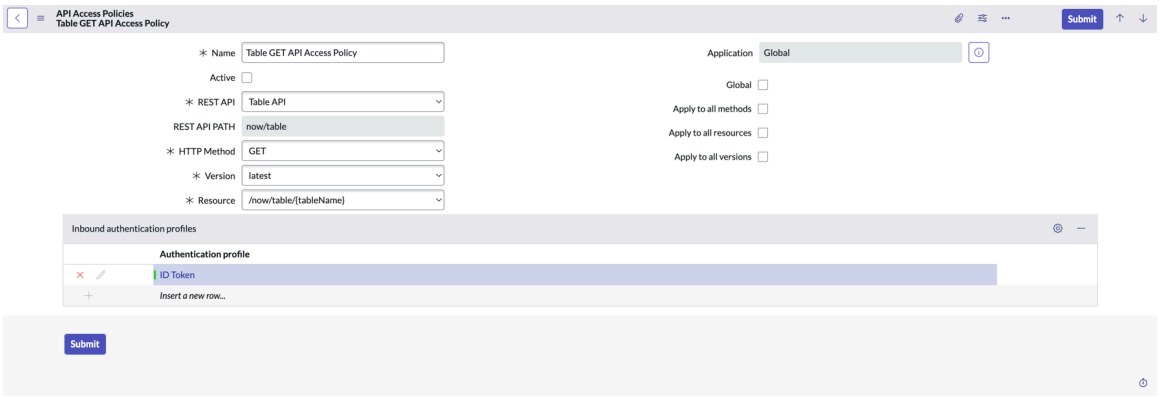
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Erforderliche Rolle: admin
- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Authentifizierungsprofile erstellen.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.



API-Zugriffsrichtlinien

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API**.
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **now/attachment**.
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1**. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST-API erstellen möchten, müssen Sie für jede Version eine eigene Richtlinie erstellen.
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	API automatisch ausgefüllt. Beispiel: **/now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Methoden anwenden	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.

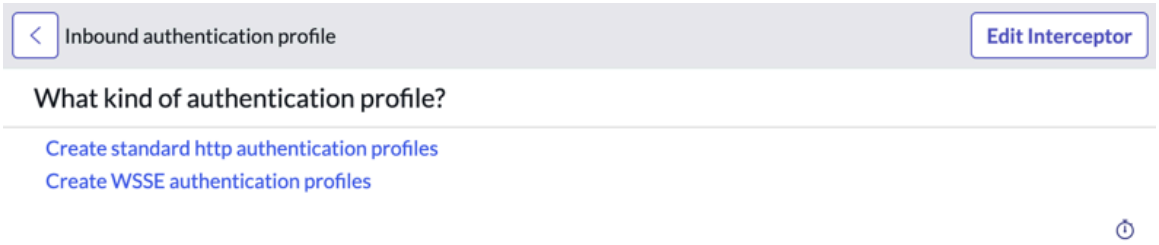
Hinweis:
Weitere Informationen zur Priorisierung von API-Zugriffsrichtlinien finden Sie unter Priorisierung der API-Zugriffsrichtlinie.

4. Doppelklicken Sie auf **Neue Zeile einfügen**.
5. Wählen Sie ein eingehendes Authentifizierungsprofil aus der Liste aus, und klicken Sie auf das Speichern-Symbol .
   Sie können beispielsweise Basisauthentifizierung, **ID-Token**, **zertifikatbasierte**Authentifizierung, **OAuth**oder **WSSE-Authentifizierung hinzufügen**.

   a. Um ein oder mehrere eingehende Authentifizierungsprofile hinzuzufügen, klicken Sie auf **Neu**, um ein neues Profil zu erstellen.

   b. **Welche Art von Authentifizierungsprofilen auswählen?**.
   - **Standardmäßiges http-Authentifizierungsprofil erstellen**
   - **WSSE-Authentifizierungsprofile erstellen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Speichern Sie den Datensatz nach dem Erstellen des Authentifizierungsprofils.

6. Klicken Sie auf **Absenden**, um die REST-API-Zugriffsrichtlinie zu übermitteln.

Priorisierung der API-Zugriffsrichtlinie

Erfahren Sie mehr über die Logik der Richtlinienpriorisierung, wenn für Ihre ServiceNow® -Instanz mehrere API-Zugriffsrichtlinien konfiguriert sind.

API-Zugriffsrichtlinien werden basierend auf dem Typ der REST-API-Richtlinie priorisiert, die für Ihre ServiceNow® -Instanz festgelegt ist.

Der Ansatz besteht darin, unterschiedliche Gewichtungen für jeden Teil der API zu definieren, z. B. Methode, Ressource und Version.

Die API-Richtlinie wird zuerst für nicht global und dann global priorisiert. Mit anderen Worten, eine nicht globale Zugriffsrichtlinie überschreibt immer eine globale API-Zugriffsrichtlinie.

Die Priorisierungslogik lautet wie folgt:

Priorisierung

Felder	Priorität	Priorisierungslogik
Methode, Ressource und Version	1	Wenn die 3 Felder mit der Richtlinie übereinstimmen, hat diese Richtlinie die 1. Priorität.
Method+-Ressource	2	Wenn die beiden Felder mit der Richtlinie übereinstimmen, hat diese Richtlinie die erste Priorität.
Ressource + Version	3	Wenn die 2 Felder zusammen mit dem Feld Auf **alle Methoden anwenden** mit der Richtlinie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Priorisierung (Fortsetzung)

Felder	Priorität	Priorisierungslogik
		übereinstimmen, hat diese Richtlinie die 3. Priorität.
Ressource	4	Wenn das Feld zusammen mit dem Feld Auf **alle Methoden anwenden** mit der Richtlinie übereinstimmt, hat diese Richtlinie die 4. Priorität.
Methode + Version	5	Wenn die 2 Felder zusammen mit dem Feld Auf **alle Ressourcen anwenden** mit der Richtlinie übereinstimmen, hat diese Richtlinie die 5. Priorität.
Methode	6	Wenn das Feld zusammen mit dem Feld Auf **alle Ressourcen anwenden** mit der Richtlinie übereinstimmt, hat diese Richtlinie die 5. Priorität.
Version	7	Wenn das Feld zusammen mit den Feldern Auf **alle Methodenanwenden und Auf alle Versionen anwenden** mit der Richtlinie übereinstimmt, hat diese Richtlinie die 7. Priorität.
Global und Anwenden auf alle Methoden	8	Wenn die Felder **Global** auf „ wahr “ und **„Auf alle Methoden anwenden“ auf** „ falsch “ gesetzt sind, hat diese Richtlinie die 8. Priorität.
Global und Anwenden auf alle Methoden	9	Wenn die Felder **Global** auf „ wahr “ und **Auf alle Methoden anwenden auf** „ wahr “ gesetzt sind, hat diese Richtlinie die 9. Priorität.

Filterkriterien für APIs

Filterkriterien enthalten Filterbedingungen oder Abfragen, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden. Richtlinieneingaben werden verwendet, um ein oder mehrere Filterkriterien zu gruppieren und die Richtlinienbedingungen einer Authentifizierungsrichtlinie zu definieren. Zum Beispiel definiert ein IP-Filterkriterium eine IP-Adresse im CIDR-Format (Classless Inter-Domain Routing) oder einen Bereich von IP-Adressen.

Sie können Filterkriterien basierend auf der IP-Adresse, der Rolle und der Benutzergruppe des Benutzers erstellen.

Hinweis:
Sie verwenden auch die Filterkriterien, die aus dem Modul **„Adaptive Authentifizierung** “ erstellt wurden. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Filterkriterien für APIs mit demselben Verfahren wie Filterkriterien für die adaptive Authentifizierung erstellen. Nähere Informationen hierzu finden Sie unter Filterkriterien.

Zugehörige Informationen

Erstellen Sie IP-Filterkriterien

Erstellen Sie Rollenfilterkriterien

Erstellen Sie Gruppenfilterkriterien

API-Authentifizierungsrichtlinien

Authentifizierungsrichtlinien werten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen aus und erlauben oder verweigern den Zugriff abhängig von den Übereinstimmungskriterien.

Sie können die integrierte globale Sperrrichtlinie verwenden oder eine Authentifizierungsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Die globale Blockierungsrichtlinie lehnt die Authentifizierungsanforderungen von Benutzern und APIs basierend auf den angegebenen Filterkriterien ab.

Hinweis:
Verwenden oder ändern Sie keine Richtlinien für „Zugriff zulassen“ und „Zugriff verweigern“. Diese Richtlinien sind nur für Benutzeranmeldungen gedacht.

Erstellen Sie eine API-Authentifizierungsrichtlinie

Mit Authentifizierungsrichtlinien können Sie Zugriffsbeschränkungen für die APIs basierend auf den angegebenen Filterkriterien erzwingen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Authentifizierungsrichtlinie**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

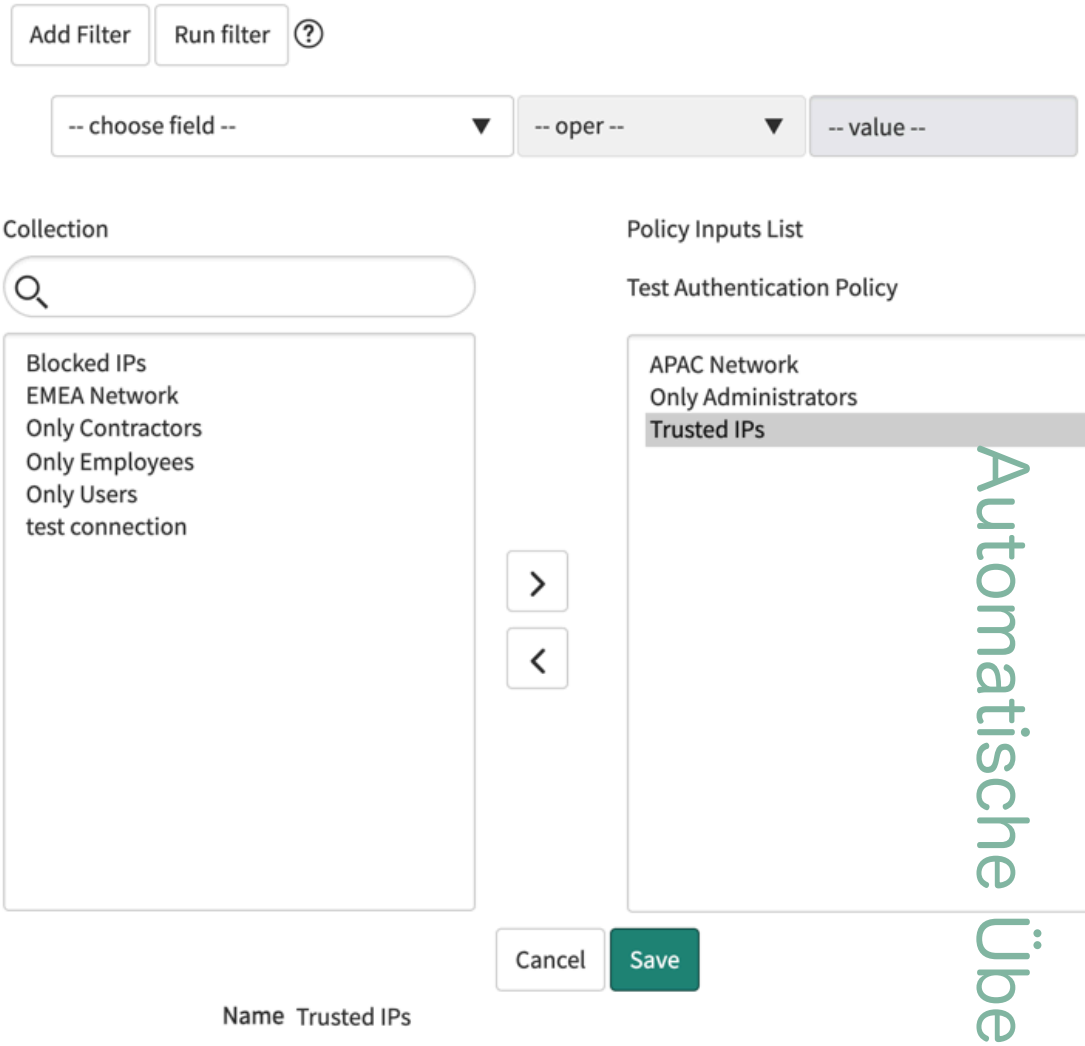
Richtlinienformular

Feld	Beschreibung
Name	Name zur Identifizierung der Richtlinie.
Beschreibung	Kurzbeschreibung der Richtlinie.
Anwendung	Umfang der Anwendung.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Wählen Sie auf der Registerkarte Richtlinieneingaben die Option **Bearbeiten** aus, um die vorhandenen Filterkriterien hinzuzufügen.
   Sie können auch eine neue Richtlinieneingabe erstellen. Weitere Informationen finden Sie unter Richtlinieneingaben erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verschieben Sie ein oder mehrere Filterkriterien aus der Liste „Sammlungen“ in die Liste „Richtlinieneingaben“.



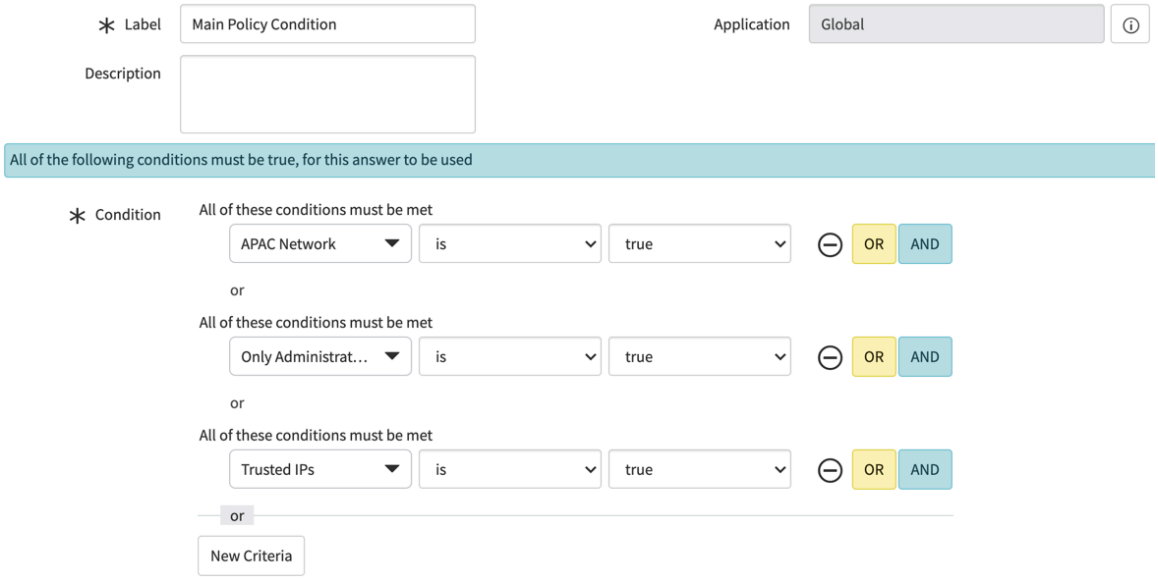
7. Wählen Sie **Speichern**.
8. Wählen Sie auf der Registerkarte Richtlinienbedingungen die Option **Neu**aus.
9. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name der Richtlinienbedingung.
Beschreibung	Kurzbeschreibung der Richtlinienbedingung.
Anwendung	Umfang der Anwendung.
Bedingung	Eine oder mehrere Bedingungen, die mit dem **ODER** -Filter kombiniert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Wählen Sie **Absenden**.

Konfigurieren Sie die globale Blockierungsrichtlinie für APIs

Die globale Blockierungsrichtlinie verweigert die Authentifizierungsanforderungen von Benutzern und APIs basierend auf den angegebenen Richtlinienbedingungen. Diese Richtlinie kann als Alternative zur IP-Adresszugriffssteuerung verwendet werden.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Globale Sperrrichtlinie**.
2. Klicken Sie auf der Registerkarte **Richtlinieneingaben** auf **Bearbeiten**.
3. Wählen Sie ein oder mehrere Filterkriterien aus der Liste **Sammlung** aus, und verschieben Sie sie in die Liste **Globale Sperrrichtlinie**.
   Sie können auch zusätzliche Filter hinzufügen.
4. Klicken Sie auf der Registerkarte **Richtlinienbedingungen** auf **Neu**.
5. Füllen Sie im Formular die folgenden Felder aus:

Bedingungsformular

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination mehrerer Richtlinieneingaben (Filterkriterien), die zum Auswerten von Authentifizierungsanforderungen verwendet wird. Sie können beispielsweise Bedingungen erstellen, die nur Auftragnehmer aus einer Liste vertrauenswürdiger IP-Adressen zulassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-API-Authentifizierungsbereich

Unterstützung des Authentifizierungsbereichs für REST APIs.

Vor Release Washington DC ist jedes Zugriffstoken oder OIDC-Token mit dem Anwendungsbereich useraccount verknüpft, der vollständigen Zugriff auf die REST APIs des Benutzers hat. Ab Release Washington DC werden die OAuth-Token-Umfänge eingeführt, um Zugriff nur auf die bestimmten REST-APIs zu ermöglichen.

Wenn eine OAuth-Entität mit einem Authentifizierungsbereich verknüpft ist, wird das von dieser OAuth-Entität ausgegebene oder verwaltete Token nur für den Zugriff auf die REST APIs verwendet (eine OAuth-Entität kann mit mehreren Authentifizierungsbereichen verknüpft sein). Für die neue OAuth-Entität ist der Standard-Auth-Bereich leer. Sie müssen den Auth-Bereich manuell mit der OAuth-Entität verknüpfen.

Hinweis:

- Nachdem der REST-API-Authentifizierungsbereich aktiviert und dem Authentifizierungsbereich für die REST-API hinzugefügt wurde, können alle vorhandenen OAuth-Token nicht mehr auf diese API zugreifen, es sei denn, der Administrator fügt diesen Authentifizierungsbereich der entsprechenden OAuth-Entität hinzu
- Der Administrator ist dafür verantwortlich, sicherzustellen, dass die oauth_entity über den richtigen Authentifizierungsbereich verfügt, nachdem der Authentifizierungsbereich mit der REST-API verknüpft wurde.
- Von ServiceNow ausgegebene OAuth-Zugriffstoken unterstützen den Authentifizierungsbereich.
- OIDC-Token, die nicht von [] ausgegeben werden, werden von ServiceNowServiceNow validiert.
- Das OIDC-Token hat seinen Bereich vom IdP, wenn Sie ein ID-Token benötigen. Hier gilt der Authentifizierungsbereich für ServiceNow anstelle der Drittpartei (IdP).

Konfigurationen für den REST-API-Bereich

Führen Sie die folgenden Aufgaben aus, um den REST-API-Bereich zu konfigurieren:

- Erstellen Sie einen Authentifizierungsbereich
- Verknüpfen Sie den Authentifizierungsbereich mit der REST-API
- Verknüpfen Sie den Authentifizierungsbereich mit der OAuth-Entität
- Führen Sie den OAuth-Flow aus, um das OAuth-Zugriffstoken zu erhalten
- Verwenden Sie das OAuth-Zugriffstoken, um den API-Aufruf durchzuführen

Aktivieren Sie den REST-API-Auth-Bereich

Sie können das Plugin „REST API Auth Scope“ (com.glide.rest.auth.scope) aktivieren, um die OAuth-Entität mit Authentifizierungsbereichen zu verknüpfen.

Vorbereitungen
Installieren Sie die folgenden Plugins:

- OAuth 2.0
- REST-API-Provider

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Authentifizierungsbereich
- REST-API-Bereich

Hinweis:
Das Plugin *REST API Scope* wird als Teil des Release Tokyo] hinzugefügt.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „REST-API-Authentifizierungsbereich“ (*com.glide.rest.auth.scope*).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Eigenschaften und Tabellen des REST-API-Authentifizierungsbereichs

Das Plugin „REST API Auth Scope“ (com.glide.rest.auth.scope) enthält die folgenden Systemeigenschaften, Tabellen und Skripts.

REST-API-Authentifizierungsbereichseigenschaften

REST API-Auth-Bereich fügt die folgenden Systemeigenschaften hinzu.

Eigenschaften

Name	Beschreibung
com.glide.rest.api.auth.scope.check.enable	Diese Eigenschaft wird verwendet, um die Prüfung des Authentifizierungsbereichs auf Plattformebene zu deaktivieren. Bei „false“ wird während der Laufzeit die Prüfung des Authentifizierungsbereichs übersprungen, unabhängig davon, ob er mit der RETS-API verknüpft ist oder nicht. Standardmäßig ist diese Eigenschaft auf „true“ festgelegt. Diese Eigenschaften werden verwendet, wenn Sie das Verhalten des vorherigen Release wiederherstellen möchten.
com.glide.oauth.token.scope.useraccount	Diese Eigenschaft wird nur verwendet, wenn der Authentifizierungsbereich *useraccount* gelöscht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften (Fortsetzung)

Name	Beschreibung
	und vom Endbenutzer manuell wieder hinzugefügt wird. In diesem Fall wird die Sys-ID für *useraccount* geändert. Diese Eigenschaft muss auf die neue sys_id aktualisiert werden. Während der Laufzeit wird die Sys-ID des Authentifizierungsbereichs anstelle des Namens des Authentifizierungsbereichs verwendet.

REST-API-Authentifizierungsbereichstabellen

REST-API-Authentifizierungsbereich in den folgenden Tabellen.

Tabellen

Name	Beschreibung
Authentifizierungsbereich (sys_auth_scope)	Diese Tabelle definiert den Authentifizierungsbereich, der mit der REST-API und der OAuth-Entität verknüpft werden kann. Der Name des Authentifizierungsbereichs muss eindeutig sein und ist global.
REST-API-Authentifizierungsbereich (sys_api_access_scope)	Diese Tabelle verknüpft die REST-API mit dem Authentifizierungsbereich.

Konfigurieren Sie den REST-API-Authentifizierungsbereich

Verknüpfen Sie die OAuth-Entität mit einem Authentifizierungsbereich, um das Token für den Zugriff auf die REST APIs zu verwalten, die mit dem Authentifizierungsbereich verknüpft sind.

Vorbereitungen
Installieren Sie die folgenden Plugins:

- OAuth 2.0
- REST-API-Provider
- Authentifizierungsbereich
- REST-API-Authentifizierungsbereich

Hinweis:
Das Plugin *REST API Auth Scope* wird als Teil des Release Tokyo] hinzugefügt.

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **API-Authentifizierungsbereiche** > **REST-API-Authentifizierungsbereich**. Die Seite „REST API-Auth-Bereiche“ wird angezeigt.
2. Um einen neuen REST-API-Authentifizierungsbereich zu konfigurieren, klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

REST-API-Authentifizierungsbereich

Name	Ein eindeutiger Name, der den Auth-Bereich der REST-API identifiziert.
Aktiv	Aktivieren Sie die Checkbox, um die Konfiguration zu aktivieren.
Anwendung	Schreibgeschützter Anwendungsbereich.
REST-API	Die REST-API, auf die der Authentifizierungsbereich angewendet wird. Zum Beispiel die Tabellen-API.
Authentifizierungsbereich	Wählen Sie den Authentifizierungsbereich über das Suchsymbol aus.
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: now/table.
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Wählen Sie die Methode aus der Dropdown-Liste aus. Sie können das Feld **Authentifizierungsbereich auf alle HTTP-Methoden in dieser API anwenden** im Formular manuell deaktivieren, um die Methode auszuwählen.
REST API-Version	Version der API. Beispiel: v1. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Sie können das Feld **Authentifizierungsbereich auf alle Versionen in dieser API anwenden** im Formular manuell deaktivieren, um die Version auszuwählen.
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: /now/table. Sie können das Feld **Authentifizierungsbereich auf alle Ressourcen in dieser API anwenden** im Formular manuell deaktivieren, um die Ressourcen auszuwählen.

Automatische Übersetzung

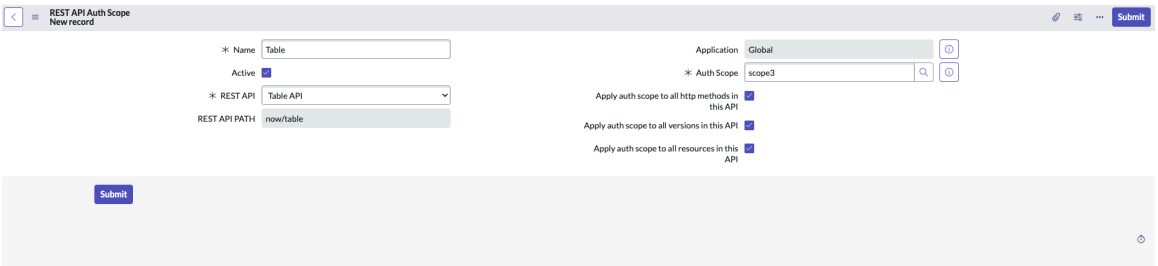
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierungsbereich auf alle HTTP-Methoden in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle HTTP-Methoden in der API angewendet.
Authentifizierungsbereich auf alle Versionen in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle Versionen in der API angewendet.
Authentifizierungsbereich auf alle Ressourcen in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle Ressourcen in der API angewendet

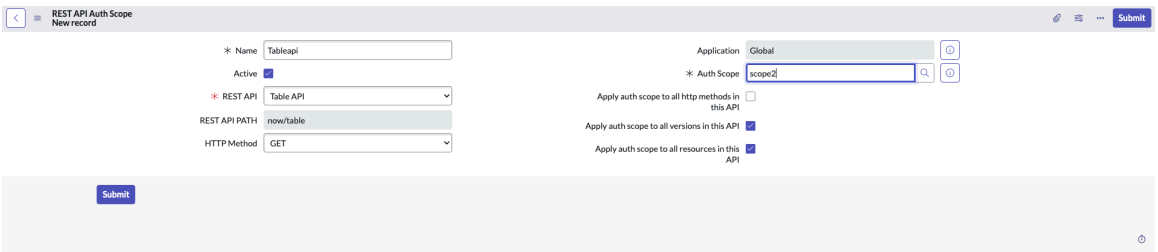
4. Klicken Sie auf **Absenden**.
   Basierend auf der ausgewählten REST-API und dem ausgewählten Auth-Bereich ruft die APIs Informationen ab, die für den Bereich spezifisch sind.

Example: Erwägen Sie die Erstellung von drei REST-API-Auth-Bereichen für die Tabellen-API

Der erste Authentifizierungsbereich wird der **Tabellen-API** zugeordnet, wobei alle HTTP-Methoden, -Versionen und -Ressourcen aktiviert sind.

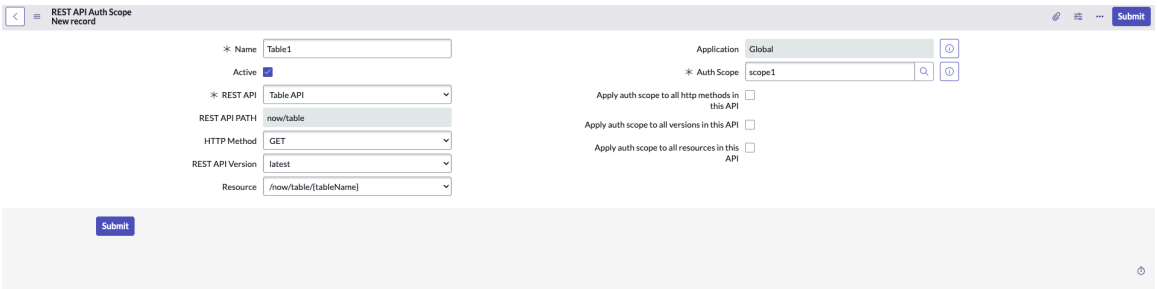


Der zweite Authentifizierungsbereich wird der **Tabellen-API** zugeordnet, wobei alle Versionen und Ressourcen aktiviert sind. Sie wählen jedoch die HTTP-Methode, in diesem Beispiel die **GET-** Methode.



Der dritte Authentifizierungsbereich wird der **Tabellen-API** zugeordnet, ohne dass die HTTP-Methoden, -Versionen und -Ressourcen aktiviert sind. Sie wählen die HTTP-Methode, die Version und die Ressource jedoch manuell aus. In diesem Beispiel ist die HTTP-Methode **GET**, die REST-API-Version ist **aktuell**und die Ressource ist `/now/table/{tableName}`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn alle diese Authentifizierungsbereiche erstellt werden, können Sie die **GET** -Methode mit allen drei Bereichen verwenden, aber für die Methoden **POST**, **PUT**, **DELETE**oder **PATCH** kann nur **scope3** verwendet werden.

Problembehandlung für den REST-API-Bereich

Aktionen zur Problembehandlung können helfen, häufige Probleme beim Einrichten oder Ausführen des REST-API-Bereichs zu beheben.

Problembehandlung

Vorfall	Aktion
Die REST-API ist mit dem Authentifizierungsbereich verknüpft. Zur Laufzeit findet jedoch keine Prüfung des Authentifizierungsbereichs statt, auch wenn die Bearer-Token-Authentifizierung verwendet wird.	• Stellen Sie sicher, dass der Datensatz sys_api_access_policy aktiv ist. Laufzeit ignoriert inaktive Datensätze. • Überprüfen Sie, ob die Eigenschaft `com.glide.rest.api.auth.scope.check.enable` auf „false“ festgelegt ist. • Überprüfen Sie, ob das OAuth-Token über den Authentifizierungsbereich useraccount verfügt.
Die REST-API ist mit [] verknüpft, das Zugriffstoken mit `auth_scope2auth_scope1`kann jedoch auch darauf zugreifen.	• Überprüfen Sie, ob dieser Datensatz aktiv ist. • Suchen Sie nach diesem REST und anderen Datensätzen, die dieselben APIs, aber unterschiedliche Methoden, Versionen oder Ressourcen aufweisen.
Die REST-API ist mit dem Authentifizierungsbereich verknüpft, zur Laufzeit findet jedoch keine Prüfung des Authentifizierungsbereichs für `basicAuth` und `mutualAuth`statt.	Dies wird erwartet, da der REST-API-Authentifizierungsbereich nur für das OAuth-Zugriffstoken oder OIDC-Token gilt. BasicAuth, Sitzungscookie und zertifikatbasierte Authentifizierung werden nicht angewendet.
Der REST-API-Aufruf gibt bei Verwendung des OAuth-Zugriffstokens 403 zurück.	Überprüfen Sie die Fehlermeldung „Erforderlicher API-Zugriffsbereich fehlt“. Wenn gefunden, schlägt die Prüfung des Authentifizierungsbereichs für diese REST-API fehl
Vordefinierter Anwenderaccount wurde gelöscht und kann nicht sicher wiederhergestellt werden.	Exportieren Sie das Benutzerkonto als XML aus der anderen Instanz, und importieren Sie es, oder erstellen Sie ein Benutzerkonto, und ändern Sie die Systemeigenschaft

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung (Fortsetzung)

Vorfall	Aktion
	`glide.oauth.token.scope.useraccount` für den neu erstellten sys_id-Datensatz.

Häufige Fragen

Im Folgenden finden Sie einige der häufig gestellten Fragen bei der Verwendung des Auth-Bereichs der REST-API:

Kann ein OAuth-Token mit mehreren Authentifizierungsbereichen verknüpft werden?

Ja, eine oauth_entity kann mit mehreren Authentifizierungsbereichen verknüpft werden. Jedes von dieser oauth_entity ausgegebene OAuth-Token hat dieselben Authentifizierungsbereiche.

Können verschiedene OAuth-Token mit unterschiedlichen Authentifizierungsbereichen auf dieselbe REST-API zugreifen?

Ja, für dieselbe REST-API kann von verschiedenen Authentifizierungsbereichen darauf zugegriffen werden. Solange ein Authentifizierungsbereich übereinstimmt, gibt der Authentifizierungsbereich die Ergebnisse zurück.

Kann das OAuth-Zugriffstoken mit dem Authentifizierungsbereich „useraccount“ **auf REST APIs zugreifen?**

Ja, der Anwenderaccount hat vollständigen Zugriff auf den Authentifizierungsbereich.

Kann der OAuth-Umfang des OAuth-Zugriffstokens dynamisch geändert werden?

Ja, die bereichsbezogene Authentifizierung ist nicht mit dem Zugriffstoken in der Tabelle oauth_credential hartcodiert. Stattdessen wird der Authentifizierungsbereich zur Laufzeit von der verknüpften oauth_entity abgerufen.

Kann das OAuth-Token nach der Aktualisierung dieselben Authentifizierungsbereiche beibehalten?

Ja, der Authentifizierungsbereich ändert sich nach der Token-Aktualisierung nicht, es sei denn, oauth_admin ändert den mit oauth_entityverknüpften Authentifizierungsbereich.

Der vordefinierte **Datensatz für den Benutzeraccount-Authentifizierungsbereich wird gelöscht. Kann ein neuer Authentifizierungsbereich mit dem Namen** „Benutzeraccount **“ erstellt werden?**

Das Erstellen eines neuen Authentifizierungsbereichs mit demselben Benutzerkonto funktioniert nicht. Zur Laufzeit wird die sys_id anstelle des Namens verwendet, um die Prüfung des Authentifizierungsbereichs durchzuführen. Ändern Sie die Systemeigenschaft `glide.oauth.token.scope.useraccount` in den neu erstellten sys_id -Datensatz.

Wenn der Administrator die mit oauth_entity**verknüpfte bereichsbezogene Authentifizierung ändert, werden dann auch alle vorhandenen OAuth-Zugriffstoken geändert, die von dieser OAuth-Entität ausgegeben werden?**

Ja, der Authentifizierungsbereich ist nicht direkt mit dem OAuth-Zugriffstoken verknüpft, er wird zur Laufzeit von oauth_entity abgerufen.

Können verschiedene OAuth-Zugriffstoken, die von derselben oauth_entity **ausgegeben werden, unterschiedliche Authentifizierungsbereiche haben?**

Nein, jeder Zugriff auf das Token wird von derselben oauth_entity ausgegeben und hat immer dieselben Authentifizierungsbereiche.

Kann ein Benutzer verschiedene Authentifizierungsbereiche für einen bestimmten Endpunkt definieren?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nein, es gibt eine eindeutige Einschränkungsprüfung für einen bestimmten REST-API-Endpunkt. Für denselben REST-API-Endpunkt können jedoch mehrere übereinstimmende Authentifizierungsbereiche vorhanden sein.

Wird die Authentifizierungsbereichsprüfung auch für BasicAuth verwendet?

Nein, die Prüfung des Authentifizierungsbereichs erfolgt nur auf das OAuth-Zugriffstoken und das OIDC-Token. Sie wird nicht für `basicAuth` und `mutualAuth`angewendet.

SOAP-API-Zugriffsrichtlinien

Mit SOAP-API-Zugriffsrichtlinien können Sie den Zugriff auf eingehende SOAP-APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie einschränken.

Mit den SOAP-API-Zugriffsrichtlinien können Sie das eingehende Authentifizierungsprofil und die API-Zugriffsrichtlinien auf eingehende SOAP- und geskriptete SOAP-APIs anwenden.

Sie können ServiceNow API-Zugriffsrichtlinien wie IP-Bereiche und rollenbasierte Einschränkungen nutzen, um eingehende SOAP-API-Aufrufe basierend auf der Authentifizierung zuzulassen oder zu verhindern.

Als Administrator können Sie die folgenden Aktionen ausführen, um die Richtlinien anzuwenden.

- Aktivieren Sie die Plugins SOAP API Access Policy und Authentication Profile. Weitere Informationen finden Sie unter Aktivieren Sie die SOAP-API-Zugriffsrichtlinie.
- Erstellen Sie SOAP-API-Zugriffsrichtlinien, und ordnen Sie diese Richtlinien einem Authentifizierungsprofil zu. Weitere Informationen finden Sie unter Erstellen Sie eine SOAP-API-Zugriffsrichtlinie und Erstellen Sie ein Authentifizierungsprofil.

  Hinweis:
  Die Richtlinien gelten für die SOAP-Tabellen-API oder die geskriptete SOAP-API. Neben dem Standard -HTTP- und WSSE-Authentifizierungsprofil.

- Erstellen Sie Authentifizierungsrichtlinien wie IP-Bereich und rollenbasierte Einschränkungen, und ordnen Sie diese Richtlinie dem Authentifizierungsprofil zu. Weitere Informationen finden Sie unter Erstellen Sie eine API-Authentifizierungsrichtlinie.

Aktivieren Sie die SOAP-API-Zugriffsrichtlinie

Installieren Sie für die SOAP-API-Zugriffsrichtlinie das Plugin „SOAP API Access Policy“ (com.glide.soap.policy).

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das folgende Element wird mit dem SOAP API Access Policy-Plugin installiert: Processor Access Policy (com.glide.processor.policy)

Abhängiges Plugin: Authentifizierungsprofil (com.glide.auth.profile)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „SOAP API Access Policy“ (com.glide.soap.policy).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Erstellen Sie ein Authentifizierungsprofil

Erstellen Sie ein Authentifizierungsprofil, und fügen Sie dem Profil eine oder mehrere Authentifizierungsrichtlinien hinzu. Sie können auch die standardmäßig verfügbaren Authentifizierungsprofile **ID-Token** und **OAuth-Token** konfigurieren.

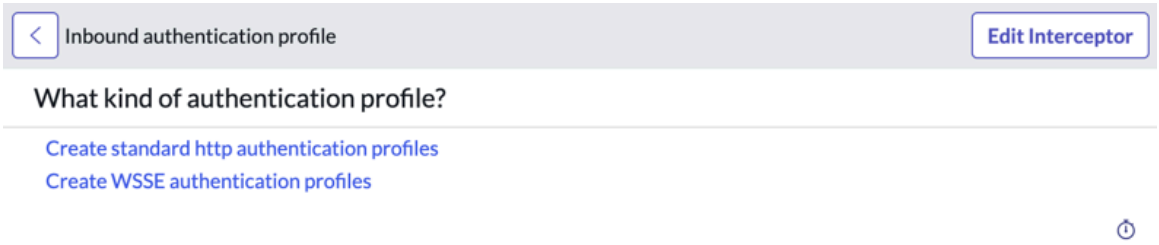
Vorbereitungen
Erforderliche Rolle: admin

Hinweis:
Sie können Authentifizierungsrichtlinien, IP-Bereiche, rollenbasierte, benutzerbasierte usw. mit gegenseitiger Authentifizierung und benutzerdefinierter Authentifizierung anwenden.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**.
2. Wählen Sie **Neu**.
   Das System zeigt die Nachricht an. Welche Art von Authentifizierungsprofil?
3. **Welche Art von Authentifizierungsprofilen auswählen?**.
   - **Standardmäßiges http-Authentifizierungsprofil erstellen**
   - **WSSE-Authentifizierungsprofile erstellen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Felder des Formulars aus.

Formular „Standard Authentication Profile“ (Standardauthentifizierungsprofil)

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Beschreibung	Beschreibung der Authentifizierungsrichtlinie.
Aktiv	Option zum Aktivieren der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Typ	Typ der verfügbaren Authentifizierung. Sie können **Basisauthentifizierung**, **ID-Token**, **Zertifikatbasierte**Authentifizierung, **OAuth**oder **WSSE** (bei WSSE-Authentifizierungsprofil) auswählen.
OAuth-Entität	OAuth-Entitätsprofil. Dieses Feld wird nur angezeigt, wenn **ID-Token** oder **OAuth** unter **Typ**ausgewählt wird.

5. Doppelklicken Sie auf **Neue Zeile einfügen**.
6. Wählen Sie eine Authentifizierungsrichtlinie aus der Liste aus und klicken Sie auf das Speichern-Symbol .

Hinweis:
Wählen Sie nicht **Zugriffsrichtlinie zulassen** oder **Zugriffsverweigerungsrichtlinie**aus. Diese Richtlinien sind nur für Benutzeranmeldungen gedacht.

Sie können eine oder mehrere Authentifizierungsrichtlinien für ein Authentifizierungsprofil hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Authentifizierungsprofil geändert wird, gibt die Autorisierungskopfzeile einen Wert zurück, der für die zu diesem Zeitpunkt vorgenommenen Änderungen spezifisch ist. Um alle im Header „WWW-Authenticate“ zurückgegebenen Authentifizierungsschemas abzurufen, müssen Sie glide.security.response.authenticate.header.auth_profile.first_scheme_only auf **false**aktivieren. Die Antwort wird mit mehreren Kopfzeilen zurückgegeben. Beispiel:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Erstellen Sie eine SOAP-API-Zugriffsrichtlinie

Erstellen Sie eine API-Zugriffsrichtlinie, und ordnen Sie ein Authentifizierungsprofil zu, um den Authentifizierungstyp für eine SOAP-API einzuschränken. Sie können beispielsweise eine API-Zugriffsrichtlinie erstellen, die nur die ID-Token-Authentifizierung für eine SOAP-API zulässt.

Vorbereitungen

- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Authentifizierungsprofile erstellen.
- Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Zugriffsrichtlinien für SOAP-API**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

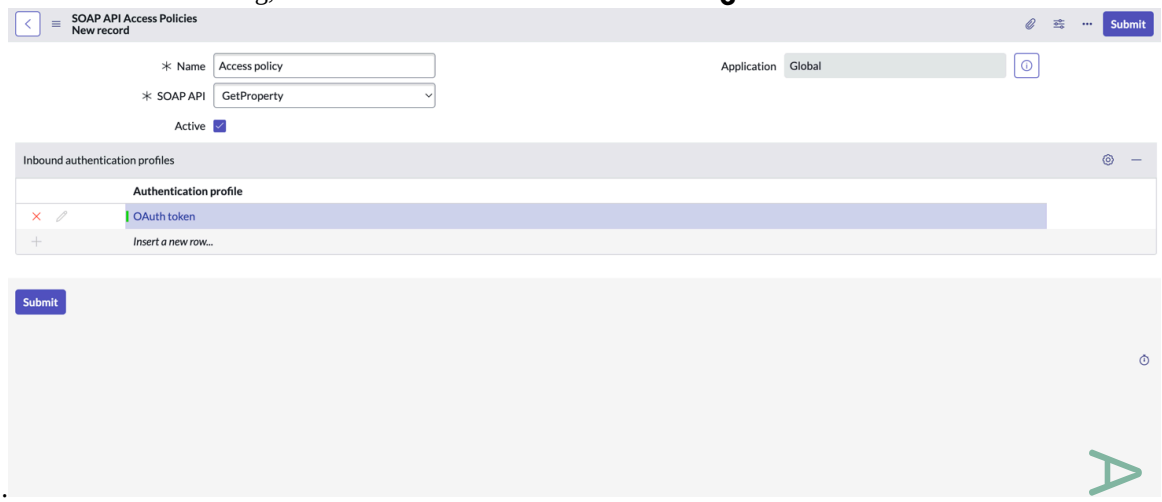
Formular „API-Zugriffsrichtlinien“

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
SOAP-API	SOAP-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **GetProperty-API**.
Anwendung	Umfang der Anwendung.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.

4. Doppelklicken Sie im Abschnitt „Eingehende Authentifizierung“ auf **Neue Zeile einfügen**.
5. Wählen Sie ein eingehendes Authentifizierungsprofil aus der Liste aus, und klicken Sie auf das Speichern-Symbol .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

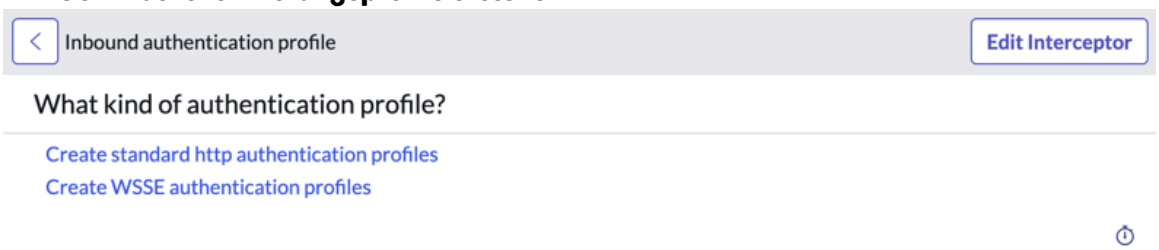
Sie können beispielsweise Basisauthentifizierung, **ID-Token**, **zertifikatbasierte**Authentifizierung, **OAuth**oder **WSSE-Authentifizierung** **hinzufügen**.



a. Um ein oder mehrere eingehende Authentifizierungsprofile hinzuzufügen, klicken Sie auf **Neu**, um ein neues Profil zu erstellen.

b. Welche Art von Authentifizierungsprofilen auswählen?.

- **Standardmäßiges http-Authentifizierungsprofil erstellen**
- **WSSE-Authentifizierungsprofile erstellen**



c. Um ein WSSE-Authentifizierungsprofil zu erstellen, füllen Sie die Felder des Formulars aus.

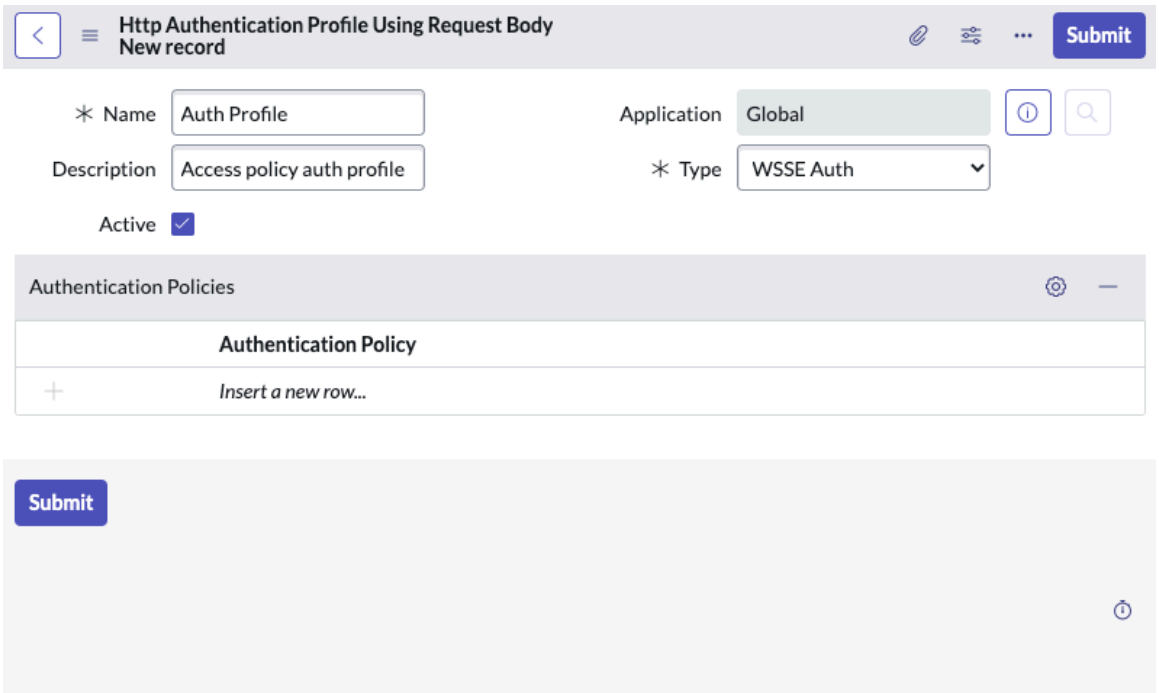
WSSE-Authentifizierungsprofil

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Beschreibung	Beschreibung des Authentifizierungsprofils.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Umfang der Anwendung.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
Typ	WSSE Auth als Authentifizierungsprofil WSSE (Web Security).



d. Speichern Sie den Datensatz nach dem Erstellen des Authentifizierungsprofils.

6. Klicken Sie auf **Absenden**, um die SOAP-API-Zugriffsrichtlinie zu übermitteln.

Erstellen Sie eine globale API-Zugriffsrichtlinie, um SOAP-APIs zu schützen

Erstellen Sie eine einzelne globale API-Zugriffsrichtlinie, um alle SOAP-APIs zu schützen.

Vorbereitungen

- Erforderliche Rolle: admin
- Installieren Sie das Plugin „ **Prozessorzugriffsrichtlinie“** (com.glide.processor.policy).
- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Authentifizierungsprofile erstellen.

In den folgenden Schritten wird beschrieben, wie Sie eine einzelne globale Zugriffsrichtlinie erstellen, um alle SOAP-APIs zu schützen.

Hinweis:
Die auf den einzelnen SOAP-API-Ebenen definierten Richtlinien überschreiben die globale Zugriffsrichtlinie der **SOAPProcessor-** Ebene.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Prozesszugriffsrichtlinien**.

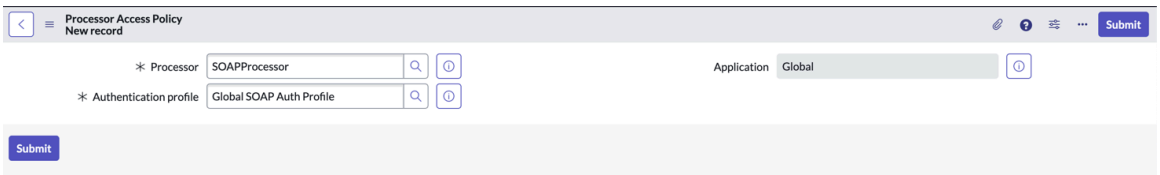
2. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Zugriffsrichtlinie verarbeiten“.

Feld	Beschreibung
Prozessor	Name zur Identifizierung der Authentifizierungsrichtlinie. Wählen Sie beispielsweise **SOAPProcessor** (Authentifizierungsprofil) aus.
Anwendung	Umfang der Authentifizierungsrichtlinie. Standard: Global
Authentifizierungsprofil	Typ des Authentifizierungsprofils. Wählen Sie **Globales SOAP-Authentifizierungsprofil**aus.



3. Wählen Sie **Absenden**.

Filterkriterien für APIs

Filterkriterien enthalten Filterbedingungen oder Abfragen, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden. Richtlinieneingaben werden verwendet, um ein oder mehrere Filterkriterien zu gruppieren und die Richtlinienbedingungen einer Authentifizierungsrichtlinie zu definieren. Zum Beispiel definiert ein IP-Filterkriterium eine IP-Adresse im CIDR-Format (Classless Inter-Domain Routing) oder einen Bereich von IP-Adressen.

Sie können Filterkriterien basierend auf der IP-Adresse, der Rolle und der Benutzergruppe des Benutzers erstellen.

Hinweis:
Sie verwenden auch die Filterkriterien, die aus dem Modul **„Adaptive Authentifizierung** “ erstellt wurden. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Sie können Filterkriterien für APIs mit demselben Verfahren wie Filterkriterien für die adaptive Authentifizierung erstellen. Nähere Informationen hierzu finden Sie unter Filterkriterien.

Zugehörige Informationen

Erstellen Sie IP-Filterkriterien

Erstellen Sie Rollenfilterkriterien

Erstellen Sie Gruppenfilterkriterien

API-Authentifizierungsrichtlinien

Authentifizierungsrichtlinien werten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen aus und erlauben oder verweigern den Zugriff abhängig von den Übereinstimmungskriterien.

Sie können die integrierte globale Sperrrichtlinie verwenden oder eine Authentifizierungsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Die globale Blockierungsrichtlinie lehnt die Authentifizierungsanforderungen von Benutzern und APIs basierend auf den angegebenen Filterkriterien ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Verwenden oder ändern Sie keine Richtlinien für „Zugriff zulassen“ und „Zugriff verweigern“. Diese Richtlinien sind nur für Benutzeranmeldungen gedacht.

Erstellen Sie eine API-Authentifizierungsrichtlinie

Mit Authentifizierungsrichtlinien können Sie Zugriffsbeschränkungen für die APIs basierend auf den angegebenen Filterkriterien erzwingen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Authentifizierungsrichtlinie**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

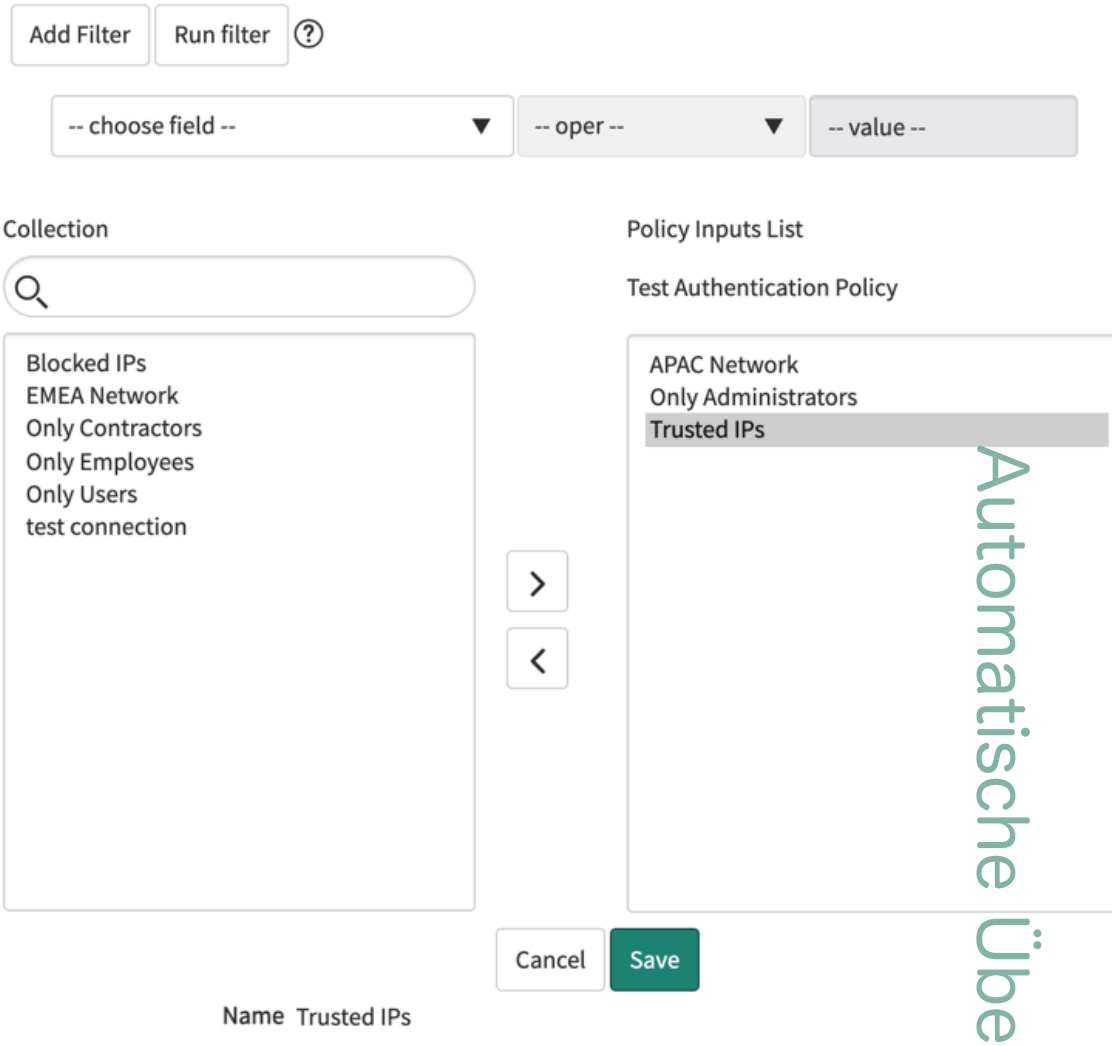
Richtlinienformular

Feld	Beschreibung
Name	Name zur Identifizierung der Richtlinie.
Beschreibung	Kurzbeschreibung der Richtlinie.
Anwendung	Umfang der Anwendung.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Wählen Sie auf der Registerkarte Richtlinieneingaben die Option **Bearbeiten** aus, um die vorhandenen Filterkriterien hinzuzufügen.
   Sie können auch eine neue Richtlinieneingabe erstellen. Weitere Informationen finden Sie unter Richtlinieneingaben erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verschieben Sie ein oder mehrere Filterkriterien aus der Liste „Sammlungen“ in die Liste „Richtlinieneingaben“.



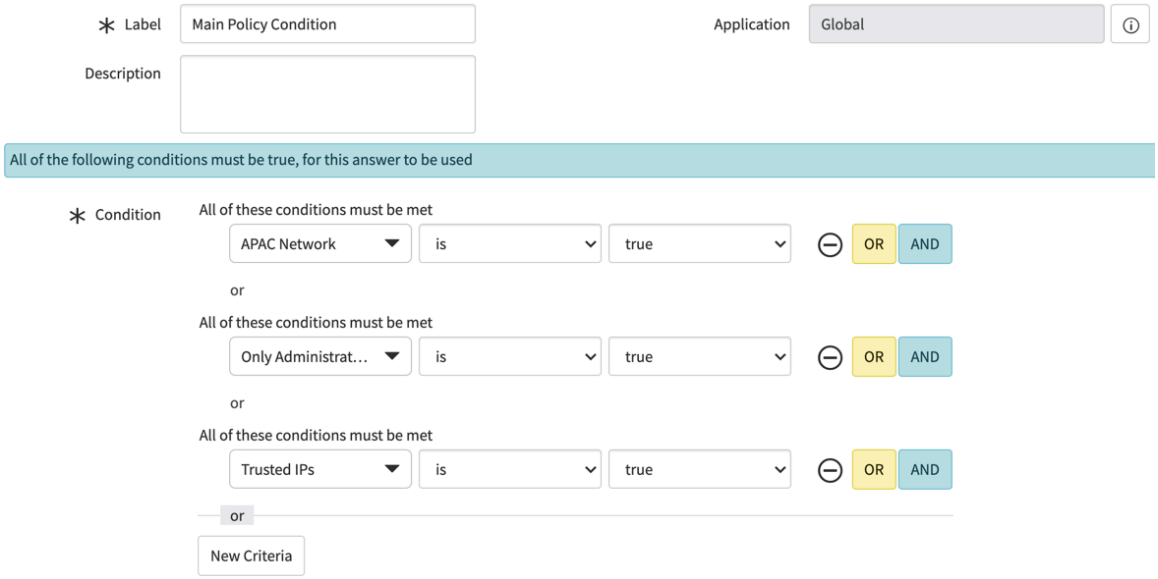
7. Wählen Sie **Speichern**.
8. Wählen Sie auf der Registerkarte Richtlinienbedingungen die Option **Neu**aus.
9. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name der Richtlinienbedingung.
Beschreibung	Kurzbeschreibung der Richtlinienbedingung.
Anwendung	Umfang der Anwendung.
Bedingung	Eine oder mehrere Bedingungen, die mit dem **ODER** -Filter kombiniert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Wählen Sie **Absenden**.

Konfigurieren Sie die globale Blockierungsrichtlinie für APIs

Die globale Blockierungsrichtlinie verweigert die Authentifizierungsanforderungen von Benutzern und APIs basierend auf den angegebenen Richtlinienbedingungen. Diese Richtlinie kann als Alternative zur IP-Adresszugriffssteuerung verwendet werden.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Globale Sperrrichtlinie**.
2. Klicken Sie auf der Registerkarte **Richtlinieneingaben** auf **Bearbeiten**.
3. Wählen Sie ein oder mehrere Filterkriterien aus der Liste **Sammlung** aus, und verschieben Sie sie in die Liste **Globale Sperrrichtlinie**.
   Sie können auch zusätzliche Filter hinzufügen.
4. Klicken Sie auf der Registerkarte **Richtlinienbedingungen** auf **Neu**.
5. Füllen Sie im Formular die folgenden Felder aus:

Bedingungsformular

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination mehrerer Richtlinieneingaben (Filterkriterien), die zum Auswerten von Authentifizierungsanforderungen verwendet wird. Sie können beispielsweise Bedingungen erstellen, die nur Auftragnehmer aus einer Liste vertrauenswürdiger IP-Adressen zulassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsrichtlinie für System-/Exportprozessoren

Möglichkeit für System-/Exportprozessoren, die Prozessorzugriffsrichtlinie zu nutzen, um alle Exportendpunkte zu sichern.

Möglichkeit, alle Exportendpunkte zu sichern und das eingehende Authentifizierungsprofil und die Prozessorzugriffsrichtlinien auf globaler Ebene oder Instanzebene anzuwenden.

Hinweis:

- Nicht öffentliche Prozessoren, einschließlich der Exportprozessoren wie CSV, PDF usw., werden für Zugriffsrichtlinien unterstützt.
- Skriptprozessoren werden auch für Zugriffsrichtlinien unterstützt.

Beispiel-Anwendungsfälle

- Der Administrator kann den RSS-Prozessor blockieren, wenn er nicht beabsichtigt, ihn zu verwenden, indem er die API-Zugriffsrichtlinie nutzt.
- Der Administrator kann ein Authentifizierungsprofil mit Basic Authentication erstellen und eine Authentifizierungsrichtlinie zuordnen, die immer als „falsch“ ausgewertet wird.

  Beispiel: Erstellen Sie IP-Kriterien mit einem Bereich von `0.0.0.0` bis `255.255.255.255` (fügen Sie auch IPv6-Adressraum hinzu), und fügen Sie dann eine Richtlinienbedingung mit dem Operator „false“ hinzu. Auf diese Weise werden Richtlinienbedingungen immer als „falsch“ ausgewertet, und die API-Zugriffsrichtlinie blockiert den Zugriff, unabhängig davon, woher die Anforderung stammt.

- Zugriff auf den Prozessor nur aus einem vertrauenswürdigen Netzwerk zulassen

Aktivieren Sie die Prozessorzugriffsrichtlinie

Installieren Sie für Prozessoren das Plugin „Prozessorzugriffsrichtlinie“ (`com.glide.processor.policy`).

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit der Prozessorzugriffsrichtlinie installiert:

- Systemeigenschaft: com.glide.auth.profile.supported.processor.list
- Modul in der Navigation: Prozessorzugriffsrichtlinien

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Processor Access Policy“ (com.glide.processor.policy).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nächste Maßnahme

.
Konfigurieren Sie das Authentifizierungsprofil für die Prozessoren. Weitere Informationen finden Sie unter Konfigurieren Sie das Authentifizierungsprofil für den Prozessor.

Konfigurieren Sie das Authentifizierungsprofil für den Prozessor

Wenden Sie ein Authentifizierungsprofil für die Exportprozessoren an.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: Processor Access Policy (com.glide.processor.policy)

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Prozesszugriffsrichtlinien**.
2. Klicken Sie auf **Neu**, um dem Prozessor ein Authentifizierungsprofil hinzuzufügen.
3. Füllen Sie die Felder des Formulars aus.

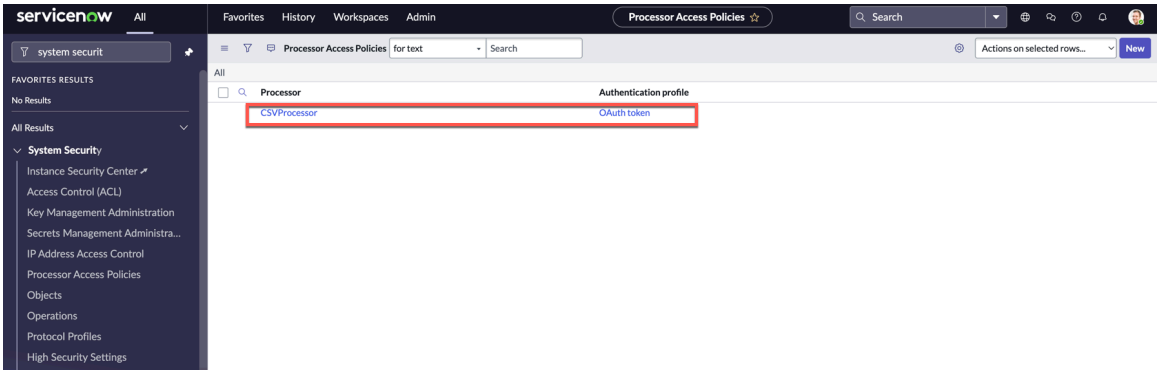
Formular „Zugriffsrichtlinie verarbeiten“.

Feld	Beschreibung
Prozessor	Name zur Identifizierung der Authentifizierungsrichtlinie. **Hinweis:** Öffentliche Prozessoren werden nicht unterstützt. Wenn ein nicht unterstützter Prozessor ausgewählt wird, wird während der Übermittlung des Prozessors ein Fehler angezeigt.
Anwendung	Umfang der Authentifizierungsrichtlinie. Standard: Global
Authentifizierungsprofil	Typ des Authentifizierungsprofils. Sie können **ID-Token** oder **OAuth-Token**auswählen.

4. Klicken Sie auf **Absenden**.
Das Authentifizierungsprofil wird auf den Prozessor angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise wird das OAuth-Authentifizierungsprofil für den CSV-Prozessor konfiguriert. In diesem Fall müssen Sie das OAuth-Zugriffstoken für den Export mit CSV als Exportoption verwenden.



Zertifikatbasierte Authentifizierung

Mit der zertifikatsbasierten Authentifizierung können Sie Benutzeranmeldungen oder eingehende API-Anforderungen mithilfe von Zertifikaten einer vertrauenswürdigen Zertifizierungsstelle (CA) gegenseitig authentifizieren.

Hinweis:
Die zertifikatsbasierte Authentifizierung wird in der lokalen Instanz mit aktivierter Edge Encryption nicht unterstützt.

Zertifikatsbasierte Authentifizierung für Benutzeroberflächenanmeldungen

Ermöglichen Sie Endbenutzern die Verwendung von PIV- (Personal Identity Verification) oder CAC-Karten (Common Access Card), um sich bei Now Platform oder Serviceportal anzumelden, anstatt einen Benutzernamen und ein Passwort zu verwenden. Informationen zum Einrichten der gegenseitigen Authentifizierung für Anmeldungen an der Benutzeroberfläche finden Sie unter Richten Sie die zertifikatsbasierte Authentifizierung ein.

Nach der Einrichtung der zertifikatsbasierten Authentifizierung können Endbenutzer die Einrichtung abschließen und sich anmelden. Weitere Informationen finden Sie unter Melden Sie sich mit der zertifikatsbasierten Authentifizierung an.

Zertifikatsbasierte Authentifizierung für eingehende Webservices

Authentifizieren Sie eingehende Anforderungen bei ServiceNow SOAP- und REST-APIs. Informationen zum Einrichten der gegenseitigen Authentifizierung für eingehende Webservices finden Sie unter Richten Sie die zertifikatsbasierte Authentifizierung ein.

Richten Sie die zertifikatsbasierte Authentifizierung ein

Richten Sie die gegenseitige Authentifizierung für benutzeroberflächenbasierte Anmeldungen oder eingehende Webservices ein.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergewissern Sie sich, dass Ihre Instanz ein ADCv2-Lastenausgleichsmodul verwendet. Weitere Informationen finden Sie imWissensartikel ADCv2-Migration . Wenn Ihre Instanz das ADCv2-Lastenausgleichsmodul nicht verwendet, wenden Sie sich an Now Support.

Prozedur

Richten Sie die zertifikatsbasierte Authentifizierung ein, um:

- Ermöglichen Sie Endbenutzern die sichere Anmeldung bei Now Platform oder Serviceportal mit PIV- oder CAC-Karten. Nachdem die zertifikatsbasierte Authentifizierung aktiviert wurde, können Sie das PEM-Zertifikat selbst registrieren, oder ein Administrator kann das Zertifikat für Sie zuordnen. Weitere Informationen finden Sie unter Melden Sie sich mit der zertifikatsbasierten Authentifizierung an.
- Aktivieren Sie die gegenseitige Authentifizierung für eingehende Webservices. Sobald die zertifikatsbasierte Authentifizierung eingerichtet ist, verwendet das System die bereitgestellten Zertifikate, um Anforderungen für den Zugriff auf ServiceNow REST- und SOAP-APIs gegenseitig zu authentifizieren.

Aktivieren Sie die zertifikatsbasierte Authentifizierung

Sie können das Plugin für die zertifikatsbasierte Authentifizierung (com.glide.auth.mutual) für Now Platform aktivieren, wenn Sie die Administratorrolle innehaben.

Vorbereitungen

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Tabellen werden mit der zertifikatsbasierten Authentifizierunginstalliert:

- sys_user_certificate
- sys_ca_certificate
- sys_ca_certificate_api_track

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „ Certificate-based Authentication “ (com.glide.auth.mutual).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Registrieren Sie das CA-Zertifikat

Registrieren Sie Stammzertifikate oder Zwischenzertifikate, um sie für die Authentifizierung verfügbar zu machen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **CA-Zertifikatkette**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „Zertifizierungszertifikat für gegenseitige Authentifizierung“

Feld	Beschreibung
Name	Name zur Identifizierung des Zertifikats.
Ablaufbenachrichtigung	Option, um Benutzer zu warnen, wenn ein Zertifikat abläuft.
Benachrichtigung bei Ablauf	Liste der Benutzer, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage, an denen eine Benachrichtigung an Benutzer gesendet wird, bevor ein Zertifikat abläuft.
Aktiv	Option zum Aktivieren des Client-Zertifikats.
Format	PEM
Typ	Typ des Zertifikats. Verfügbare Optionen: ○ **CA-Zert**: Das CA-Stammzertifikat. Kann auch Zwischenzertifikate in die Kette einbeziehen. CA-Zertifikate werden automatisch mit dem Lastenausgleichsmodul synchronisiert. Verwenden Sie diese Option nach Möglichkeit, um zu vermeiden, dass ein erforderliches Zertifikat in der Kette fehlt. ○ **Zwischenzertifikat**: Ein Zwischenzertifikat in der Zertifikatkette. Dieses Zertifikat verbleibt nur in der Instanz und wird nicht mit dem Lastenausgleichsmodul synchronisiert. Verwenden Sie diese Option nur, wenn Sie einer vorhandenen Kette ein Zwischenzertifikat hinzufügen müssen.
Kurzbeschreibung	Kurzbeschreibung des Benutzer-Client-Zertifikats.

Hinweis:
Während des Zertifikat-Uploads werden die schreibgeschützten Felder **Gültig ab**, **Ablaufdatum**, **Ablaufdatumin Tagen**, Aussteller und **Antragsteller**, **Zertifikatkette**und **PEM-Zertifikat** extrahiert und automatisch ausgefüllt.

4. Klicken Sie auf **Absenden**.
5. **Wahlweise:** Klicken Sie auf **Speicher/Zertifikate** validieren, um das Zertifikat zu validieren.

Ordnen Sie das PEM-Zertifikat dem Benutzer zu

Ordnen Sie Benutzern PEM-Zertifikate zu, damit sie sich mit PIV- oder CAC-Karten anmelden oder eingehende Anforderungen authentifizieren können. Sie können einem Benutzer mehrere PEM-Zertifikate zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Erforderliche Rolle: admin
- Vergewissern Sie sich, dass Sie das PEM-Zertifikat (Privacy Enhanced Mail) des Benutzers haben.

Hinweis:
Nach der Konfiguration „PEM-Zertifikat zu Anwender zuordnen“ schlägt „Zertifikat überprüfen“ fehl. Dies liegt daran, dass das PEM-Zertifikat nicht gespeichert wird.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **Benutzer-zu-Zertifikat-Zuordnung** und klicken Sie auf **Neu**.
2. Füllen Sie im Formular die folgenden Felder aus:

Formular „Benutzer-Client-Zertifikat“

Feld	Beschreibung
Name	Name des Benutzer-Client-Zertifikats.
Ablaufbenachrichtigung	Option, um Benutzer zu warnen, wenn ein Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage, an denen eine Benachrichtigung an Benutzer gesendet wird, bevor ein Zertifikat abläuft.
Benachrichtigung bei Ablauf	Liste der Benutzer, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Aktiv	Option zum Aktivieren des Client-Zertifikats.
Benutzer	Benutzer, der dem Client-Zertifikat zugeordnet ist. Das System empfängt das Client-Zertifikat entweder von der eingehenden Anforderung oder der Zertifikatregistrierungund verwendet dann den in diesem Feld angegebenen Benutzer, um eine Sitzung zur Ausführung der Anforderung zu initiieren.
Kurzbeschreibung	Kurzbeschreibung des Benutzer-Client-Zertifikats.
Format	Das PEM-Format (Privacy Enhanced Mail) ist ein base64-codiertes DER-Zertifikat (Distinguished Encoding Rules).
Typ	Client-Zertifikat Dieses Feld ist schreibgeschützt.

Hinweis:
Während des Zertifikat-Uploads werden die schreibgeschützten Felder **Gültig ab**, **Ablaufdatum**, **Ablaufdatum**, **Aussteller**und **Betreff** extrahiert und automatisch ausgefüllt.

3. Klicken Sie auf das Anhangsymbol, und laden Sie das Zertifikat hoch.
4. Klicken Sie auf **Absenden**.
Das Zertifikat wird validiert und dem angegebenen Benutzer zugeordnet, wenn das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) stammt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Eigenschaften der zertifikatsbasierten Authentifizierung

Verwenden Sie Systemeigenschaften, um zertifikatbasierte Authentifizierungsfunktionen zu aktivieren oder zu deaktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **Eigenschaften**.
2. Füllen Sie die Felder im Formular aus.

Formular „Eigenschaften der zertifikatsbasierten Authentifizierung“

Eigenschaft	Beschreibung
Zertifikatbasierte Authentifizierung aktivieren	Option zum Aktivieren der zertifikatsbasierten Authentifizierung für Anmeldungen an der Benutzeroberfläche und eingehende Webservices. Standardwert: true
Option „Mit PIV/CAC anmelden“ auf dem Anmeldebildschirm anzeigen	Zeigt die Option **Mit PIV/CAC-Karte** anmelden auf dem Anmeldebildschirm an. Ermöglicht Benutzern die Anmeldung mit zertifikatbasierter Authentifizierung über die -Benutzeroberfläche. Standardwert: false
Automatische Weiterleitung für die zertifikatbasierte Anmeldung aktivieren	Legt fest, ob der Benutzer **auf Mit PIV/CAC-Karte** anmelden klicken muss, nachdem er ein registriertes Zertifikat ausgewählt und seine PIN eingegeben hat. Aktivieren Sie diese Option, um den Benutzer automatisch anzumelden, nachdem er ein registriertes Client-Zertifikat ausgewählt und seine PIN eingegeben hat. Deaktivieren Sie diese Option, damit der Benutzer **auf Mit PIV/CAC-Karte** anmelden klicken muss, nachdem er ein registriertes Client-Zertifikat ausgewählt und seine PIN eingegeben hat. Standardwert: false

Melden Sie sich mit der zertifikatsbasierten Authentifizierung an

Nachdem Ihr Administrator die zertifikatsbasierte Authentifizierung eingerichtet hat, können Sie das Client-Zertifikat registrieren und sich mit Ihrer PIV-Karte (Personal Identity Verification) oder CAC-Karte (Common Access Card) anmelden.

Registrieren Sie das Client-Zertifikat für Ihre PIV- oder CAC-Karte

Bevor Sie sich mit Ihrer PIV- oder CAC-Karte bei Now Platform anmelden, müssen Sie das Client-Zertifikat Ihrer PIV- oder CAC-Karte registrieren. Wenn Sie das Client-Zertifikat nicht registrieren können, wenden Sie sich an Ihren Administrator. Ihr Administrator kann auch das Client-Zertifikat Ihrer PIV- oder CAC-Karte registrieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass die zertifikatsbasierte Authentifizierung aktiviert ist.
- Vergewissern Sie sich, dass ein Kartenleser mit Ihrem Computer verbunden und Ihre PIV- oder CAC-Karte eingelegt ist.
- Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

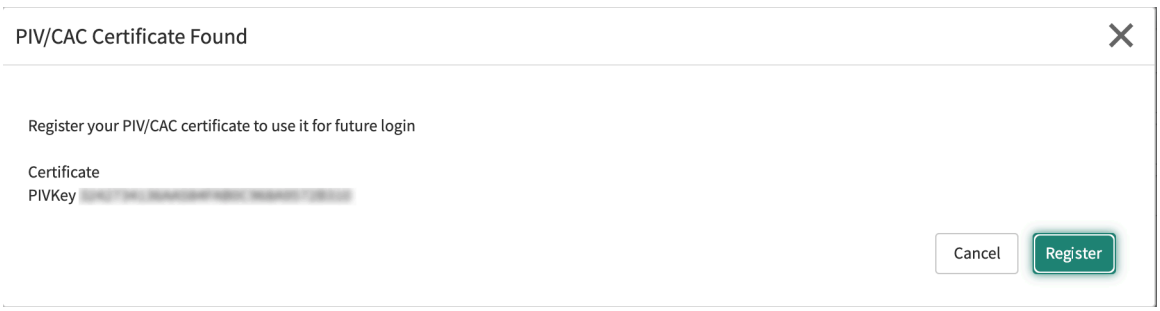
Wenn Sie einen Administrator benötigen, um Ihr Client-Zertifikat zu registrieren, finden Sie weitere Informationen unter Ordnen Sie das PEM-Zertifikat dem Benutzer zu.

Prozedur

1. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Now Platform an.
2. Klicken Sie im **Benutzermenü** auf Ihren Namen, und wählen Sie **Profil**aus.

3. Klicken Sie unter **Zugehörige Links**auf **Client-Zertifikat registrieren**.

   Wenn ein gültiges Zertifikat verfügbar ist, wird die folgende Meldung angezeigt:

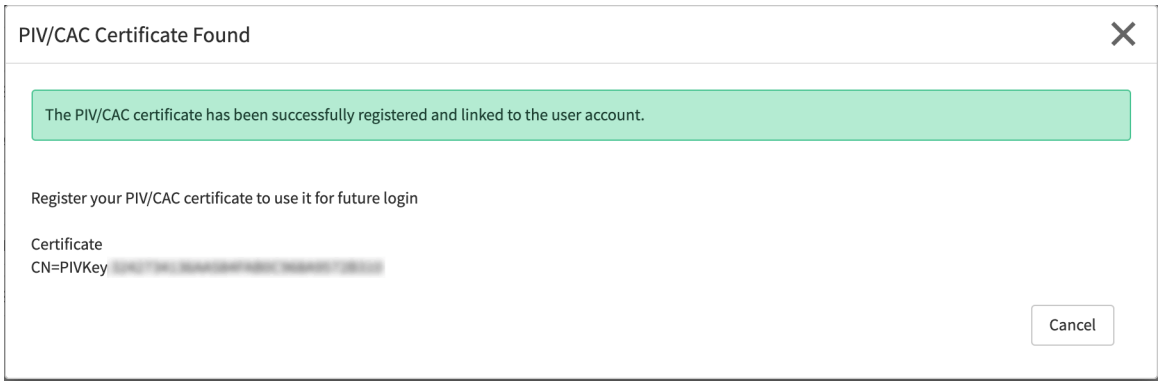


4. Klicken Sie auf **registrieren**.

   Nach erfolgreicher Registrierung wird die folgende Meldung angezeigt:

   Das PIV/CAC-Zertifikat wurde registriert und mit dem Anwenderaccount verknüpft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie sich das nächste Mal bei Ihrer Now Platform anmelden, können Sie sich mit Ihrer PIV- oder CAC-Karte anmelden. Weitere Informationen finden Sie unter Melden Sie sich mit der PIV- oder CAC-Karte bei Now Platform an.

Melden Sie sich mit der PIV- oder CAC-Karte bei Now Platform an

Sie können sich mit Ihrer PIV- oder CAC-Karte anstelle von Benutzername und Passwort anmelden, wenn die zertifikatsbasierte Authentifizierung für Now Platformaktiviert ist.

Vorbereitungen

- Erforderliche Rolle: keine
- Stellen Sie sicher, dass die zertifikatsbasierte Authentifizierung aktiviert ist.
- Stellen Sie sicher, dass ein PIV- oder CAC-Kartenleser mit Ihrem Computer verbunden ist.
- Stellen Sie sicher, dass Ihnen ein Client-Zertifikat Ihrer PIV- oder CAC-Karte zugeordnet ist. Weitere Informationen finden Sie unter Registrieren Sie das CA-Zertifikat.

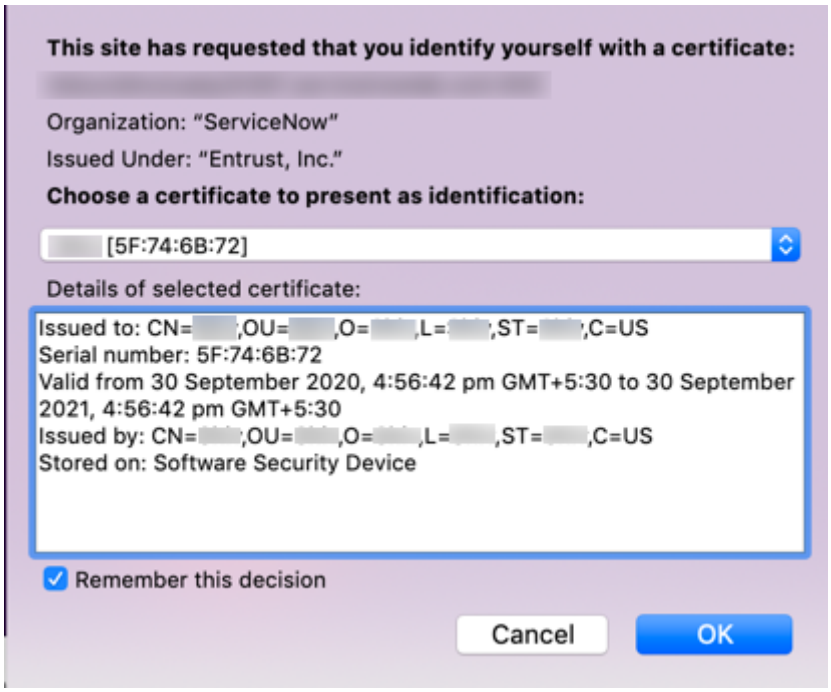
Prozedur

1. Legen Sie Ihre PIV- oder CAC-Karte in den Kartenleser ein.
2. Navigieren Sie in einem Browser zu Ihrer Instanz.
   Der Browser fordert zur Eingabe einer PIN für Ihre PIV- oder CAC-Karte auf.
3. Geben Sie die PIN Ihrer PIV- oder CAC-Karte in die Eingabeaufforderung des Browsers ein.

   Hinweis:
   Wenn Sie Ihre PIN vergessen haben, wenden Sie sich an Ihren Administrator.

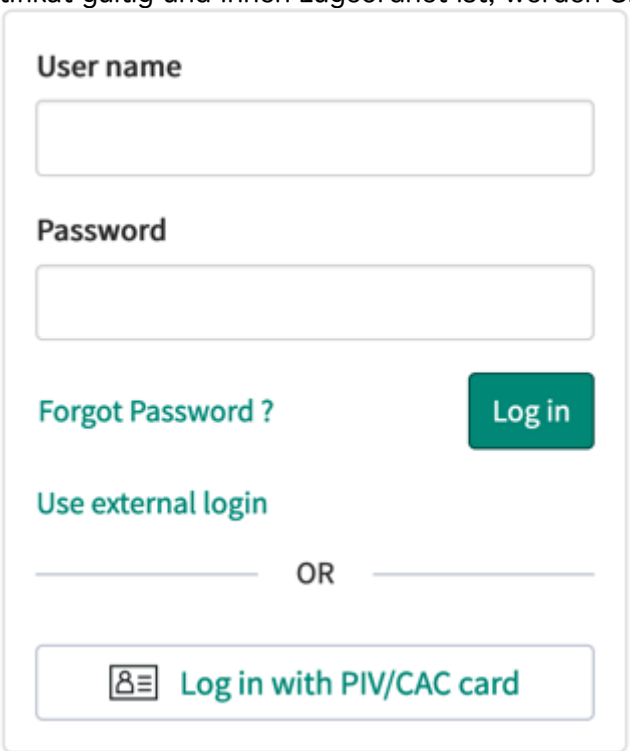
4. Wenn Sie eine korrekte PIN eingeben, zeigt der Browser eine Aufforderung zur Auswahl eines Zertifikats an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie in der Browser-Eingabeaufforderung ein Zertifikat aus.

   Wenn das Zertifikat gültig und Ihnen zugeordnet ist, werden Sie zur Anmeldeseite



   weitergeleitet.

6. Klicken Sie **auf Mit PIV/CAC-Karte** anmelden.

   Um sich von der Now Platform abzumelden, müssen Sie den PIV oder CAC aus dem Kartenleser entfernen und dann den Browser schließen.

Ihre Client-Zertifikate verwalten

Zeigen Sie Client-Zertifikate an, die Ihrem Konto zugeordnet sind, und löschen Sie sie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass die zertifikatsbasierte Authentifizierung aktiviert ist.
- Erforderliche Rolle: keine

Prozedur

1. Melden Sie sich bei Now Platform mit Ihrem Benutzernamen und Passwort an.
2. Klicken Sie im **Benutzermenü** auf Ihren Namen, und wählen Sie **Profil**aus.

3. Klicken Sie unter **Zugehörige Links**auf **Client-Zertifikate verwalten**.
   Die Tabelle „Benutzer-Client-Zertifikate“ [sys_user_certificate] wird geöffnet und zeigt Zertifikate an, die Ihrem Konto zugeordnet sind.
4. Zeigen Sie Zertifikate an, die Ihrem Konto zugeordnet sind, oder löschen Sie sie.

Benutzerdefinierte URLs, die Ihrer Instanz zugeordnet sind

Sie können Ihre ServiceNow -Instanz so konfigurieren, dass sie über eine Unternehmens-Branding-URL oder eine benutzerdefinierte URL zugänglich ist.

Übersicht über benutzerdefinierte URLs

Sie können eine benutzerdefinierte URL verwenden, damit die Instanz ServiceNow von einer oder mehreren Unternehmens-Branding-URLs oder benutzerdefinierten URLs aus zugänglich ist.

Benutzerdefinierte URLs können einem bestimmten Portal zugeordnet werden. Beispielsweise kann der Administrator http://support.acme.com für das CSM-Portal und http://hr.acme.com für das HR-Portal definieren. In einer solchen Situation müssen Benutzer zur Authentifizierung auf Grundlage der benutzerdefinierten URL, auf die sie zugreifen, zu verschiedenen IdPs umgeleitet werden.

Wichtig:

- Erstellen Sie keine benutzerdefinierte URL mit mehr als 100 Domänen pro Instanz.
- Sie müssen zuerst den benutzerdefinierten URL-Datensatz aus der Instanz ServiceNow löschen und dann alle DNS-Einträge (Domain Name Server) vom DNS-Server löschen.
- Jede Löschung eines DNS-Eintrags vom DNS-Server vor dem Löschen eines benutzerdefinierten URL-Datensatzes aus der Instanz ServiceNow führt dazu, dass die Löschung anderer entsprechender benutzerdefinierter URL-Datensätze aus ServiceNowblockiert wird.

Von Tokyoaus können Sie Benutzern erlauben, automatisch zu angegebenen IdPs umzuleiten, die im benutzerdefinierten URL-Datensatz definiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Benutzerdefinierte URLs sind für lokale Kunden- oder Entwicklerinstanzen nicht verfügbar. Außerdem muss die URL öffentlich zugänglich sein.

Nur der Besitzer der Domäne auf oberster Ebene (TLD) oder einer Subdomäne kann die benutzerdefinierte URL für eine DNS-Subdomäne konfigurieren. Beispielsweise kann Ihre Instanz die folgende festgelegte URL und zusätzliche benutzerdefinierte URLs haben:

Beispiel für eine benutzerdefinierte URL

Beispiel-URLs	Verwendung
https://acme.service-now.com	Der anfängliche Domänenname für Acme, der mit der Instanz ServiceNow geliefert wurde.
https://support.acme.com	Eine benutzerdefinierte URL, die Ihrer ServiceNow -Instanz zugeordnet ist. Diese URL wird als Alias (CNAME) des ursprünglichen Domänennamens bezeichnet.
https://US-support.acme.com	Eine sekundäre benutzerdefinierte URL, die einem Service Portal in Ihrer Instanz zugeordnet ist. Ihre Instanz kann mehrere benutzerdefinierte URLs zu demselben Service Portal unterstützen.

Überlegungen zu benutzerdefinierten URLs außerhalb Ihrer Instanz

Bevor Sie eine benutzerdefinierte URL zuordnen können, müssen Sie eine URL über einen Domänenanbieter besitzen (oder erwerben). Es sind auch bestimmte Konfigurationen erforderlich, bevor Sie eine benutzerdefinierte URL in Ihrer Instanz erstellen und zuordnen können.

Benutzerdefinierte URL-Konfigurationen

Konfigurationselemente	Beschreibung
Legen Sie den CNAME mit dem Provider fest	Der CNAME-Datensatz muss als Instanz-URL ServiceNow festgelegt werden.
Bestimmen Sie Ihren dedizierten VIP-Status	Der Status von VIP.

Hinweis:
Wenn Sie CNAME-Datensätze löschen oder aktualisieren, die auf Ihre Instanz verweisen, müssen Sie diese Reihenfolge einhalten, um zu vermeiden, dass Datensätze in der Instanz hängen bleiben. Löschen Sie zuerst die CNAME-Datensätze aus Ihrer Instanz, und entfernen oder aktualisieren Sie dann die CNAME-Einstellung bei Ihrem DNS-Provider.

Aktivieren Sie benutzerdefinierte URLs

Aktivieren Sie benutzerdefinierte URLs, die in Ihrer ServiceNow -Instanz eingerichtet werden sollen. Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „Benutzerdefinierte URL“ (com.snc.customurl) aktivieren.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**.
2. Suchen Sie nach dem Plugin „ **Benutzerdefinierte URL** “ und klicken Sie darauf.

   Hinweis:
   Wählen Sie nicht das Plugin „ **Benutzerdefinierte URL – Intern** “ aus, das eine interne Komponente für geskriptete benutzerdefinierte URL-APIs ist.

3. Klicken Sie im Datensatz „Benutzerdefinierte URL“ auf den zugehörigen Link **Aktivieren/Reparieren**.
4. Klicken Sie im Fenster Plugin-Aktivierung auf **Aktivieren**.
   Wenn das Fenster „Plugin-Aktivierung“ mit einer Meldung erneut geöffnet wird, dass das Plugin aktiviert ist, klicken Sie auf **Formular schließen und neu laden, um in diesem Formular** zu bleiben.
5. Suchen Sie in der zugehörigen Liste „Plugin-Dateien“ nach der folgenden Eigenschaft, und ändern Sie den Einstellungswert:

Option	Bezeichnung
glide.customurl.enabled	Um benutzerdefinierte URLs zu aktivieren, legen Sie den Wert auf **True**fest. Standardmäßig ist diese Eigenschaft auf **False**festgelegt, was bedeutet, dass Sie keine benutzerdefinierte URL zuordnen können. **Hinweis:** Um diese Funktion zu deaktivieren, setzen Sie diese Eigenschaft zurück auf **False**.

6. Klicken Sie auf **Aktualisieren**.

Legen Sie eine benutzerdefinierte URL als Instanz-URL fest

Fügen Sie Ihrer Instanzkonfiguration eine benutzerdefinierte URL hinzu, die anstelle Ihrer URL ServiceNow verwendet werden soll.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen das benutzerdefinierte URL-Plugin aktivieren und eine URL erworben oder registriert haben, bevor Sie die benutzerdefinierte URL zu Ihrer Instanz hinzufügen.

Prozedur

1. Navigieren zu **Alle** > **Benutzerdefinierte URL** > **Benutzerdefinierte URL**.
2. Sie sollten entweder:
   - Klicken Sie auf **Neu**, um einen neuen Domänennamen zuzuordnen, der für Ihre Instanz neu ist.
   - Wählen Sie eine bereits eingerichtete benutzerdefinierte URL aus, die als Instanz-URL festgelegt werden soll.
3. Füllen Sie die entsprechenden Felder aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerdefinierte URL-Felder

Feld	Beschreibung
Domänenname	Vollständig qualifizierter Domänenname (FQDN) der benutzerdefinierten URL. Der FQDN ist eine CNAME-Umleitung, die im Nameserver-Datensatz für die benutzerdefinierte Domäne erstellt wird. **Hinweis:** Beispielsweise können Sie im Nameserver für acme.com einen Eintrag erstellen: `support.acme.com 300 IN CNAME acme.servicenow.com`
Ist Instanz-URL	Checkbox, um diese benutzerdefinierte URL für alle ausgehenden URLs zu aktivieren. Nur eine aktive benutzerdefinierte URL kann die Instanz-URL sein. Um diese Einstellung für eine benutzerdefinierte URL zu aktivieren, klicken Sie im URL-Datensatz auf **Als Instanz-URL** festlegen. Alle vorherigen benutzerdefinierten URLs werden dann entfernt.
Status	Status des benutzerdefinierten URL-Datensatzes. Wenn der Status **Active**lautet, wird die benutzerdefinierte URL bereitgestellt und kann verwendet werden.
Serviceportal	Service Portal, das Sie verwenden möchten, wenn Sie Benutzer mit der benutzerdefinierten URL zu Ihrer Instanz umleiten.
Identitätsanbieter	Mit dem Identitätsanbieter für die benutzerdefinierte URL können Sie Benutzern erlauben, automatisch zu den im benutzerdefinierten URL-Datensatz definierten IdPs umzuleiten.

Eine benutzerdefinierte URL sollte innerhalb von sechs Stunden in Ihrer Instanz aktiviert werden. Ein Hintergrundauftrag fragt alle 30 Minuten den Abschluss des benutzerdefinierten URL-Auftrags ab.

Hinweis:

- Sie müssen zuerst den benutzerdefinierten URL-Datensatz aus der Instanz ServiceNow löschen und dann alle DNS-Einträge (Domain Name Server) vom DNS-Server löschen.
- Jede Löschung eines DNS-Eintrags vom DNS-Server vor dem Löschen eines benutzerdefinierten URL-Datensatzes aus der Instanz ServiceNow führt dazu, dass die Löschung anderer entsprechender benutzerdefinierter URL-Datensätze aus ServiceNowblockiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerdefinierte URL mit Identitätsanbieter

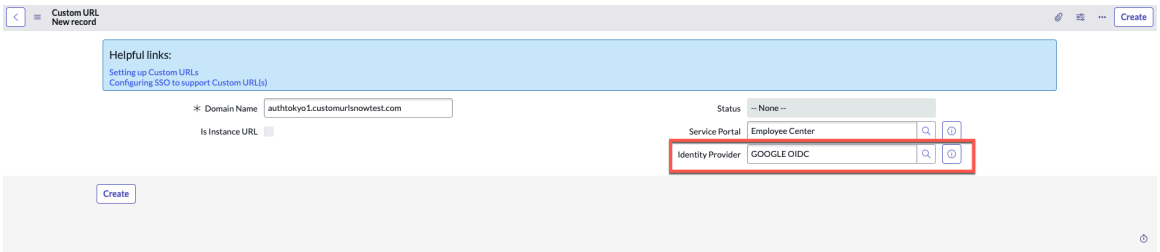
Legen Sie Ihre benutzerdefinierte URL beim Identitätsanbieter fest, damit sich der Benutzer bei seinem IdP anmelden kann.

Vorbereitungen

Erforderliche Rolle: admin

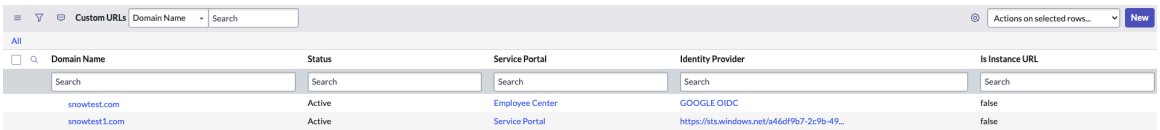
Prozedur

1. Navigieren zu **Alle** > **Benutzerdefinierte URL** > **Benutzerdefinierte URL**.
2. Klicken Sie auf **Neu**.
3. Geben Sie die Details des IdP im Feld **Identitätsanbieter** an.
   Informationen zu anderen Feldern finden Sie unter Legen Sie eine benutzerdefinierte URL als Instanz-URL fest.



4. Klicken Sie auf **Erstellen**.

   Der Datensatz wird erstellt und auf der Seite „Benutzerdefinierte URL“ angezeigt.



   Wenn auf die benutzerdefinierte URL zugegriffen wird, wird der Benutzer an den konfigurierten Identitätsanbieter weitergeleitet. In diesem Fall wird der Benutzer beim Zugriff auf snowtest.comzum **Employee Center**und dann zum Identitätsanbieter Google weitergeleitet.

   Hinweis:

   - Wenn das Feld Serviceportal leer ist und das Feld „Identitätsanbieter“ definiert ist, wird der Benutzer beim Zugriff auf die benutzerdefinierte URL direkt zum konfigurierten Identitätsanbieter geleitet.
   - Wenn sowohl das Feld Serviceportal als auch das Feld Identitätsanbieter definiert ist und der Benutzer beim Zugriff auf die benutzerdefinierte URL mit dem definierten Serviceportal auf die benutzerdefinierte URL zugreift, wird der Benutzer zum konfigurierten Identitätsanbieter navigiert.
   - Wenn sowohl das Feld Serviceportal als auch das Feld „Identitätsanbieter“ definiert ist und der Benutzer beim Zugriff auf die benutzerdefinierte URL mit einem anderen Portal, das nicht definiert ist, auf die benutzerdefinierte URL zugreift, wird der Benutzer zum Identitätsanbieter für die automatische Umleitung navigiert, sofern für die Instanz konfiguriert.

5. Verwenden Sie die -Anmeldeinformationen, um sich bei der Anwendung anzumelden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum benutzerdefinierten URL-Rechenzentrumsauftrag

Jede benutzerdefinierte URL, die Ihrer Instanz zugeordnet ist, verfügt über einen entsprechenden ServiceNow-Rechenzentrumsauftrag, der ausgeführt wird und URL-Informationen anzeigt, die für Ihre Instanz relevant sind, wie in der Tabelle beschrieben.

Auftragsfeld	Beschreibung
Auftrags-ID	Eindeutige ID des Auftrags, der die Domäne der benutzerdefinierten URL überprüft.
Letzte Ausführung um	Datum und Uhrzeit der letzten Ausführung des Auftrags.
Nutzlast	Liste der Domänen oder benutzerdefinierten URLs, die zur CERT-Bereitstellung an das Rechenzentrum gesendet wurden.
Abrufanzahl	Anzahl der Abfragen der Ergebnisse für diesen Auftrag.
Ergebnis	Überprüft und validiert jede Domäne oder benutzerdefinierte URL, die in einer Nutzlast gesendet wird.
Status	Status des Rechenzentrumsauftrags.

Generieren von SP-Metadaten für benutzerdefinierte SAML/SSO-URL-Installationen

Für eine SAML- oder SSO-Installation müssen die SP-Metadaten für den IdP generiert werden, bevor die benutzerdefinierte URL-Instanz generiert wird.

Vorbereitungen

Erforderliche Rolle: admin

Der IdP benötigt SP-Metadaten für die Instanz, um Anforderungen zu authentifizieren und weiterzuleiten.

Hinweis:
Das Hinzufügen der Assertion Consumer Service-URL (SP-Anmelde-URL) kann für jeden IdP (Azure, ADFS oder Okta) unterschiedlich sein.

Prozedur

1. Wählen Sie Ihr installiertes SSO-Plugin aus:

Option	Bezeichnung
Mehrfachanbieter-SSO	Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**. Wählen Sie einen IdP aus, und klicken Sie auf die Schaltfläche **Metadaten generieren**. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschafteneinstellungen.
SAML 2-SSO	Navigieren zu **SAML 2 Single Sign-on** > **Metadaten**. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschafteneinstellungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Kopieren Sie die SP-Metadaten in das Textfeld.

   Beispiel:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

  <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Stellen Sie die SP-Metadaten der Instanz für den IdP bereit.
   Zum Beispiel ermöglicht SSOCircle einem Benutzer, die SP-Metadaten online bereitzustellen.

4. **Wahlweise:** So richten Sie benutzerdefinierte URLs in Azure ein:

   a. Wechseln Sie zu **App-Registrierungen**.

   b. Wählen Sie im Menü **Alle Apps** aus.

   c. Wählen Sie die **ServiceNow-App aus**.

   d. Klicken Sie auf Einstellungen, um die URL zu konfigurieren.

5. **Wahlweise:** So richten Sie benutzerdefinierte URLs in Okta ein:

   a. Erstellen Sie zwei ServiceNow UD Okta-Anwendungen.

   b. Eine Okta-Anwendung für die Instanz-URL „service-now.com“.

   c. Eine Okta-Anwendung für die benutzerdefinierte URL.

   Hinweis:

   - Deaktivieren Sie die **Option Authentifizierung** erzwingen in der Okta-Konfiguration, damit die **Testverbindung** erfolgreich ausgeführt wird.
   - Wenn Sie den Identitätsanbieter-Datensatz testen, der der Basis-URL zugeordnet ist, stellen Sie sicher, dass Sie sich bei der Instanz mit der Basis-URL anmelden müssen.
   - Wenn Sie den Identitätsanbieter testen, der der benutzerdefinierten URL zugeordnet ist, stellen Sie sicher, dass Sie sich mit der benutzerdefinierten URL bei der Instanz angemeldet haben.

6. **Wahlweise:** Um die OAuth-Authentifizierung zu verwenden, richten Sie die Umleitungs-URL als alle registrierten benutzerdefinierten URLs in der OAuth-Anwendungsendpunktkonfiguration für die externen Clientanwendungen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Umleitungs-URL ist gleichbedeutend mit der Rückruf-URL, an die der Autorisierungsserver umleitet.

7. **Wahlweise:** Um den Google reCAPTCHA-Service zu verwenden, richten Sie ein API-Schlüsselpaar ein.

Benutzerdefinierte URL – Fehler und Korrekturen

Eine Liste der häufigsten Fehler und zugehörigen Korrekturen für das Setup und die Konfiguration einer benutzerdefinierten URL.

Fehler beim Setup

Fehlermeldung	Beheben
Benutzerdefinierte URL kann nicht erstellt werden. Versuchen Sie es später erneut.	Möglicherweise liegt ein Problem außerhalb Ihrer Kontrolle vor, das die Erstellung der benutzerdefinierten URL beeinträchtigt. Führen Sie zu einem anderen Zeitpunkt aus, bevor Sie sich an den Support wenden. **Hinweis:** Das Erstellen einer benutzerdefinierten URL dauert normalerweise 30 Minuten. Wenn es länger dauert, wenden Sie sich an https://support.servicenow.com/now?draw=case.
Die Anforderung für eine neue benutzerdefinierte URL kann nicht gesendet werden, da eine andere Anforderung für eine benutzerdefinierte URL für Ihre Instanz noch ausgeführt wird.	Überprüfen Sie den Status Ihrer benutzerdefinierten URL-Aufträge, bevor Sie eine neue Anforderung senden.
Sie müssen die folgenden Eigenschaften löschen, bevor die Instanz-URL festgelegt werden kann: Glide-Proxy, Glide-Servlet.	
Die Bereitstellung von<custom_domain> wird noch ausgeführt. Dieser Prozess kann bis zu X Stunden dauern. Ihr Instanzadministrator erhält eine Benachrichtigung, wenn dieser Prozess abgeschlossen ist.	Nachdem die Bereitstellung auf einer Instanz für eine benutzerdefinierte URL gestartet wurde, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor sich der Status ändert.
<custom_domain>ist jetzt als neue Instanz-URL festgelegt.<base.service-now.com> ist noch in Betrieb, aber alle neuen URLs, z. B. in Benachrichtigungen, verwenden .	Nur eine URL kann als Instanz-URL festgelegt werden. Die anderen URLs, die Ihrer Instanz zugeordnet sind, können aktiv sein, aber nur die Instanz-URL kann Benachrichtigungen verwenden.
Die benutzerdefinierte URL<custom_domain> ist so eingestellt, dass er sofort aus der Instanzkonfiguration entfernt und wiederhergestellt wird<base.service-now.com> . setzt eine Zuordnung zu dieser Instanz fort, solange der CNAME-Datensatz in Ihrem DNS festgelegt ist.	Diese Nachricht bestätigt, dass Sie Ihre benutzerdefinierte URL ändern möchten. Durch Akzeptieren dieser Bestätigung initiieren Sie die Änderung der URL zu Ihrer Instanz. Jede URL, die sich in Ihrer Domänennamenliste befindet, kann als benutzerdefinierte URL aktiv sein, es sei denn, Sie entfernen sie aus dem CNAME-Datensatz Ihres Providers.
Sie können glide.servlet.uri nicht ändern. Diese Eigenschaft wird von der benutzerdefinierten URL festgelegt.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung	Beheben
Sie können glide.proxy.host nicht ändern. Diese Eigenschaft wird von der benutzerdefinierten URL festgelegt.	
Der CNAME-Datensatz für<custom_domain> zeigt nicht auf<base.service-now.com> .	Die Konfiguration auf der URL-Anbieterseite ist nicht korrekt. Überprüfen Sie Ihre Konfiguration im CNAME-Datensatz.
CNAME-Datensatz für fehlt<custom_domain> .	Der CNAME-Datensatz muss von Ihrem URL-Provider konfiguriert werden, bevor die benutzerdefinierte URL für Ihre Instanz festgelegt werden kann.

LDAP-Integration

Eine LDAP-Integration ermöglicht es Ihrer Instanz, Ihren vorhandenen LDAP-Server als primäre Quelle für Benutzerdaten zu verwenden.

Administratoren integrieren ein LDAP-Verzeichnis (Lightweight Directory Access Protocol), um den Benutzeranmeldungsprozess zu optimieren und administrative Aufgaben wie das Erstellen von Benutzern und das Zuweisen von Rollen zu automatisieren. Eine LDAP-Integration ermöglicht es dem System, Ihren vorhandenen LDAP-Server als primäre Quelle für Benutzerdaten zu verwenden. Normalerweise ist eine LDAP-Integration auch Teil einer Single Sign-on-Implementierung.

Die Integration verwendet die Anmeldeinformationen des LDAP-Servicekontos, um den eindeutigen Namen (Distinguished Name, DN) des Benutzers vom LDAP-Server abzurufen. Wenn der DN-Wert für den Benutzer angegeben ist, wird die Integration mit dem DN und dem Passwort des Benutzers erneut an LDAP gebunden. Das vom Benutzer eingegebene Passwort ist vollständig in der HTTPS-Sitzung enthalten. Die Integration speichert niemals LDAP-Passwörter.

Die Integration verwendet eine schreibgeschützte Verbindung, die nie in das LDAP-Verzeichnis schreibt. Die Integration fragt nur Informationen ab und aktualisiert dann die interne Datenbank entsprechend.

Hinweis:
Ausführliche Informationen zum Einrichten der Integration finden Sie unter Setup der LDAP-Integration.

Hinweis:
Wenn Ihre Instanz eine LDAP-Integration verwendet und die Active Directory-Einstellungen erfordern, dass Benutzer ihr Passwort bei der Anmeldung zurücksetzen, können sich Ihre Benutzer nicht bei der Instanz anmelden. Die Instanz kann das Active Directory-Passwort eines Anwenders nicht ändern.

Funktionen der LDAP-Integration

Zu den Funktionen der LDAP-Integration gehören die folgenden.

Geplante LDAP-Aktualisierung

Ein geplanter Scan Ihres LDAP-Servers wird normalerweise einmal pro Nacht ausgeführt. Sie fragt die Attribute aller zutreffenden Benutzerdatensätze ab und vergleicht sie mit dem Account auf unseren Servern. Wenn es einen Unterschied gibt, ändern wir unseren Benutzerdatensatz mit dem geänderten Attribut. Die Belastung des LDAP-Servers während der Aktualisierung hängt davon ab, wie viele Datensätze abgefragt werden und wie viele

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute verglichen werden. Wir empfehlen, die Aktualisierung außerhalb der Spitzenzeiten zu planen. Ein großer Aktualisierungsvorgang kann sich auf andere geplante Vorgänge auswirken, z. B. auf das Ausführen von Berichten, und sollte so geplant werden, dass Konflikte so gering wie möglich gehalten werden.

LDAP-Listener

Der LDAP-Listener ist unsere Version einer persistenten Abfrage (oder persistenten Suche). Wir geben eine ständige Abfrage für Änderungen an Ihrem LDAP-Server aus und lauschen ständig auf eine Antwort. Vorausgesetzt, Ihr Server unterstützt eine persistente Suche, werden alle an einem Ihrer zutreffenden LDAP-Konten vorgenommenen Änderungen an den LDAP-Listener zurückgegeben und innerhalb von etwa 10 Sekunden an Ihre Instanz gesendet. Dies ist ein äußerst nützliches Tool, mit dem wir nahezu in Echtzeit eine Kopie der Account-Details Ihrer Anwender erhalten, ohne auf die nächste geplante Aktualisierung warten zu müssen.

LDAP-Anmeldung bei Bedarf

Nachdem eine LDAP-Integration eingerichtet wurde, kann die Instanz neuen Benutzern erlauben, sich beim System anzumelden, auch wenn sie noch kein Konto in der Instanz haben. Wenn ein neuer Benutzer versucht, sich bei der Instanz anzumelden, prüft die Integration, ob dieser Benutzer über ein Konto in der Instanz verfügt. Wenn die Integration kein vorhandenes Benutzerkonto findet, wird der eingegebene Benutzername automatisch vom LDAP-Server abgefragt. Wenn ein passender LDAP-Account gefunden wird, versucht die Integration, sich mit dem vom Benutzer eingegebenen Passwort zu authentifizieren. Wenn das Passwort gültig ist, erstellt die Instanz einen Account für den Benutzer, füllt den Account mit allen zutreffenden LDAP-Informationen und meldet den Benutzer bei der Instanz an.

Bei der Anmeldung bei Bedarf wird die LDAP-Benutzerimport-Transformationszuordnung verwendet. Weitere Informationen zu Anforderungen für Transformationszuordnungen finden Sie unter LDAP-Transformationszuordnungen.

LDAP-Datenauffüllung

Hinweis:
Die in dieser Integration beschriebene Funktionalität ist standardmäßig nicht verfügbar. Diese Integration umfasst eine Anpassung nach der Bereitstellung, die von einem erfahrenen Administrator oder von ServiceNow professionellen Serviceberatern durchgeführt wird.

Eine Integration mit den LDAP-Servern ermöglicht es Ihnen, die Datenbank der Instanz schnell und einfach mit Benutzerdatensätzen aus der vorhandenen LDAP-Datenbank zu füllen. Um Dateninkonsistenzen zu vermeiden, können Sie eingehende LDAP-Datensätze erstellen, ignorieren oder überspringen.

Sie können auch die Daten begrenzen, die die Integration importiert, indem Sie LDAP-Attribute angeben, sodass nur die Daten importiert werden, die Sie für eine Instanz verfügbar machen möchten. Normalerweise werden die von Ihnen angegebenen LDAP-Attribute Teil der Integrationstransformationszuordnung. Wenn Sie keine LDAP-Attribute angeben, importiert die Integration alle verfügbaren Objektattribute vom LDAP-Server. Die Instanz speichert importierte LDAP-Daten in temporären Import Set-Tabellen. Je mehr Attribute Sie importieren, desto länger ist die Importzeit. Weitere Informationen finden Sie unter Geben Sie die LDAP-Attribute an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Authentifizierung

Verwenden Sie die LDAP-Authentifizierung für den Zugriff mit LDAP-Anmeldeinformationen.

Wenn ein Benutzer auf der Anmeldeseite Netzwerkanmeldeinformationen eingibt:

1. Die Instanz übergibt die Anmeldeinformationen an einen LDAP-Server, um die Instanz zu finden.
2. Bei RDNs wird die DN-Zeichenfolge des Benutzers validiert. Sie validiert nur, ob für mindestens eine der LDAP-OU-Konfigurationen mit `table=sys_user` ein RDN konfiguriert ist.
3. Der LDAP-Server antwortet mit einer autorisierten oder nicht autorisierten Nachricht, anhand derer das System bestimmt, ob der Zugriff gewährt werden soll.

Durch die Authentifizierung bei Ihrem LDAP-Server greifen Benutzer mit denselben Anmeldeinformationen auf die Plattform zu, die sie für andere interne Ressourcen in Ihrer Netzwerkdomäne verwenden. Außerdem können Sie vorhandene Passwörter und Sicherheitsrichtlinien wiederverwenden, die bereits vorhanden sind. Beispielsweise verfügt der LDAP-Server möglicherweise bereits über Richtlinien für Kontosperrung und Passwortablauf.

Wenn Sie LDAP aktivieren, aktualisiert das System Benutzerdatensätze mit diesen Feldern.

LDAP-Benutzerdatensatz aktualisiert

Feld	Beschreibung
Quelle	Gibt an, ob LDAP zur Validierung eines Benutzers verwendet wird. Wenn die Quelle mit ldap beginnt, wird der Benutzer über LDAP validiert. Wenn die Quelle nicht mit ldap beginnt, wird das Passwort im Benutzerdatensatz verwendet, um den Benutzer bei der Anmeldung zu validieren.
LDAP-Server	Gibt an, welcher LDAP-Server den Benutzer authentifiziert, wenn mehrere LDAP-Server vorhanden sind.

Hinweis:
Das System unterstützt keine LDAP-Passwortauthentifizierung über einen MID-Server. Eine Instanz muss in der Lage sein, eine direkte Verbindung mit einem LDAP-Server herzustellen, um die Passwortauthentifizierung zu unterstützen.

Grundlegendes zur LDAP-Integration

Eine LDAP-Integration ermöglicht es Ihrer Instanz, Ihren vorhandenen LDAP-Server als primäre Quelle für Benutzerdaten zu verwenden.

Voraussetzungen für die LDAP-Integration

- Der Verzeichnisdienstserver muss LDAP v3-konform sein
- Eingehender Netzwerkzugriff durch die Firewall muss zulässig sein (an den LDAP-Server).
- Externe IP oder Name des LDAP-Servers
- Benutzeranmeldeinformationen mit schreibgeschütztem Zugriff
- Für LDAPS ein PKI-Zertifikat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Timing der LDAP-Integration

LDAP-Integrationen werden normalerweise vor dem Go-Live der Instanz durchgeführt, können jedoch jederzeit integriert werden.

Datenintegrität des LDAP-Servers

Einige Benutzer befürchten, dass ein Dritter (in diesem Fall die Instanz) Änderungen (Schreibvorgang) an Ihrem LDAP-Server vornimmt. Bei einer LDAP-Integration schreibt Ihre Instanz nicht in das interne LDAP-Verzeichnis. Die Instanz fragt Informationen ab und aktualisiert ihre Datenbank entsprechend.

Am internen LDAP-Server werden von der Instanz keine Änderungen vorgenommen. Das Servicekonto ist schreibgeschützt.

Die meisten Änderungen (einschließlich Ergänzungen) an Ihrem LDAP-Server sind innerhalb von Sekunden für die Instanz verfügbar, je nachdem, wie viele Komponenten der vollständigen LDAP-Integration vorhanden sind.

Um die Synchronisierung der LDAP-Datensätze zu gewährleisten, planen Sie einen regelmäßigen Scan des LDAP-Servers, um Änderungen zu erfassen.

Die Instanz synchronisiert keine Abteilungsdatensätze. Benutzer und Gruppenmitgliedschaften werden durch den LDAP-Listener-Mechanismus und eine tägliche vollständige LDAP-Suche auf dem neuesten Stand gehalten, aber die Instanz löscht keine dieser Einträge, nachdem sie aus LDAP entfernt wurden.

Wenn ein Eintrag gelöscht werden soll, wird auch der gesamte Verlauf gelöscht, und alle Verweise darauf werden gelöscht. Konfigurationselemente (CIs), SLA-Vereinbarungen, Softwarelizenzen, Bestellungen und Servicekatalogeinträge haben alle einen Verweis auf die Abteilung. Wenn die Abteilung gelöscht wird, werden diese Verweise gelöscht. Es gibt viele Verweise auf Benutzer. Wenn ein Benutzer gelöscht wird, geht der gesamte Verlauf der Aktionen dieses Benutzers verloren. Derzeit liegt die Entscheidung, ob gelöscht wird oder nicht, bei unseren Kunden.

Sicherheit

Die Verbindung wird von einem einzelnen Computer mit einer festen IP-Adresse über einen bestimmten Port in Ihrer Firewall hergestellt. Die Authentifizierung erfolgt mit einem schreibgeschützten LDAP-Konto Ihrer Wahl. Sie können Standard-LDAP verwenden oder die öffentliche Seite eines in Ihrem Verzeichnis installierten SSL-Zertifikatsladen. In diesem Fall können wir LDAPS verwenden. Um eine weitere Sicherheitsebene hinzuzufügen, bieten wir auch die Option eines Punkt-zu-Punkt-IPSEC-VPN-Tunnels an. Wenden Sie sich an Ihren Account Manager, um Einzelheiten und Preise zu erfahren.

Sichere LDAP-Verbindungen

Verbindung	Beschreibung
MID-Server	Um Ihren LDAP-Server vor externem Netzwerkdatenverkehr zu schützen, installieren Sie einen MID-Server im lokalen Netzwerk, und konfigurieren Sie das System so, dass die Kommunikation mit dem MID-Server über einen sicheren Kanal erfolgt.
LDAPS	Um eine verschlüsselte LDAPS-Verbindung herzustellen, laden Sie die öffentliche Seite des SSL-Zertifikats Ihres LDAP-Servers. Die Integration verwendet das Zertifikat, um die gesamte Kommunikation zwischen dem LDAP-Server und der Instanz zu verschlüsseln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichere LDAP-Verbindungen (Fortsetzung)

Verbindung	Beschreibung
VPN	Wenn Sie den LDAP-Server mit einem verschlüsselten Punkt-zu-Punkt-IPSEC-VPN-Tunnel sichern möchten, wenden Sie sich an Ihren Account Manager, um Einzelheiten und Preise zu erfahren.

Ein weiterer zu berücksichtigender Sicherheitsaspekt sind die in einer LDAP-Integration freigegebenen Daten. Um die für Ihre Instanz verfügbar gemachten Daten zu begrenzen, geben Sie Attribute in Ihrer Transformationszuordnung an. Weitere Informationen finden Sie unter LDAP-Transformationszuordnungen.

LDAP-Daten werden in die Instanz importiert

Es wird empfohlen, Attribute so zu definieren, dass nur die erforderlichen Daten importiert werden. Definierte Attribute werden der Instanzbenutzerdatenbank zugeordnet.

Wir können die Frage, welche spezifischen Attribute benötigt werden, nicht beantworten, da dies vom Umfang des Projekts und den Geschäftsanforderungen abhängt.

Unterstützte Typen von LDAP-Servern

Die Instanz wurde erfolgreich in Microsoft Active Directory, Novell, Domino (lotus Notes) und Open LDAP integriert. Wir verwenden JNDI als Schnittstelle zum LDAP-Server. Solange Ihr LDAP-Server LDAP v3-konform ist, ist die Integration erfolgreich.

LDAP Single Sign-on

Neben der mit dem LDAP-Import bereitgestellten Datenauffüllungsfunktion können Sie die von der Anwendung unterstützte Funktion „Externe Authentifizierung“ verwenden, um zu verhindern, dass sich Ihre Benutzer jedes Mal neu anmelden müssen.

Mehrere LDAP-Domänen

Die empfohlene Methode für die Verarbeitung mehrerer Domänen besteht darin, für jede Domäne einen separaten LDAP-Serverdatensatz zu erstellen. Jeder LDAP-Serverdatensatz muss auf einen Domänencontroller für diese Domäne verweisen. Das bedeutet, dass das lokale Netzwerk Verbindungen zu jedem der Domänencontroller zulassen muss.

Nach der Erweiterung auf mehr als eine Netzwerkdomäne ist es wichtig, dass Sie eindeutige LDAP-Attribute für die Anwendungsbenutzernamen identifizieren und Zusammenfügungswerte importieren. Ein allgemeines eindeutiges Zusammenfügungsattribut für Active Directory ist objectSid. Eindeutige Benutzernamen können je nach LDAP-Datendesign variieren. Allgemeine Attribute sind email oder userPrincipalName.

Umgang mit Abfragelimits

Standardmäßig hat Active Directory 2000/2003 ein LDAP-Abfragelimit (maxPageSize) von 1000 Objekten, um übermäßige Lasten und Denial-of-Service-Angriffe zu verhindern. Wir haben zwei Methoden, um mit dieser Grenze umzugehen.

Die Standardmethode besteht darin, die Abfrage so aufzubrechen, dass weniger als 1000 Objekte gleichzeitig zurückgegeben werden. Fragen Sie beispielsweise nur Objekte ab, die mit dem Buchstaben „a“ beginnen, und fragen Sie dann „b“-Objekte ab. Die effizientere Methode für große Umgebungen besteht darin, Paging zu aktivieren. Paging wird

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

standardmäßig auf allen Microsoft Active Directory-Servern unterstützt. Die Ergebnisse werden automatisch in mehrere Ergebnismengen aufgeteilt, sodass die Abfrage nicht in mehrere Anforderungen aufgeteilt werden muss.

LDAP-Abfragetyp

Wenn ein LDAP-Passwort angegeben wird, wird eine einfache Bindung durchgeführt. Wenn kein LDAP-Passwort angegeben ist, wird „none“ verwendet. In diesem Fall muss der LDAP-Server die anonyme Anmeldung zulassen.

LDAP-Authentifizierung

Wir verwenden die bereitgestellten Servicekonto-Anmeldeinformationen für LDAP, um den Anwender-DN vom LDAP-Server abzurufen. Angesichts des DN-Werts für den Benutzer führen wir eine erneute Bindung mit LDAP durch, wenn der DN des Benutzers und das bereitgestellte Passwort angegeben werden.

Passwortspeicher

Das vom Benutzer eingegebene Passwort ist vollständig in seiner HTTPS-Sitzung enthalten. Wir speichern dieses Passwort nirgendwo.

LDAP-Authentifizierung einrichten

Diese Felder im Benutzerdatensatz beziehen sich auf LDAP:

- **Quelle**: Das Feld „Quelle“ gibt an, ob ein Benutzer mithilfe von LDAP validiert wird. Wenn das Quellfeld mit „ldap“ beginnt, wird der Anwender über LDAP validiert. Wenn das Feld „Quelle“ nicht mit „ldap“ beginnt, wird das Passwort im Benutzerdatensatz verwendet, um den Benutzer bei der Anmeldung zu validieren.
- **LDAP-Server**: Die Instanz unterstützt mehrere LDAP-Server, daher bestimmt das Feld LDAP-Server, welcher Server zur Authentifizierung des Benutzers verwendet werden soll.

Anforderungen für die LDAP-Integration

Überprüfen Sie die Anforderungen für die LDAP-Integration, einschließlich eines PKI-Zertifikats und eines LDAP-konformen Verzeichnisdienstservers.

Die LDAP-Integration erfordert:

- Einen LDAP v3-konformen Verzeichnisdienstserver
  - Ermöglicht eingehenden Netzwerkzugriff durch die Firewall (an den LDAP-Server)
  - (Optional) Akzeptiert anonyme Anmeldung
  - (Optional) Unterstützt Paging für große LDAP-Abfragen
- Die externe IP-Adresse oder der vollständig qualifizierte Domänenname des LDAP-Servers. Sie können auch einen MID-Server verwenden.
- Ein schreibgeschütztes LDAP-Konto Ihrer Wahl
- Für mehrere Domänen: Netzwerkzugriff für jeden Domänencontroller
- Für LDAPS ein PKI-Zertifikat
- Für LDAP-Listener ein Microsoft Active Directory-Server, der persistente Abfragen (ADNotify) unterstützt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte LDAP-Server

Unter Verwendung von *JNDI* als Schnittstelle mit dem LDAP-Server wurde die Instanz erfolgreich in die folgenden Server integriert:

- Microsoft Active Directory
- Novell
- Domino (lotusische Notizen)
- Öffnen Sie LDAP

LDAP-Abfragelimits

Standardmäßig hat Active Directory 2000/2003 ein LDAP-Abfragelimit (maxPageSize) von 1000 Objekten, um übermäßige Lasten und Denial-of-Service-Angriffe zu verhindern. Das System verfügt über zwei Methoden, um mit diesem Grenzwert umzugehen.

- Die Standardmethode besteht darin, die Abfrage so aufzuteilen, dass weniger als 1000 Objekte gleichzeitig zurückgegeben werden. Fragen Sie beispielsweise nur Objekte ab, die mit dem Buchstaben „a“ beginnen, und fragen Sie dann „b“-Objekte ab.
- Die effizientere Methode für große Umgebungen besteht in der Aktivierung von Paging, das standardmäßig auf allen Microsoft Active Directory-Servern unterstützt wird. Paging teilt die Ergebnisse automatisch in mehrere Ergebnissätze auf, sodass die Integration die Abfrage nicht in mehrere Anforderungen aufteilen muss.

Setup der LDAP-Integration

Administratoren können die LDAP-Integration aktivieren, um die Anmeldung von Benutzern aus dem LDAP-Verzeichnis ihres Unternehmens zu ermöglichen.

LDAP verwendet normalerweise eine dieser Arten von Kommunikationskanälen.

LDAP-Kommunikationskanäle

Verbindung	Beschreibung	LDAP-Importunterstützung?	LDAP-Authentifizierungsunterstützung?
MID-Server-Verbindung	Kommuniziert standardmäßig über HTTP an Port 80. Dieser Kommunikationskanal erfordert kein Zertifikat. Die Verbindung zwischen dem MID Server und der Instanz erfolgt über HTTPS (Port 443). Sie können den MID Server verwenden, um Daten über LDAP zu importieren, aber Sie können den MID Server nicht für die LDAP-Authentifizierung verwenden. Fahren Sie mit Definieren des LDAP-Servers fort.	Ja	Nein
Standard-LDAP-Integration	Kommuniziert standardmäßig über TCP an Port 389. Dieser Kommunikationskanal	Ja	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Kommunikationskanäle (Fortsetzung)

Verbindung	Beschreibung	LDAP-Importunterstützung?	LDAP-Authentifizierungsunterstützung?
	erfordert kein Zertifikat. Fahren Sie mit Definieren des LDAP-Servers fort.		
SSL-verschlüsselte LDAP-Integration (LDAPS)	Kommuniziert standardmäßig über TCP an Port 636. Dieser Kommunikationskanal erfordert ein Zertifikat. Fahren Sie mit Installieren Sie das LDAP X.509-SSL-Zertifikat fort, um das Zertifikat zu erhalten und hochzuladen.	Ja	Ja
VPN-Verbindung	Kommuniziert über einen IPSEC-Tunnel. Kaufen oder erstellen Sie einen IPSEC-Tunnel in Ihrem lokalen Netzwerk. Fahren Sie mit Definieren des LDAP-Servers fort.	Ja	Ja

Wenn Sie einen MID Server verwenden, stellt der MID Server eine Verbindung zur -Instanz her, und der MID Server stellt auch eine Verbindung zum LDAP-Server her. In beiden Fällen initiiert der MID Server die Verbindung:

1. Zuerst stellt der MID Server über LDAP an Port 389 eine Verbindung zum LDAP-Server her.
2. Anschließend initiiert der MID Server eine mit HTTPS verschlüsselte Verbindung zur Instanz an Port 443, um die Daten an die Instanz zu übertragen.

Weitere Informationen zu VPNs, MID-Servern und LDAP finden Sie unter Sie benötigen kein VPN Teil II in der Community.

Installieren Sie das LDAP X.509-SSL-Zertifikat

Sie können ein X.509-Zertifikat für Ihre LDAP-Integration installieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erwerben oder generieren Sie ein SSL-Zertifikat auf Ihrem LDAP-Server.
2. Navigieren zu **LDAP** > **Zertifikat** und klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus:

Feld	Beschreibung
Name	Der Zertifikatname.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablaufbenachrichtigung	Wählen Sie diese Option aus, um eine Benachrichtigung an die Benutzer zu senden, die im Feld Bei **Ablauf benachrichtigen** ausgewählt sind. Standardmäßig ist diese Option aktiviert.
Benachrichtigung bei Ablauf	Wählen Sie die Benutzer aus, die die Benachrichtigung über den Ablauf des Zertifikats erneut aktivieren sollen. Wenn keine Benutzer ausgewählt sind, wird standardmäßig der angemeldete Benutzer zusammen mit den letzten beiden angemeldeten Benutzern mit der Administratorrolle hinzugefügt.
Tage vor Ablauf benachrichtigen	Die Anzahl der Tage vor Ablauf, an denen die Instanz die Benachrichtigung sendet. Geben Sie einen Wert von mindestens 20 ein. Für Instanzen, die auf Istanbul und spätere Releases aktualisiert wurden, wird dieser Wert auf 20 festgelegt, sofern kein höherer Wert angegeben ist.
Aktiv	Eine Checkbox, die angibt, dass dieses Zertifikat aktiv ist.
Format	Das Format des Zertifikats.
Typ	Der Zertifikatcontainer. Die Instanz erkennt Zertifikate aus Truststores, Java-Schlüsselspeichern und PKCS#12-Schlüsselspeichern.
Gültig ab	Die Instanz fügt diesem Feld automatisch das Zertifikat „Gültig ab“-Datum hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft ab	Die Instanz fügt diesem Feld automatisch das Zertifikat-Ablaufdatum hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft in Tagen ab	Die berechnete Anzahl von Tagen bis zum Ablauf.
Kurzbeschreibung	Eine Beschreibung für das Zertifikat.
Bearbeiter	Die Instanz fügt den Zertifikataussteller automatisch diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Betreff	Die Instanz fügt den Antragsteller des Zertifikats automatisch diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
PEM-Zertifikat	Geben Sie den Wert des X509-Zertifikats ein.

Hinweis:
Die Integration signiert derzeit das Zertifikat in der Kommunikation zwischen der Instanz und dem IdP nicht.

4. Klicken Sie auf **Speichern**.

Nächste Maßnahme
Klicken Sie auf **Speicher/Zertifikate validieren**, um den Truststore und das Zertifikat zu testen.

Definieren Sie einen LDAP-Server

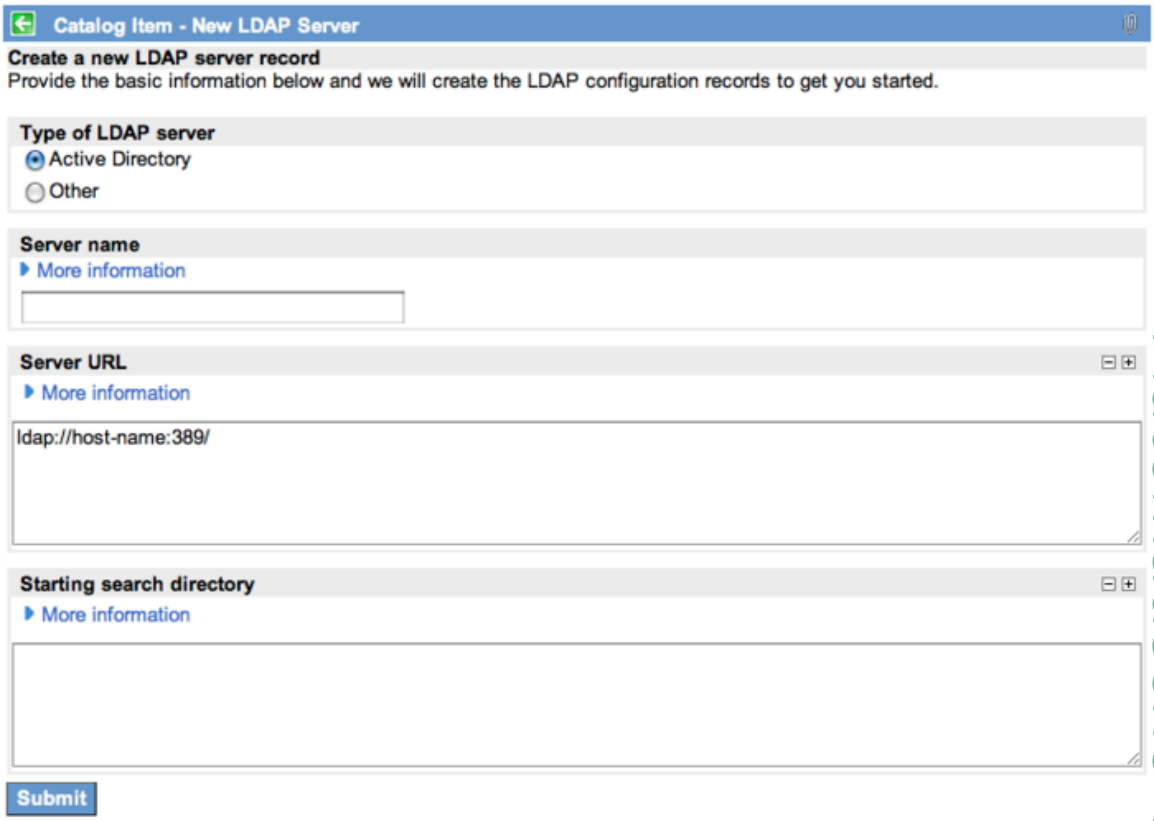
Erstellen Sie einen neuen LDAP-Serverdatensatz in der -Instanz.

Vorbereitungen
Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **Neuen Server erstellen**.
2. Füllen Sie die Formularfelder aus.



Im Feld **Server-URL** werden die gültigen URLs aller Server durch ein Leerzeichen getrennt angezeigt. Server werden zuerst nach Betriebsstatus **sortiert**, wobei Server mit dem Status In Betrieb zuerst und dann nach dem von Ihnen angegebenen Wert für die **Reihenfolge** sortiert werden. Der zuerst aufgeführte Server ist der primäre LDAP-Server. Die anderen sind redundante Server.

Hinweis:
Zwischen der Änderung des tatsächlichen Betriebsstatus und der Anzeige tritt eine geringfügige Verzögerung auf.

Alternativ können Sie einen redundanten LDAP-Server hinzufügen, indem Sie zu einem vorhandenen LDAP-Server-Datensatz navigieren und eine Zeile in die eingebettete Liste der LDAP-Server-URLs einfügen.

3. Klicken Sie auf **Absenden**.

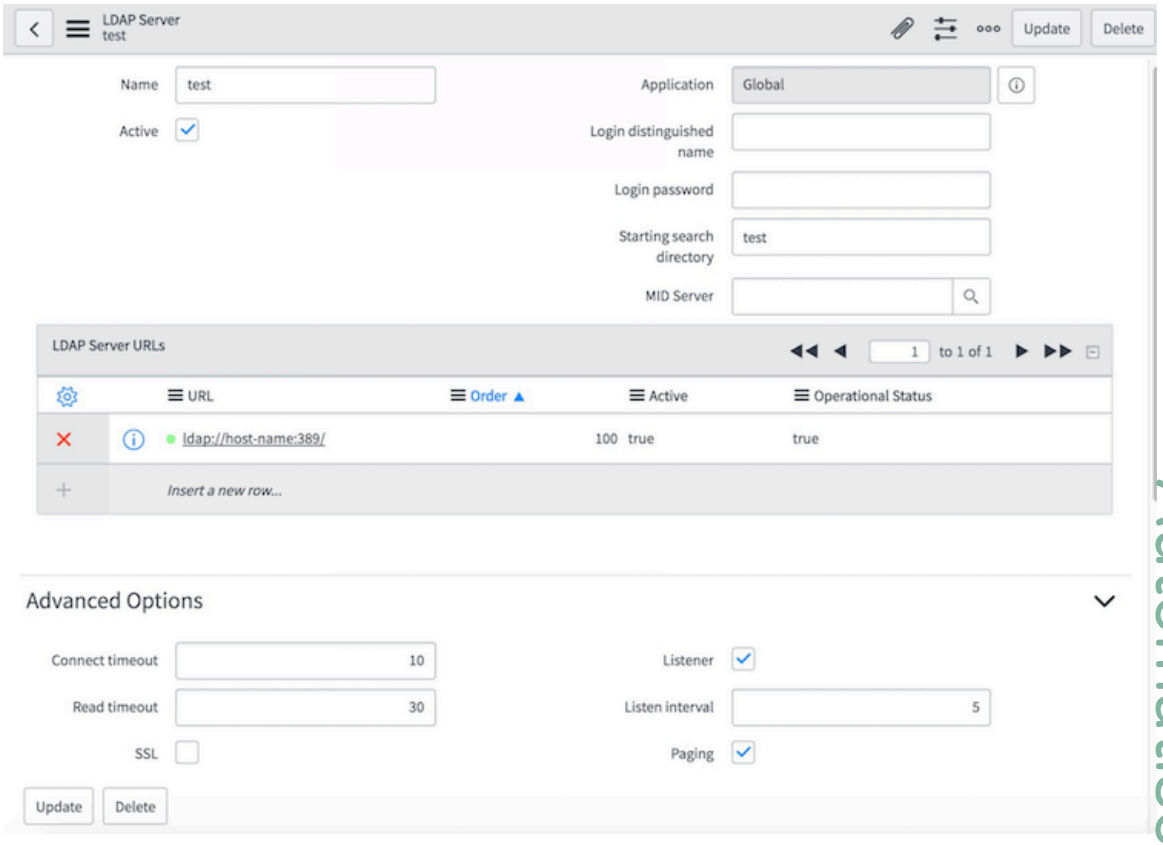
Hinweis:
Sie können auch einen vorhandenen LDAP-Server-Datensatz ändern, indem Sie zu navigieren **System-LDAP** > **LDAP-Server** und die erforderlichen Änderungen vornehmen.

4. Nehmen Sie nach Bedarf Änderungen an den Feldern vor.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „LDAP-Server“.



Feld	Beschreibung
Name	Geben Sie den Namen des Servers ein.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, wenn der Server aktiv ist.
LDAP-Server-URLs	Geben Sie die URLs der primären und der Sicherungs-LDAP-Server ein. Server werden zuerst nach Betriebsstatus sortiert, wobei Server mit dem Status In Betrieb zuerst und dann nach dem von Ihnen angegebenen Wert für die Reihenfolge sortiert werden. Der zuerst aufgeführte Server ist der primäre LDAP-Server. Die anderen sind redundante Server.
Server-URL	Geben Sie die URL des Servers ein. Konfigurieren Sie das Formular, um dieses Feld bei Bedarf hinzuzufügen. Es handelt sich um ein berechnetes schreibgeschütztes Feld, das die Liste der LDAP-Server anzeigt, die Sie auch im Feld **LDAP-Server-URLs** sehen können, getrennt durch ein Leerzeichen und geordnet nach Betriebsstatus und den Reihenfolgenwerten der URLs.
Eindeutiger Anmeldename	Geben Sie den eindeutigen Namen (Distinguished Name, DN) des Benutzers ein, der die LDAP-Verbindung authentifiziert. Für den Zugriff auf einen LDAP-Verzeichnisserver muss der Benutzername das vollständige Format des eindeutigen Namens aufweisen: servicenow@service-now.com
Anmeldepasswort	Geben Sie das Passwort des Servers ein.
Suche im Verzeichnis wird gestartet	Geben Sie den relativen eindeutigen Namen (RDN) des Standardsuchverzeichnisses ein. Alle Abfragen an diesen LDAP-Server werden von diesem RDN gestartet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	Wählen Sie den MID Server aus, den Sie für die Verbindung mit dem LDAP-Server verwenden möchten. Wenn Sie einen MID Server zum Herstellen einer LDAP-Verbindung verwenden, müssen Sie den LDAP-Server keinem externen Netzwerkdatenverkehr aussetzen. Außerdem muss kein VPN-Tunnel zwischen Ihrem LDAP-Server und den ServiceNow -Rechenzentren eingerichtet werden. **Hinweis:** ◦ Der MID Server-Benutzer muss über die Rolle user_admin verfügen, um LDAP-Server-Konfigurationsdatensätze lesen zu können. ◦ Folgendes ist mit dem MID Server nicht verfügbar: ▪ LDAP-Authentifizierung ▪ SSL-Verbindung
Connect-Zeitüberschreitung	Wenn ein MID Server konfiguriert ist, wird die Verbindung unabhängig von dieser Einstellung nach 10 Sekunden beendet. Diese Einstellung ist hartcodiert und kann nicht geändert werden.
Zeitüberschreitung beim Lesen	Geben Sie an, wie viele Sekunden die Integration LDAP-Daten lesen muss. Die Integration beendet das Lesen von LDAP-Daten, nachdem die Verbindung die Zeitüberschreitung beim Lesen überschritten hat. Wenn Sie eine SSL-Verbindung aktivieren, können Sie mit der Systemeigenschaft`com.glide.ssl.read.timeout`auch einen Zeitüberschreitungswert für das Lesen festlegen. Wenn Sie Zeitüberschreitungswerte für dieses Feld und die Systemeigenschaft eingeben, hat der niedrigste Zeitüberschreitungswert Vorrang.
SSL	Aktivieren Sie diese Checkbox, damit der LDAP-Server eine SSL-verschlüsselte Verbindung herstellen muss. Wenn Sie einen MID Server ausgewählt haben, ist dieses Feld nicht verfügbar. Wenn Sie eine LDAPS-Integration verwenden und der Standard-SSL-Port 636 ist, ist keine weitere Konfiguration erforderlich. SSL wird automatisch aktiviert. Wenn die LDAPS-Integration einen anderen SSL-Port verwendet, definieren Sie die alternativen SSL-Verbindungseigenschaften. **Hinweis:** Stellen Sie sicher, dass ein Netzwerkadministrator die lokale Firewall so konfiguriert, dass der Anwendungsserver auf den LDAP-Server zugreifen kann. Wenn sich der LDAP-Server in einem internen Netzwerk befindet, leitet die Firewall die IP-Adresse des Anwendungsservers durch die Firewall an den richtigen Port weiter (oder NATs).
Listener	Aktivieren Sie dieses Kontrollkästchen, damit die Integration regelmäßig Microsoft Active Directory-Server oder LDAP-Server abfragt, die die Steuerung persistenter Suchanforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	unterstützen. Wenn Sie einen MID Server ausgewählt haben, ist die Listener-Funktionalität für diesen MID Server verfügbar. Weitere Informationen finden Sie unter Aktivieren Sie einen LDAP-Listener, und legen Sie Systemeigenschaften fest.
Listenintervall (Zeitüberschreitungswert)	Geben Sie den Listener-Zeitüberschreitungswert in der Anzahl der Minuten an, in denen die Integration bei jeder Verbindung auf LDAP-Daten lauscht. Die Integration beendet das Abhören von LDAP-Daten, nachdem die Verbindung das Abhörintervall überschritten hat.
Paging	Aktivieren Sie diese Checkbox, damit der LDAP-Server LDAP-Attributdaten in mehrere Ergebnissätze aufteilt, anstatt mehrere Abfragen zu senden.

Hinweis:
Wenn Sie ein LDAP-Passwort angeben, führt die Integration einen Simple Bind-Vorgang durch. Wenn Sie kein LDAP-Passwort angeben, muss der LDAP-Server die anonyme Anmeldung zulassen, oder die Integration kann keine Verbindung zum LDAP-Server herstellen.

Ergebnisse

Wenn ein LDAP-Server-Datensatz auf „Aktiv“ gesetzt ist, testet das System automatisch jede Verbindung, um sie zu validieren.
Validierungen umfassen:

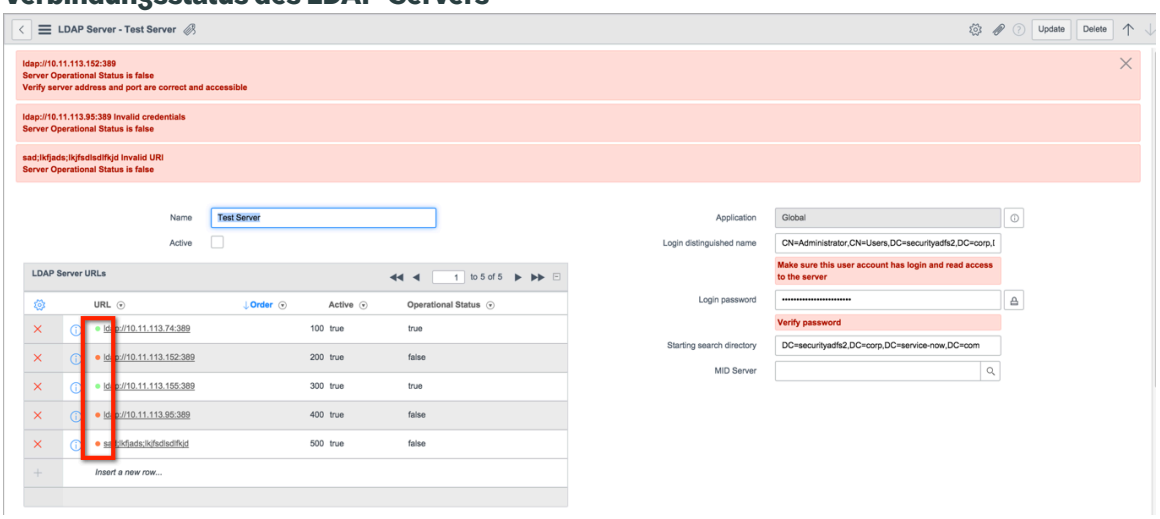
- Der LDAP-Server ist über die angegebene URL und den angegebenen Port zugänglich
- Die LDAP-Server-URL ist ordnungsgemäß formatiert
- Die Anmeldeinformationen sind gültig

Ab dem Fuji-Release zeigt das System farbige Punkte neben jeder Server-URL an:

Symbole für LDAP-Serververbindung

Farbe	Beschreibung
Grün	Der Server, sofern aktiv und betriebsbereit.
Grau	Der Server ist weder aktiv noch betriebsbereit.
Rot	Der Server ist aktiv, aber nicht betriebsbereit.

Verbindungsstatus des LDAP-Servers



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie einen LDAP-Listener, und legen Sie Systemeigenschaften fest

Das Aktivieren eines Listeners ist optional. Wenn diese Option aktiviert ist, benachrichtigt ein Listener das System, LDAP-Datensätze zu verarbeiten, sobald eine Aktualisierung auf dem LDAP-Server vorliegt.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Ein *Listener* ist ein dedizierter Prozess, der regelmäßig nach Änderungen auf dem LDAP-Server sucht.

Der Listener kann auf einem Microsoft Active Directory-Server bereitgestellt werden, der persistente Abfragen (ADNotify) unterstützt, oder auf einem LDAP-Server, der die Steuerung persistenter Suchanforderungen unterstützt (mit OID 2.16.840.1.113730.3.4.3).

Wenn der LDAP-Server eine persistente Suche unterstützt, erkennt der LDAP-Listener alle Benutzer- und Gruppenänderungen, die an einem der entsprechenden LDAP-Konten vorgenommen werden, und leitet sie innerhalb von etwa 10 Sekunden an Ihre Instanz weiter. Dadurch kann die Instanz nahezu in Echtzeit eine Kopie der Account-Details Ihrer Benutzer erhalten, ohne auf die nächste geplante Aktualisierung warten zu müssen. Der LDAP-Listener kann nur Objekte synchronisieren, die den Tabellen „Benutzer“ [sys_users] und „Gruppe“ [sys_user_group] zugeordnet sind.

Hinweis:
Wenn ein Benutzer über den Listener hinzugefügt wird, der Benutzer jedoch die durch den OE-Filter definierten Anforderungen nicht erfüllt, ignoriert die Instanz den Datensatz auf dem LDAP-Server. Wenn die Kriterien erfüllt sind, wird der Benutzer der Instanz hinzugefügt.

So aktivieren Sie einen Listener:

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. Aktivieren Sie das Kontrollkästchen **Listener**.
4. Klicken Sie auf **Aktualisieren**.

Hinweis:

Das System importiert nur Benutzerdatensätze, die dem LDAP-OE-Filter entsprechen. Eingehende Benutzerdatensätze, die die Filteranforderungen nicht erfüllen, werden als ungültig gekennzeichnet und vom Import ignoriert. Administratoren können die ausführliche LDAP-Protokollierung aktivieren, um festzustellen, ob eingehende Datensätze nicht mit dem LDAP-OU-Filter übereinstimmen.

5. **Wahlweise:** Navigieren Sie zur Tabelle „Systemeigenschaften“ [sys_properties], und legen Sie die Systemeigenschaften für LDAP-Listener fest.

Eigenschaften des LDAP-Listeners

Eigenschaft	Beschreibung
glide.ldap.listener.use_background_transaction	Bei „true“ wird der LDAP-Listener als Hintergrundtransaktion gestartet. Durch die Ausführung des LDAP-Listeners als Hintergrundtransaktion ka

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Transaktion durch die Kontingentregel „LDAP-Listener-Start/-Stopp-Transaktion“ nach Erreichen der maximalen Dauer (standardmäßig 5 Min abgebrochen werden. Dieses Verhalten verhindert, dass ein LDAP-Listene unbegrenzt wartet. **Hinweis:** Diese Eigenschaft gilt nur für LDAP-Verbindungen, die keinen MID Server verwenden. Verwenden Sie `glide.ldap.listener.mid.use_background_transac` um das Verhalten von LDAP-Verbindungen zu steuern, die über eine MID Server durchlaufen werden. ○ Typ: Wahr | Falsch ○ Standardwert: false ○ Speicherort: zu Tabelle „Systemeigenschaften“ [sys_prope hinzufügen
glide.ldap.listener.mid.use_background_transaction	Bei „true“ wird der LDAP-Listener als Hintergrundtransaktion gestartet. D die Ausführung des LDAP-Listeners als Hintergrundtransaktion kann die Quotenregel MID-Transaktion Start/Stopp des LDAP-Listeners die Transa abbrechen, nachdem die maximale Dauer erreicht ist (standardmäßig 5 Minuten). Dieses Verhalten verhindert, dass ein LDAP-Listener unbegren wartet. **Hinweis:** Diese Eigenschaft gilt nur für LDAP-Verbindungen, die einen MID Server verwenden. Verwenden Sie `glide.ldap.listener.use_background_transaction` das Verhalten von LDAP-Verbindungen zu steuern, die nicht über ei MID Server geleitet werden. ○ Typ: Wahr | Falsch ○ Standardwert: false ○ Speicherort: zu Tabelle „Systemeigenschaften“ [sys_prope hinzufügen
glide.ldap.listener.mid.one_listener	Bei „true“ wird nur eine einzelne ECC-Warteschlangennachricht erstellt, u den LDAP-Listener über einen MID-Server zu starten oder zu stoppen. Be „false“ können mehrere ECC-Warteschlangennachrichten erstellt werden, zur Erstellung mehrerer Threads zum Starten oder Stoppen des LDAP-Lis führt. ○ Typ: Wahr | Falsch ○ Standardwert: true ○ Speicherort: zu Tabelle „Systemeigenschaften“ [sys_prope hinzufügen

Geben Sie die LDAP-Attribute an

Geben Sie die in LDAP-Serverabfragen enthaltenen **Attribute** mithilfe des Felds LDAP-Serverattribute an. Dies kann sowohl die Leistung als auch die Sicherheit verbessern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

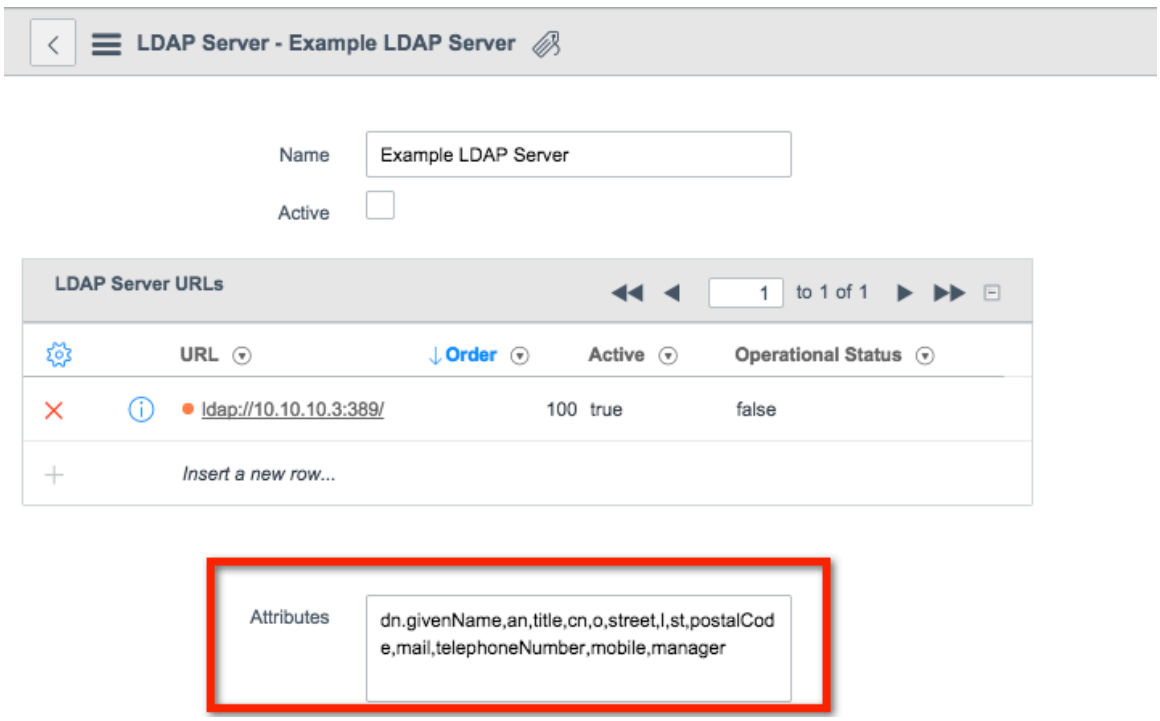
Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig lädt das System alle Attribute für jedes Objekt, für das es die Berechtigung zum Lesen von Ihrem LDAP-Server hat. Mit dem Feld **Attribute** können Sie die von der LDAP-Abfrage zurückgegebenen Attribute angeben und dadurch einschränken. Die Verwendung dieses Ansatzes für große LDAP-Importe kann die Geschwindigkeit dieser Importe erheblich verbessern.

Prozedur

Definieren Sie Attribute nach Möglichkeit explizit.

Wenn Informationen vorhanden sind, die der Instanz nicht zugänglich gemacht werden sollen, schließen Sie das Attribut aus. Wenn Sie keine LDAP-Serverattribute angeben, können Benutzertransaktionen für längere Zeiträume einfrieren, wenn neue Attribute zu einem LDAP-Serverobjekt hinzugefügt werden, da das System mit dem Laden von Daten aus den neuen Attributen ausgelastet ist.

Hinweis:
Um die in Transformationszuordnung für LDAP-Daten auswählen oder erstellen beschriebenen Manager-Suchskripts zu verwenden, geben Sie **manager** und **dn** (Distinguished Name) im Feld **Attribute** an. Keines der Attribute muss Teil einer Transformationszuordnung sein.



Testen Sie eine LDAP-Verbindung

Die Instanz testet die Verbindung jedes Mal automatisch, wenn ein Benutzer das LDAP-Serverformular öffnet. Alternativ können Sie die Verbindung zum LDAP-Server manuell über das LDAP-Serverformular testen.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig werden Fehlermeldungen im LDAP-Serverformular angezeigt, wenn Probleme beim Herstellen der Verbindung mit dem LDAP-Server auftreten.

Hinweis:
Mitarbeiter können auch die Konnektivität zwischen der Instanz und dem LDAP-Server überprüfen. Wenden Sie sich an den technischen Support, um Unterstützung bei der Überprüfung der LDAP-Konnektivität zu erhalten.

So testen Sie eine Verbindung manuell:

Prozedur
1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**.
2. Wählen Sie den zu testenden LDAP-Server aus.
3. Klicken Sie unter **Zugehörige Links**auf **Verbindung testen**.
4. Klicken Sie unter **Zugehörige Links**auf **Durchsuchen**, um sicherzustellen, dass die entsprechende LDAP-Verzeichnisstruktur für das System sichtbar ist.
5. (Optional) Wenn die Verbindung erfolgreich hergestellt wurde, klicken Sie auf **Durchsuchen**, um die LDAP-Quellverzeichnisstruktur anzuzeigen, die für die Instanz sichtbar ist.

   Hinweis:
   Die Felder **Filter** und **RDN** auf der linken Seite des Durchsuchen-Fensters werden ignoriert, wenn Sie das Suchfeld auf der rechten Seite verwenden.

Ergebnisse
Die Instanz ändert den Betriebsstatus von LDAP-Servern abhängig vom Ergebnis des Verbindungstests.

- Wenn Ihre Instanz eine Verbindung zu einem Server herstellt, dessen **Betriebsstatus** den Wert **down**aufweist, wird der Wert für den **Betriebsstatus** automatisch in **up**geändert. Diese Funktionalität wird sowohl für automatische als auch für manuelle Verbindungstests unterstützt.
- Wenn keine Verbindung zu einem Server hergestellt werden kann, dessen **Betriebsstatus** den Wert **up**hat, wird der Wert des **Betriebsstatus** automatisch in **down**geändert. Diese Funktionalität wird nur für automatische Verbindungstests unterstützt, nicht für manuelle Tests.

Definieren von LDAP-Organisationseinheiten

Eine Definition der Organisationseinheit (OE) gibt die LDAP-Quellverzeichnisse an, die für die Integration verfügbar sind.

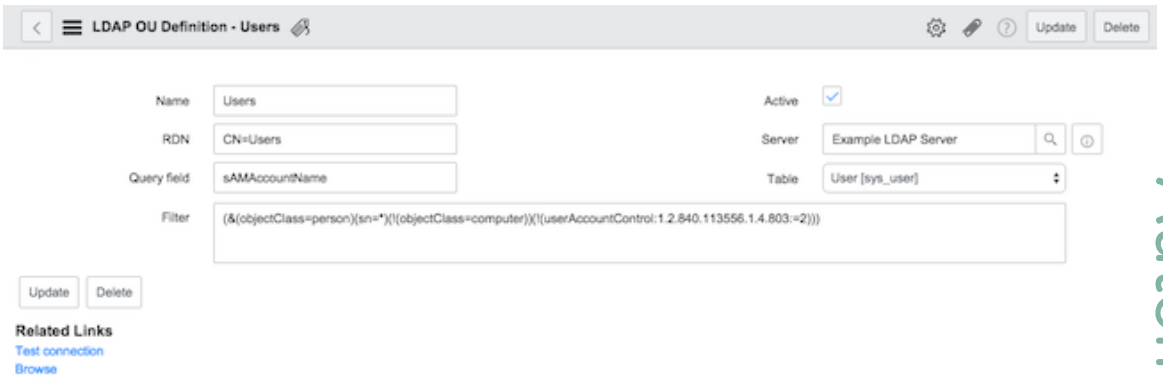
Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
OE-Definitionen können Standorte, Personen oder Benutzergruppen enthalten. Jede LDAP-Serverdefinition enthält zwei Beispiel-OU-Definitionen: eine für den Import von Gruppen in das System und eine für Benutzer.

Prozedur
1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie in der zugehörigen Liste **„LDAP-OE-Definitionen** “ entweder die Beispiel-OE-Definition **Gruppen** oder **Benutzer** aus.
4. Füllen Sie das Formular „LDAP-OU-Definition“ aus (siehe Tabelle).
5. Klicken Sie auf **Aktualisieren**.
   Das System testet automatisch die Verbindung zum LDAP-Server.
6. Klicken Sie unter **Zugehörige Links**auf **Durchsuchen**, um die von der OE-Definition zurückgegebenen LDAP-Verzeichnisdatensätze anzuzeigen.



Formular „OE-Definition“

Feld	Beschreibung
Name	Geben Sie den Namen an, den die Integration beim Verweisen auf diese OE verwendet. Der hier eingegebene Name wird zu einem LDAP-Ziel im Datenquellen-Datensatz.
RDN	Geben Sie den relativen eindeutigen Namen des Unterverzeichnisses an, das Sie durchsuchen möchten. Dieser RDN wird mit dem Startsuchverzeichnis aus der LDAP-Serverdefinition kombiniert, um das Unterverzeichnis zu identifizieren, das Informationen für diese Organisationseinheit enthält. Die Beispiel-OE-Definition verwendet beispielsweise den RDN-Wert `CN=Users`, um das LDAP-Verzeichnis `CN=Users,DC=service-now,DC=com` und ein beliebiges Verzeichnis darunter zu durchsuchen. Dieses Feld muss mit einem Unterverzeichnis in Ihrem LDAP-System übereinstimmen.
Abfragefeld	Geben Sie den Namen des Attributs auf dem LDAP-Server an, um Datensätze abzufragen. Das Abfragefeld muss sowohl in einzelnen als auch in mehreren Domäneninstanzen eindeutig sein. Um die besten Ergebnisse zu erzielen, verwenden Sie E-Mail-Adressen oder andere Anmeldeinformationen, die den Benutzer in einer Instanz mit mehreren Domänen eindeutig identifizieren. Active Directory verwendet das Attribut **sAMAccountName**. Andere LDAP-Server verwenden in der Regel das **cn-** Attribut. **Hinweis:** Das **Feld Abfrage** muss dem Feld Benutzer- **ID** in der Benutzertabelle [sys_user] zugeordnet werden. Beispiel: Wenn sich ein Active Directory-Benutzer als `joe.example` anmeldet, müssen ein Benutzerdatensatz mit dem Benutzer- **ID** -Wert von **joe.example** und ein LDAP-Datensatz mit dem **sAMAccountName** -Wert von **joe.example vorhanden sein**.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die OE-Definition zu aktivieren und Administratoren das Testen des Datenimports zu ermöglichen. Die Integration kann jedoch nur Daten aus aktiven OU-Definitionen in das System übernehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tabelle	Geben Sie die Tabelle an, die die zugeordneten Daten von Ihrem LDAP-Server empfängt. Wählen Sie für Benutzer **Benutzer (sys_user)**und für Gruppen **Gruppe (sys_group) aus**.
Filter	Geben Sie eine LDAP-Filterzeichenfolge ein, um bestimmte Datensätze auszuwählen, die aus der OE importiert werden sollen. Je spezifischer die LDAP-Filterabfrage ist, desto effizienter ist die Abfrage. Beispielsweise verwendet die LDAP-OU-Definition Benutzer den folgenden Filter, um Datensätze auszuwählen, die als Person klassifiziert sind, einen **sn** -Attributwert haben, keine Computer sind und nicht als inaktiv gekennzeichnet sind: `(&(objectClass=person)(sn=*)(!(objectClass=computer)) (!(userAccountControl:1.2.840.113556.1.4.803:=2)))` Eine Beschreibung der LDAP-Filtersyntax finden Sie, indem Sie im Internet nach `LDAP-Filter RFC`suchen.

Example: Beispiel für Definitionen von Organisationseinheiten

Angenommen, Sie haben einen LDAP-Server mit der folgenden Verzeichnisstruktur:

dc=meine-Domäne,dc=com

- ou = Gruppen
  - cn = Entwicklung
  - cn = HR
  - cn = Vertrieb
- ou = Benutzer
  - ou = Entwicklung
  - OU = HR
  - ou = Vertrieb

Angenommen, Sie möchten die HR-Gruppe und die HR-Benutzer aus der Anwendung ausschließen. Führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen LDAP-Serverdatensatz mit dem Startsuchverzeichnis dc=my-domain,dc=com.
2. Erstellen Sie einen OE-Definitionsdatensatz für ou=Groups mit einem Filter, um cn=HR auszuschließen.
3. Erstellen Sie einen OE-Definitionsdatensatz für ou=Users mit einem Filter, um ou=HR auszuschließen.

Wenn Sie keine zusätzlichen Attribute oder Filter mit einer OU-Definition angeben, gibt die LDAP-Abfrage die gesamte Unterstruktur aus dem Startverzeichnis und dem RDN zurück.

In diesen Beispielen hätte eine OU-Definition mit dem RDN-Wert ou=Groups und ohne Filter alle Gruppen zurückgegeben. Ebenso hätte eine OU-Definition mit dem RDN-Wert ou=Users und ohne Filter alle Benutzer und untergeordneten Organisationseinheiten zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Datenquelle für LDAP

Jede LDAP-Definition einer Organisationseinheit (OE) verfügt über eine eigene zugehörige Liste von Datenquellen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Sowohl der **LDAP-Server** als auch die **LDAP-OE-Definition** müssen aktiv sein, damit die Testladeaktion ordnungsgemäß funktioniert. Wenn die Testlast zum ersten Mal aktiviert wird, erfasst das System bis zu 20 Datensätze, um die Länge der Import Set-Felder zu bestimmen. Wenn die Stichprobendatensätze keine Werte für das Feld **Benutzer-ID** enthalten, legt das System die Feldlänge für alle nachfolgenden Importe auf die Standardlänge von 40 fest. Beim Import werden alle importierten Daten abgeschnitten, die die Feldlänge der Import Set-Tabelle überschreiten. Darüber hinaus wird das Feld **Benutzer-ID** auf maximal 40 Zeichen gekürzt. Beachten Sie, dass die 20 geladenen Datensätze nicht umgewandelt werden können und nur zu Testzwecken dienen. Wenn die Testdatensätze Werte für das Feld **Benutzer-ID** enthalten, wird die Feldlänge basierend auf der Feldlänge der längsten Benutzer-ID in den Testdatensätzen festgelegt.

So erstellen Sie eine neue Datenquelle:

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. Wählen Sie in der zugehörigen Liste „ **LDAP-OU-Definitionen** “ ein Element aus, z. B. **Gruppen** oder **Benutzer**.
4. Klicken Sie in der zugehörigen Liste „ **Datenquellen“** auf **Neu**.
5. Füllen Sie das Formular „Datenquelle“ aus (siehe Tabelle).
6. Klicken Sie auf **Absenden**.
7. Klicken Sie unter **Zugehörige Links**auf **Testladen von 20 Datensätzen**, um zu testen, ob die Datenquelle LDAP-Daten in die Importtabelle übernehmen kann.

Formular „Datenquellen“.

Feld	Beschreibung
Name	Geben Sie den Namen an, den die Integration beim Verweisen auf diese Datenquelle verwendet.
Tabellenname für Importsatz	Geben Sie den Namen der Staging-Tabelle ein, in der das System die importierten LDAP-Datensätze und -Attribute vorübergehend platziert. Überprüfen Sie diese Tabelle, um importierte LDAP-Datensätze anzuzeigen. Sie können denselben Import Set-Tabellennamen für alle LDAP-Datenquellen verwenden.
Typ	Wählen Sie **LDAP** aus, um anzugeben, dass es sich bei den importierten Daten um LDAP-Daten handelt. Nachdem Sie den Typ **LDAP**ausgewählt haben, wird im Formular das Feld **LDAP-Ziel** angezeigt.
LDAP-Ziel	Wählen Sie die LDAP-OE-Definition aus, die dieser Datenquelle zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Benutzer automatisch bereitstellen

Sie stellen automatisch Benutzer bereit, die sich auf dem LDAP-Server, aber noch nicht in Ihrer Instanz befinden.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

Erstellen Sie die folgenden Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties]:

LDAP-Eigenschaften

LDAP-Eigenschaft	Beschreibung
glide.ldap.authentication	Aktiviert die LDAP-Authentifizierung durch Verwendung von LDAP zum Authentifizieren von Benutzern. Legen Sie diese Eigenschaft auf „ **true** “ (Standardwert) fest.
glide.ldap.user.autoprovision	Aktiviert LDAP im System, um automatisch Benutzer in der Benutzertabelle [sys_user] zu erstellen, wenn der Benutzer in LDAP vorhanden ist, sich aber noch nicht in der Instanz befindet. Legen Sie diese Eigenschaft auf „ **true** “ (Standardwert) fest.

Beide Eigenschaften müssen auf „ **true** “ festgelegt werden, damit die automatische Bereitstellung funktioniert.

LDAP-Integration über MID Server

Administratoren können die Integration mithilfe einer LDAP-Datenquelle über einen MID Server (Management, Instrumentation, and Discovery) durchführen.

Der MID Server ermöglicht die Kommunikation und Bewegung von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services. Weitere Informationen zur Installation eines MID Servers finden Sie unter MID Server-Installation .

Wenn Sie einen MID Server zum Herstellen einer LDAP-Verbindung verwenden, müssen Sie den LDAP-Server keinem externen Netzwerkdatenverkehr aussetzen. Dadurch entfällt die Notwendigkeit, einen VPN-Tunnel zwischen Ihrem LDAP-Server und den Rechenzentren einzurichten. Der MID Server-Benutzer muss über die Rolle user_admin verfügen, um LDAP-Server-Konfigurationsdatensätze lesen zu können.

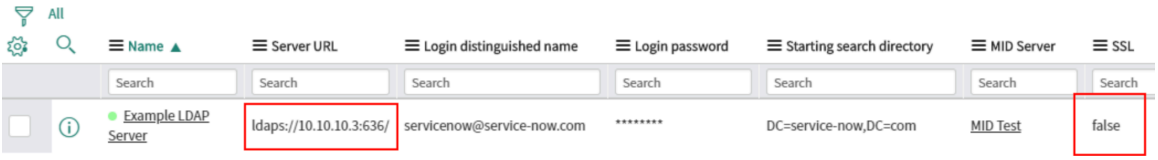
Hinweis:
Der MID Server lässt die Verwendung der UI-Aktion nicht zu<instance> `/sys_ui_action.do?sys_id=1b4f7ef30a0001060058e223c9a5744c`, um Benutzer- und Gruppendatensätze aus LDAP zu aktualisieren.

Eine MID Server-Verbindung kommuniziert standardmäßig über HTTP an Port 80. Dieser Kommunikationskanal erfordert kein Zertifikat. Die Verbindung zwischen dem MID Server und der Instanz erfolgt über HTTPS (Port 443). Die Instanz stellt über LDAP oder LDAPS direkt eine Verbindung zum LDAP-Server her. Diese Verbindung kann entweder über das Internet oder über einen VPN-Tunnel hergestellt werden.

Hinweis:
LDAP kann bei Passwortauthentifizierung nicht über den MID Server kommunizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für eine sichere Kommunikation über SSL müssen Sie ein SSL-Zertifikat für den MID Server hinzufügen. Ändern Sie die LDAP-Server-URL von LDAP in LDAPS, und wechseln Sie zu Port 636.



Hinweis:
Wenn Sie einen neuen LDAP-Server erstellen, wird die MID Server-SSL-Kennzeichnung standardmäßig auf „falsch“ gesetzt. Sie können dieses Verhalten ignorieren.

Informationen zum Festlegen von Verbindungseigenschaften für einen bestimmten LDAP-Server finden Sie unter Definieren Sie einen LDAP-Server.

Konfigurieren Sie die LDAP-Verbindungsüberwachung

Ändern oder deaktivieren Sie die LDAP-Verbindungsüberwachung und -Benachrichtigungen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Instanz sendet automatisch eine E-Mail an Benutzer, die in der Gruppe der LDAP-Administratoren konfiguriert sind, wenn eine LDAP-Serververbindung fehlschlägt. Dabei wird die E-Mail-Benachrichtigung “ (LDAP-Verbindung fehlgeschlagen) verwendet, die von der geplanten Aufgabe **„LDAP Connection Test**“ (LDAP-Verbindungstest) gestartet wird. Diese E-Mail-Benachrichtigung ist standardmäßig aktiviert.

Hinweis:
Die Instanz sendet die E-Mail-Benachrichtigung nur, wenn mindestens ein Mitglied in der Gruppe der LDAP-Administratoren vorhanden ist. Stellen Sie sicher, dass Sie diese Gruppe mit den Benutzern ausfüllen, die die E-Mail erhalten sollen.

Standardmäßig testet die regelmäßige Aufgabe die Verbindung alle 15 Minuten. So ändern Sie dieses Intervall oder deaktivieren die Überwachung:

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
2. Öffnen **Sie den LDAP-Verbindungstest**.
3. Führen Sie einen der folgenden Schritte aus:
   - Ändern Sie das Intervall im Feld **Wiederholungsintervall**.
   - Deaktivieren Sie die Überwachung, indem Sie das Kontrollkästchen **Aktiv** deaktivieren.

Importieren Sie Binärdaten über einen MID-Server

Als Administrator können Sie BLOB-Daten (Binary Large Object) mit einer LDAP-Integration über den MID Server importieren.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Fügen Sie den Namen der LDAP-Spalte, aus der Sie Binärdaten importieren möchten, der Systemeigenschaft glide.ldap.binary_attributes hinzu.
2. Fügen Sie eine MID Server-Eigenschaft mit dem Namen glide.ldap.binary_attributes und demselben Wert hinzu, den Sie für die Systemeigenschaft festgelegt haben.

Problembehandlung bei der LDAP-Integration über MID Server

Bei der Integration von LDAP über MID Server können Probleme in den folgenden Bereichen auftreten.

Sie können diese Probleme beheben, indem Sie die Ausgaben in der Warteschlange für externe Kommunikationskanäle (ECC) anzeigen (**Discovery** > **Ausgabe und Artefakte** > **ECC-Warteschlange**) an.

Testverbindungsprobleme

Beim Definieren von OEs auf dem Server wird die zugehörige Liste **Testverbindung** verwendet, um die LDAP-Verbindung zu überprüfen. Wenn Sie auf diesen Link klicken, sollte die ECC-Warteschlange eine einzelne Ausgabenachricht mit dem **Themennamen LDAPConnectionTesterProbe anzeigen**. Nach Abschluss des Tests auf dem MID Server sollte in der ECC-Warteschlange eine Eingabenachricht mit demselben Themennamen angezeigt werden. Wenn in der Spalte **Name** für die Eingabenachricht **true angezeigt**wird, war der Test erfolgreich. Führen Sie einen Drilldown in den Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

Verbindung testen

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:24:17	mid.server.local_mid	LDAPConnectionTesterProbe	true	04a952038f21010036bf21ca47e79a30	input	processed	2013-07-29 13:24:19
2013-07-29 13:24:04	mid.server.local_mid	LDAPConnectionTesterProbe		04a952038f21010036bf21ca47e79a30	output	processed	2013-07-29 13:24:17

Probleme durchsuchen

Beim Definieren von OEs auf dem Server wird eine zugehörige Liste **Durchsuchen** angezeigt, die zum Anzeigen der von der OE-Definition zurückgegebenen LDAP-Verzeichnisdatensätze verwendet wird. Wenn Sie auf diesen Link klicken, sollte die ECC-Warteschlange eine einzelne Ausgabenachricht mit dem **Themennamen LDAPBrowseProbe anzeigen**. Nachdem Daten vom MID Server zurückgegeben wurden, sollte die ECC-Warteschlange eine Eingabenachricht mit demselben Themennamen anzeigen. Wenn in der Spalte **Name** für die Eingabenachricht **true angezeigt**wird, war der Test erfolgreich. Führen Sie einen Drilldown in den Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

Importprobleme laden

Beim Hochladen von Daten (z. B. mit der Funktion „Testladen von 20 Datensätzen“) sollte die ECC-Warteschlange eine einzelne Ausgabenachricht mit dem **Themennamen LDAPProbe anzeigen**.

Nachdem Daten vom MID Server zurückgegeben wurden, sollte die ECC-Warteschlange eine weitere Eingabenachricht mit der Bezeichnung **LDAPProbeCompleted anzeigen**.
Die Spalte **Name** für diese Eingabenachricht zeigt die Gesamtzahl der zurückgegebenen Datensätze an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine zusätzliche Eingabenachricht mit dem Namen **LDAPProbe**wird angezeigt. In der Spalte **Name** für diese Eingabenachricht wird die höchste Datensatznummer im Batch angezeigt. Wenn die Gesamtzahl der zurückgegebenen Datensätze 258 und die Batch-Größe 200 beträgt (Standard), werden zwei eingehende LDAPProbe-Nachrichten (200, 258) und eine eingehende LDAPProbeCompleted-Nachricht (258) empfangen.

Führen Sie einen Drilldown in den Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

Importlast

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:09:48	mid.server.local_mid	LDAPProbeCompleted	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:48	LDAPProbeResult	LDAPProbe	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:36	mid.server.local_mid	LDAPProbe		ed0a0d7a8f32010036bf21ca47e79a56	output	processed	2013-07-29 13:09:46

Achten Sie auch auf eine Ausgabenachricht namens **LDAPProbeError**.

Fehlermeldung

All > Created on Today > Topic = LDAPProbeError

Created	Agent	Topic	Source	Queue	State	Processed	Error string
2014-02-20 14:52:55	mid.server.localdublinmid	LDAPProbeError	MID Server reported error: java.lang.Exc...	output	error	2014-02-20 14:53:02	No message handler for this message.

Klicken Sie auf den Link in der Spalte **Name**, um die Details des Fehlers anzuzeigen.

LDAP-Paging

LDAP-Paging funktioniert nicht, wenn die Paging-Größe auf dem LDAP-Server weniger als 1000 beträgt. Legen Sie die MID Server-Eigenschaft `glide.ldap.max_results` auf einen Wert kleiner oder gleich der Paging-Größe des LDAP-Servers fest.

LDAP kann Binärdaten nicht importieren

Um binäre Daten über LDAP zu importieren, z. B. ein Benutzerfoto, müssen Sie das binäre Attribut in die MID Server-Eigenschaft `glide.ldap.binary_attributes`aufnehmen. Für das Benutzerfoto kann das Attribut `jpegphoto` lauten.

Daten importieren und zuordnen

LDAP-Importzuordnungen stimmen Felder in Ihrer LDAP-Datenbank mit Feldern in Ihrer Instanz ab.

Hinweis:
Die LDAP-Zuordnung hat Auswirkungen auf die Leistung. Daher wird empfohlen, sie außerhalb der Spitzenzeiten zu planen oder einige Datensätze gleichzeitig zu verarbeiten, um die Systemverfügbarkeit aufrechtzuerhalten.

Definieren Sie eine Transformationszuordnung, die nur die erforderlichen oder erforderlichen Attribute importiert. Abhängig von der Version der Instanz, die Sie verwenden, variiert die Methode zum Angeben von LDAP-Zuordnungsbeziehungen.

Die einfachste Möglichkeit herauszufinden, ob Sie eine Version ausführen, die die System-LDAP-Anwendung für die LDAP-Integration verwendet, besteht darin, die Anwendung im Anwendungsnavigator zu finden.

Die Option **Business Rules** ausführen wird nur für die Zieltabelle angewendet. Nur Transformationszuordnungen, die der Zieltabelle zugeordnet sind, führen die Business Rules aus, die verschiedenen Tabellen zugeordnet sind. Wenn Sie eine Benutzergruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktualisieren und Geschäftsregeln für eine Benutzergruppentabelle ausgeführt werden, müssen für die Gruppe Rollen definiert sein.

LDAP-Importzuordnungsoptionen

System-LDAP-Anwendung?	Karte
Ja	Verwenden Sie eine *Transformationszuordnung*, um Ihre Zuordnung anzugeben.
Nein	Verwenden Sie eine veraltete LDAP -*Importzuordnung*, um Ihre Zuordnung anzugeben, oder die standardmäßige LDAP-Transformation, die in Baseline-Instanzen enthalten ist. Denken Sie daran, das Feld Zusammenfügen so anzupassen, dass es mit den **richtigen** Feldern übereinstimmt.

Geplante Importe

Ein geplanter Import ermöglicht es Administratoren, LDAP-Daten nach einem regelmäßigen Zeitplan zu importieren. Standardmäßig umfasst die LDAP-Integration zwei Beispiele für geplante Importe:

- Example LDAP User Import (LDAP-Anwenderimportbeispiel)
- Example LDAP Group Import (LDAP-Gruppenimportbeispiel)

Keines der Beispiele ist standardmäßig aktiv. Ändern Sie diese geplanten Importe, um die geschäftlichen Anforderungen Ihres Unternehmens zu erfüllen.

LDAP-Transformationszuordnungen

Die Transformationszuordnung verschiebt Daten aus der Import Set-Tabelle in die Zieltabelle (Benutzer oder Gruppe).

Die LDAP-Integration verwendet standardmäßige Import Sets und Transformationszuordnungen. Sie können auch benutzerdefinierte LDAP-Transformationszuordnungen erstellen.

Wichtig:
Unabhängig davon, ob Sie benutzerdefinierte LDAP-Transformationszuordnungen auswählen oder erstellen, sollte für einen Satz von Quell- und Zieltabellen eine aktive Transformationszuordnung vorhanden sein. Wenn Sie mehrere Transformationszuordnungen für dieselbe Quell- und Zieltabelle aktivieren, kann dies zu doppelten Einträgen in der Zieltabelle führen, es sei denn, Sie führen eine Zusammenfügung mit den übereinstimmenden Feldern durch.

Standardmäßige LDAP-Transformationszuordnungen

Standardmäßig stellt das System zwei Transformationszuordnungen für LDAP-Daten bereit.

Standardmäßige LDAP-Transformationszuordnungen

Transformationszuordnung	Quelltabelle	Zieltabelle	Beschreibung
LDAP-Benutzerimport	[ldap_import]	[sys_user]	Standard-Transformationszuordnung zum Erstellen von Benutzerdatensätzen aus LDAP-Anmeldeinformationen als Teil der LDAP-On-Demand-Anmeldung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßige LDAP-Transformationszuordnungen (Fortsetzung)

Transformationszuordnung	Quelltabelle	Zieltabelle	Beschreibung
			Enthält Zuordnungen für einen Active Directory LDAP-Server.
LDAP-Gruppenimport	[ldap_group_import]	[sys_user_group]	Standard-Transformationszuordnung zum Erstellen von Gruppendatensätzen aus LDAP-OEs. Enthält Zuordnungen für einen Active Directory LDAP-Server.

Hinweis:
Standardmäßig verfügt das System nicht über eine Transformationszuordnung für LDAP-Abteilungsdatensätze.

Anforderungen für benutzerdefinierte LDAP-Transformationszuordnungen

Wenn Sie eine benutzerdefinierte Transformationszuordnung erstellen, muss die Transformationszuordnung die folgenden Zuordnungsanforderungen erfüllen.

Anforderungen für benutzerdefinierte LDAP-Transformationszuordnungen

Quelltabelle	Quellfeld	Zieltabelle	Zielfeld	Zusammenfügen	Beschreibung
ldap_import	u_source	sys_user	Quelle	false	Das Feld **u_source gibt** den LDAP-DN des importierten Benutzers oder der importierten Gruppe an. Das System verwendet dieses Feld, um zu bestimmen, dass ein Benutzer eine LDAP-Authentifizierung erfordert, um den Vorgesetzten eines Benutzers zu finden und Benutzer in Gruppen einzuteilen.
ldap_import	Wählen Sie eines der folgenden Felder aus: • u_samaccountname • u_dn • u_cn	sys_user	user_name	Wahr	Wenn LDAP in Active Directory integriert ist, wählen **Sie u_samaccountname** als Quellfeld aus. Wenn andere LDAP-Verzeichnisse verwendet werden, wählen **Sie u_dn** oder **u_cn** als Quellfeld aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterschiede zwischen LDAP-Transformationszuordnungen und veralteten Importzuordnungen

Bei der Angabe von LDAP-Zuordnungsbeziehungen mithilfe von Transformationszuordnungen gibt es einen großen Unterschied darin, wie Referenzfelder für Manager und Abteilung festgelegt werden.

Wenn Sie eine *Transformationszuordnung*verwenden, müssen Sie ein *Transformationsskript* verwenden, um Referenzen zu erstellen. Dies liegt daran, dass der Wert, der einem LDAP-Attribut wie „manager“ zugeordnet ist, der eindeutige Name (Distinguished Name, DN) des Managers ist.

Ohne zusätzliche Logik wird ein Benutzerdatensatz mit einem Managernamen erstellt, der dem eindeutigen Namen dieses Benutzers in LDAP entspricht. Die Integration enthält ein Transformationsskript, um die Erstellung dieser Referenzen zu erleichtern. Die Standard-Transformationszuordnung „LDAP-Benutzerimport“ enthält Transformationsskripts für diese Referenzen.

Vorhandene Zuordnungsbeziehungen

Wenn Sie veraltete Importzuordnungen in Transformationszuordnungen aktualisieren, können Sie die LDAP-Zuordnungsbeziehungen beibehalten, die vor dem Hinzufügen der System-LDAP-Anwendung vorhanden waren. Der LDAP-Server verfügt über ein Feld **Karte**, das auf die veraltete Importzuordnung verweist.

Hinweis:
Standardmäßig ist dieses Feld ausgeblendet, daher müssen Sie das Formular so konfigurieren, dass es angezeigt wird.

Wenn Sie zur Verwendung einer Transformationszuordnung wechseln möchten, löschen Sie den Verweis auf die veraltete Importzuordnung.

Einstellungen für LDAP-Importzuordnung

Überprüfen und verwenden Sie Attribute, um die Felder zu begrenzen, die die Integration aus der LDAP-Quelle importiert. Darüber hinaus ist es wichtig, das Feld user_name dem LDAP-Attribut zuzuordnen, das die Anmelde-ID des Benutzers enthält. Für Active Directory ist dies normalerweise das Attribut sAMAccountName. Wenn Sie ein binäres Attribut (z. B. objectSID oder objectGUID) importieren und zusammenfügen möchten, müssen Sie ein benutzerdefiniertes Transformationsskript erstellen.

Hinweis:
Jeder Wert, der dem Feld user_name zugeordnet ist, muss eindeutig sein.

Wenn Sie keine Transformationszuordnung angeben (z. B. LDAP-Benutzerimport), verwendet die Integration die folgenden Standardzuordnungen:

Standardzuordnung für LDAP-Import

Benutzerfeld oder -variable	LDAP-Attribut
user_name	sAMAccountName
E-Mail	E-Mail
Telefon	phoneNumber

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardzuordnung für LDAP-Import (Fortsetzung)

Benutzerfeld oder -variable	LDAP-Attribut
home_phone	homePhone
mobile_phone	Mobile
first_name	gegebenerName
last_name	sn
Titel	Titel
department	department
Manager	Manager
Middle_name	Initialen
u_memberof	groups
u_member	Mitglieder
u_manager	Manager

LDAP-Datentransformation

Wenn ein LDAP-Attribut einfache Daten enthält, verknüpft die Transformationszuordnung ein importiertes LDAP-Attribut mit einem entsprechenden Feld in der Zieltabelle (Benutzer oder Gruppe). Beispielsweise werden Beispieldaten im Attribut sAMAccountName dem Feld **Benutzer-ID** in der Benutzertabelle zugeordnet.

Wenn die importierten LDAP-Daten einem Referenzfeld zugeordnet sind, sucht die Instanz nach einem vorhandenen übereinstimmenden Datensatz. Wenn kein übereinstimmender Datensatz vorhanden ist, erstellt die Instanz einen neuen Datensatz für das Referenzfeld, sofern in der Feldzuordnung nichts anderes angegeben ist.

Angenommen, das LDAP-Attribut l ist dem Referenzfeld **Standort** in der Benutzertabelle zugeordnet. Immer wenn der Import einen Attributwert einführt, der nicht mit einem vorhandenen Standortdatensatzwert übereinstimmt, erstellt die Transformationszuordnung einen neuen Standortdatensatz. Der neue Standortdatensatz hat denselben Wert wie das importierte Attribut, und der importierte Benutzerdatensatz verfügt jetzt über einen Link zum neuen Standortdatensatz.

Es kann jedoch vorkommen, dass das LDAP-Attribut einen eindeutigen Namen (Distinguished Name, DN) zurückgibt, der im Wesentlichen eine Referenz zu einem anderen Datensatz im LDAP-Verzeichnis ist. Beispielsweise enthält das Attribut „manager“ in der Regel den eindeutigen Namen für den Manager des aktuellen LDAP-Verzeichniseintrags. Ein importierter DN verwendet normalerweise eine lange Textzeichenfolge wie: cn=Beth Anglin,ou=Users,dc=my-domain,dc=com.

⚠ Warnung:
Stellen Sie sicher, dass Ihre Zielfelder lang genug sind, um einen DN zu enthalten. Viele Textfelder verwenden die Standardlänge von 40, was für einige DN-Werte möglicherweise nicht lang genug ist. Das System ServiceNow schneidet jeden Wert ab, der die Feldlänge überschreitet.

Administratoren möchten normalerweise nicht, dass das System neue Benutzer aus dem DN-Wert erstellt, da der neue Benutzer keine Zuordnung zu einem vorhandenen Benutzer hat. Stattdessen möchten Administratoren, dass der Import den vorhandenen Benutzerdatensatz des Managers findet und ihn dem neu importierten Benutzer zuordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Skripteinbindung LDAPUtils enthält die Funktionen setManager und processManagers, die einen DN analysieren und nach einem vorhandenen Benutzer suchen können. Um optimale Ergebnisse zu erzielen, verwenden Sie diese Funktionen, um eine benutzerdefinierte Transformationszuordnung zu erstellen.

Beispielsweise ruft das Skript der LDAP-Benutzerimport -Transformationszuordnung die Funktion setManager auf :

```
//
// The manager coming in from LDAP is the DN value for the manager.
// The line of code below will locate the manager that matches the
// DN value and set it into the target record.  If you are not
// interested in getting the manager from LDAP then remove or
// comment out the line below
ldapUtils. setManager (source , target ) ;
```

In einigen Fällen importiert die Integration den Datensatz eines Benutzers, bevor der Benutzerdatensatz des zugeordneten Managers importiert wird. Um solche Fälle zu behandeln, sollten Sie die Funktion processManagers nach Abschluss der Transformation aufrufen. Beispielsweise verwendet die Transformationszuordnung „ **LDAP-Benutzerimport** “ ein onComplete -Transformationsskript, um die Funktion processManagers aufzurufen.

```
// It is possible that the manager for a user did not exist in the database when // the
 user was processed and therefore we could not locate and set the manager field. // The
 processManagers call below will find all those records for which a manager could  // not be
 found and attempt to locate the manager again. This happens at the end of the  // import and
 therefore all users should have been created and we should be able to  // locate the manager
 at this point
ldapUtils. processManagers ( ) ;
```

Entfernen oder kommentieren Sie die Funktionsaufrufe setManager und processManagers aus, wenn Ihre LDAP-Integration das Attribut manager nicht verwendet.

LDAP-Skripterstellung

Erstellen Sie benutzerdefinierte Transformationszuordnungen, Skripts und Geschäftsregeln, um die Anforderungen beim Importieren von Daten anzugeben.

Benutzerdefinierte Transformationszuordnungen müssen die Transformationsskripts onStart und onAfter enthalten.

Das Skript onStart sollte die Skripteinbindung LDAPUtils aufrufen und mit der Protokollierung beginnen. Zum Beispiel verfügt die Transformationszuordnung für **LDAP-Benutzerimport** über ein onStart -Skript, das den folgenden Code verwendet:

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

Das onAfter- Skript sollte die addMembers- Funktion aufrufen. Beispiel:

```
ldapUtils.addMembers (source , target ) ;
```

Legen Sie deaktivierte Active Directory-Benutzer auf inaktiv fest

Verwenden Sie das folgende Skript, um Benutzer automatisch zu deaktivieren, wenn der zugeordnete AD-Benutzer deaktiviert wird.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können deaktivierte Active Directory-Benutzer identifizieren, indem Sie den Wert des Attributs userAccountControl überprüfen. Diese Regel wird immer dann ausgeführt, wenn sich der Wert userAccountControl ändert, und deaktiviert Benutzerkonten, wenn die **Benutzerkontensteuerung** einen deaktivierten AD-Account anzeigt.

Verwenden Sie das folgende Skript, um Benutzer automatisch zu deaktivieren, wenn der zugeordnete AD-Benutzer deaktiviert wird.

Prozedur

1. Konfigurieren Sie das Benutzerformular, und erstellen Sie ein neues Ganzzahlfeld mit der Bezeichnung **Benutzerkontensteuerung**.
2. Fügen Sie dem neuen Feld eine Zuordnung für userAccountControl (extern) hinzu.
3. Erstellen Sie eine neue Geschäftsregel mit den folgenden Eigenschaften:

Deaktivieren Sie die Geschäftsregel „AD-Benutzer“.

Feld „Business Rule“	Wert
Name	Deaktivieren Sie AD-Anwender
Tabelle	Benutzer [sys_user]
Wenn	Vor
Bedingung	current.u_user_account_control.changes()

Das Feld Skript muss Folgendes enthalten:

```
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2 bit flag is enabled
if (current.u_user_account_control & disabledFlag) {
  gs.log('Disabling user: ' + current.user_name + 'userAccountControl=' +
 current.u_user_account_control);
  current.active='false';
  current.locked_out='true';
}
```

Weisen Sie LDAP-Feldwerte zu

Sie können ein Skript verwenden, um jedem Feld, für das eine Feldzuordnung vorhanden ist, einen Wert zuzuweisen.

Um beispielsweise dem Feld „sys_user.company“ einen Wert zuzuweisen, erstellen Sie eine Feldzuordnung für das Feld „Unternehmen“, und fügen Sie das folgende Transformationsskript hinzu:

```
company = "Don's Sporting Goods";
```

Schließen Sie bestimmte LDAP-Benutzer aus

Wenn Sie die LDAP-Benutzerliste mithilfe der LDAP-Filtereigenschaften nicht vollständig filtern können, können Sie Benutzer mit einem Zuordnungsskript ausschließen.

Nachdem Sie die Logik ausgeführt haben, um einen Benutzer zu identifizieren, der nicht importiert werden soll, legen Sie das Feld user_name auf eine leere Zeichenfolge fest. Dieser Benutzer wird nicht importiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
user_name='';
```

Eine Möglichkeit, Benutzer zu identifizieren, die herausgefiltert werden sollen, besteht darin, im Attribut „ distinguishedName “ nach einer Zeichenfolge zu suchen. Dieses Skript schließt beispielsweise Accounts aus, die sich nicht in einer Benutzer-OE befinden. Sie können dieses Skript verwenden, wenn Sie zu viele Anwender-OE haben, um sie in die LDAP-Option der Ziel-OE aufzunehmen.

```
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```

Eine komplexere Filtermethode ist die Verwendung regulärer Ausdrücke.

```
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3 numbers, only import these
if (c.test(nvcn)) {
 user_name = nvcn;
} else {
 gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
 user_name = "";
}
```

Legen Sie die Auswahlaktion für Referenzfeldimporte fest

Die LDAP-Transformationszuordnung bestimmt, wie Felder in der Import Set-Tabelle Feldern in vorhandenen Tabellen wie „Incident“ oder „Benutzer“ zugeordnet werden.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die LDAP-Transformationszuordnung ein Feld in der Import Set-Tabelle aktualisiert, erstellt die Integration automatisch einen neuen Datensatz, wenn ein neuer Datensatz in den LDAP-Daten vorhanden ist. Wenn die LDAP-Transformationszuordnung ein Referenzfeld aktualisiert, in dem Daten aus einer anderen Tabelle gespeichert werden, kann der Administrator neue LDAP-Datensätze erstellen, ignorieren oder ablehnen. Wenn die Integration beispielsweise einen neuen Abteilungsdatensatz erhält, der keiner vorhandenen Abteilung entspricht, möchten Sie möglicherweise alle anderen LDAP-Datensatzfelder aktualisieren, ohne einen neuen Abteilungsdatensatz in der Instanz zu erstellen. Mit der Transformationszuordnung können Sie die Datensatzerstellungsoptionen für jedes Referenzfeld festlegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **Transformationszuordnungen**.
2. Wählen Sie in der zugehörigen Liste „ **Feldzuordnungen** “ eine der folgenden Aktionen aus dem Feld Auswahlaktion aus:
   - **erstellen** – erstellt einen neuen Referenzfelddatensatz, wenn kein übereinstimmender Datensatz vorhanden ist.
   - **ignore** – ignoriert neue Datensätze im Referenzfeld und schließt die Verarbeitung aller anderen Felder in der Transformationszuordnung ab.
   - **Ablehnen** – stoppt die Transformation für den gesamten Datensatz.

Hinweis:
Die **Feldzuordnung** zeigt nur das Auswahlaktionsfeld für Referenzfelder an.

Überprüfen Sie die LDAP-Zuordnung

Aktualisieren Sie nach dem Erstellen einer LDAP-Transformationszuordnung die LDAP-Daten, um sicherzustellen, dass die Transformationszuordnung wie erwartet funktioniert.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **Geplante Lasten**.
2. Klicken Sie auf Ihren LDAP-Importauftrag.
3. Klicken Sie auf **Jetzt ausführen**.

Fehlerbehebung bei der LDAP-Integration

Wenn Sie Ihren LDAP-Server integrieren und Fragen haben, können diese Elemente Ihnen bei der Behebung des Problems helfen.

Vorabprüfungen

- Wenn LDAP nicht verfügbar ist, können sich Benutzer nicht bei der Instanz anmelden. Es wird empfohlen, lokale Konten für Administratoren zu haben, damit Administratoren bei einem Ausfall des LDAP weiterhin auf die Instanz zugreifen können.
- Überprüfen Sie das Servicekonto, um sicherzustellen, dass es nicht abgelaufen oder gesperrt ist.
- Überprüfen Sie das Format des Benutzernamens. Anstatt nur den Benutzernamen zu verwenden, versuchen Sie es mit der Domäne mit dem Benutzernamen oder username@domain.
- Vergewissern Sie sich, dass Sie den Eintrag `system_id` im Datensatz `ldap_server_config` geändert haben. Wenn Sie `system_id` unbeabsichtigt mit einem Update Set ändern, verweist `system_id` auf den falschen Knoten für die Zielinstanz und funktioniert nicht.

Fehlercodes

Die LDAP-Protokolldatei listet branchenübliche Fehlercodes für LDAP und Active Directory (AD) auf. Die LDAP-Protokolldatei ist in der Wrapper-Datei enthalten. Die LDAP-Fehlercodes sind zweistellige Nummern, während die Active Directory-Fehlercodes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dreistellige Nummern sind. Eine Liste der häufigsten Fehlercodes finden Sie unter LDAP-Fehlercodes.

Integration mehrerer Domänen

Sie können mehrere Domänen innerhalb derselben Gesamtstruktur oder in vollständig nicht vertrauenswürdigen Domänen integrieren. Es wird empfohlen, für jede Domäne einen separaten LDAP-Serverdatensatz zu erstellen. Jeder LDAP-Serverdatensatz muss auf einen Domänencontroller für die angegebene Domäne verweisen. Das bedeutet, dass Sie Verbindungen zu jedem der Domänencontroller zulassen müssen. Mehrere AD-Gesamtstrukturen über LDAP mit einem LDAP-Account werden nicht unterstützt.

Wenn Sie auf mehr als eine Domäne erweitern, ist es wichtig, eindeutige LDAP-Attribute für die Anwendungsbenutzernamen zu identifizieren und Zusammenfügungswerte zu importieren. Ein allgemeines eindeutiges Zusammenfügungsattribut für Active Directory ist `objectSid`. Eindeutige Benutzernamen variieren je nach LDAP-Datendesign. Allgemeine eindeutige Attribute sind „ `email` “ oder „`userPrincipalName`“.

Eingehende Datensätze

Unter LDAP-Transformationszuordnungen erfahren Sie, wie die Integration eingehende LDAP-Datensätze verarbeitet, bei denen übereinstimmende Werte in Referenzfeldern fehlen.

Häufige Authentifizierungsfehler

- Benutzer kann sich nicht anmelden (ungültiger DN)
- Ungültige CN
- Ungültige Verbindung

Automatische LDAP-Verbindungstests

Sie können Verbindungen zu LDAP-Servern manuell testen oder zulassen, dass ServiceNow die Verbindungen automatisch testet.

Das System testet die Verbindung automatisch:

- Jedes Mal, wenn ein Benutzer das LDAP-Serverformular öffnet.
- Über die geplante Aufgabe „LDAP-Verbindungstest“, die standardmäßig alle 15 Minuten ausgeführt wird.

  Sie können ändern, wie oft diese regelmäßige Aufgabe ausgeführt wird. Wenn diese regelmäßige Aufgabe keine Verbindung herstellen kann, wiederholt eine neue einmalige regelmäßige Aufgabe den Verbindungstest entweder nach fünf Minuten oder nach der Hälfte des Werts für das **Wiederholungsintervall** in der geplanten Aufgabe, je nachdem, was zuerst eintritt.

Fehlermeldungen werden im Formular angezeigt, wenn Probleme beim Herstellen der Verbindung mit dem LDAP-Server auftreten. Unterstützt werden auch Testverbindungen für Server hinter einem MID-Server.

Zeigen Sie die LDAP-Überwachung an

Aktuelle Informationen zu LDAP-Servern und -Listenern können Sie mit dem LDAP-Monitor anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die verfügbaren Status sind:

- Aktiv
- Inaktiv
- Fehler
- Aktiv (wird heruntergefahren...)
- Fehler (wird heruntergefahren...)

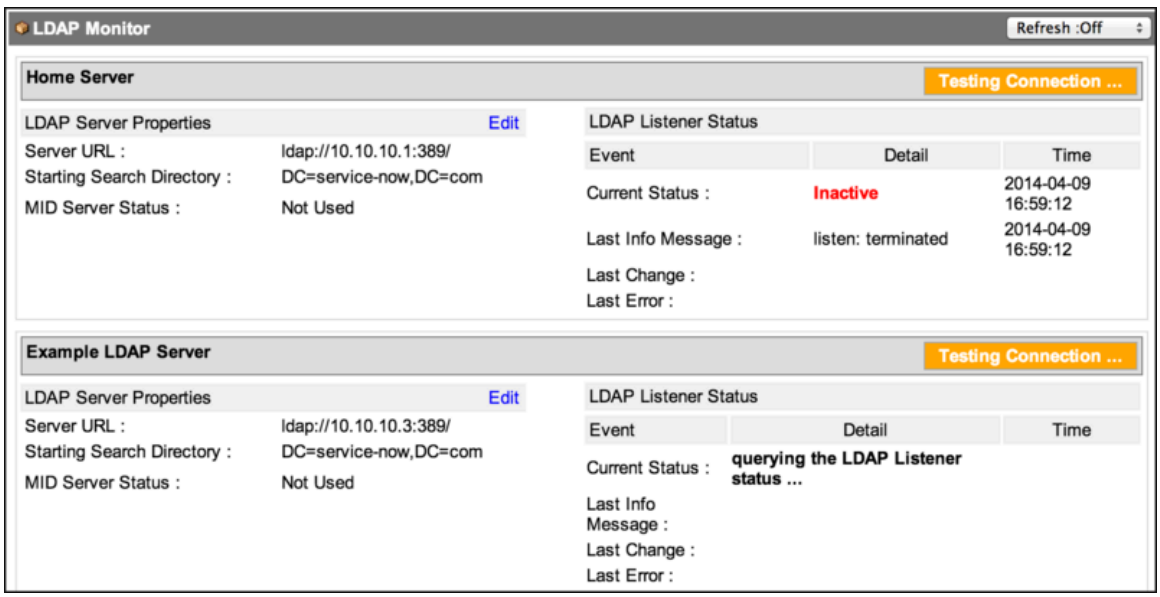
Zusätzlich zum aktuellen Status zeigt die Überwachung auch Folgendes an:

- Die letzte vom Listener erkannte Nachricht, z. B. Warten auf LDAP-Änderungen, Verbindungsfehler usw.
- Die letzte LDAP-Benutzeränderung, z. B. neuer Benutzer, aktualisierter Benutzer usw.
- Der zuletzt aufgetretene Fehler.

So zeigen Sie den LDAP-Monitor an:

Prozedur

Navigieren zu **Alle** > **LDAP** > **System-LDAP** > **LDAP-Überwachung**.



In der Tabelle finden Sie Beschreibungen der Eigenschaften und Felder auf dem Bildschirm.

LDAP-Monitor

Feld	Beschreibung
Neu laden	Sie können die Aktualisierungsrate konfigurieren, indem Sie in der Kopfzeile der LDAP-**Serverüberwachung** in das Feld Aktualisieren klicken und die Anzahl der Sekunden zwischen den einzelnen Datenaktualisierungen auswählen. Sie können auch **Keine** auswählen, um die Aktualisierung zu unterdrücken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verbindungsstatus	Die Serververbindungsanzeige befindet sich auf der rechten Seite über den Statusfeldern des LDAP-Listeners. Wenn eine Verbindung mit dem Server besteht, ist das Feld grün und zeigt *Verbunden*an. Wenn der Server nicht verbunden ist, ist das Feld rot und zeigt *Nicht verbunden*an. Wenn die Serververbindung getestet wird, ist das Feld gelb und zeigt *Testverbindung*an.
Eigenschaften des LDAP-Servers	
Bearbeiten	Während Sie LDAP-Server überwachen, können Sie Änderungen an den Eigenschaften vornehmen, indem Sie im Bildschirm „LDAP-Serverüberwachung“ auf **Bearbeiten** klicken.
Server-URL	Die Kombination aus Servername und Serverport, an dem der LDAP-Server abgehört wird Häufig wird der Port auf einen der folgenden festgelegt: • 389: Der Standardport für die Verbindung zu LDAP im Klartext • 636: Standardport für die Verbindung mit LDAP über eine SSL-Verbindung Beispielwert: ldap://10.10.10.3:389/ Ihr LDAP-Server verfügt möglicherweise über mehr als eine URL-Adresse. Dadurch werden NICHT mehrere Verzeichnisstrukturen erstellt, aus denen Sie Daten importieren können, was durch Erstellen eines weiteren LDAP-Servereintrags erreicht wird. Bei mehreren LDAP-Servern wird jedoch für Redundanz gesorgt, um einen Single Point of Failure zu vermeiden. Die LDAP-URL-Adressen werden durch ein Leerzeichen getrennt, und das System testet automatisch jede Serveradresse, bis eine gültige Verbindung hergestellt werden kann.
Suche im Verzeichnis wird gestartet	Das Startverzeichnis oder der RDN (Relative Distinguished Name), in dem das System mit der Suche nach Benutzern oder Gruppen beginnt. Beispielwert: DC=service-now,DC=com Über diesem Punkt sind keine Daten für den Import verfügbar. Die Instanz hat Einblick in das angegebene Verzeichnis und die darunter liegenden Verzeichnisse in der LDAP-Hierarchie.
MID-Serverstatus	Aktueller Verbindungsstatus des MID Servers.
Status des LDAP-Listeners	
Aktueller Status	Dies gibt an, ob der Listener aktiv ist.
Letzte Info-Nachricht	Zeigt die letzte Nachricht an, die der LDAP-Server bezüglich Benutzer- und Gruppenänderungen erhalten hat, und die Uhrzeit, zu der die Nachricht empfangen wurde.
Letzter Change	Zeigt die letzte am LDAP-Server vorgenommene Änderung und die Uhrzeit an.
Letzter Fehler	Zeigt den letzten Fehler an, der auf dem LDAP-Server aufgetreten ist, und die Uhrzeit, zu der er aufgetreten ist.

LDAP-Fehlercodes

Die LDAP-Protokolldatei listet branchenübliche Fehlercodes für LDAP und Active Directory (AD) auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardfehlercodes

Standard-LDAP-Fehler

Fehler/ Datencode	Text	Beschreibung
0	LDAP_SUCCESS	Gibt an, dass der angeforderte Clientvorgang erfolgreich abgeschlossen wurde.
2	LDAP_PROTOCOL_ERROR	Gibt an, dass der Server eine ungültige oder falsch formatierte Anforderung vom Client erhalten hat.
3	LDAP_ZEITBEGRENZUNG_ÜBERSCHREITUNG	Gibt an, dass das vom Client oder Server angegebene Zeitlimit des Vorgangs überschritten wurde. Bei Suchvorgängen werden unvollständige Ergebnisse zurückgegeben.
4	LDAP_SIZELIMIT_ÜBERSCHREITUNG	Gibt an, dass in einem Suchvorgang die vom Client oder Server angegebene Größenbeschränkung überschritten wurde. Es werden unvollständige Ergebnisse zurückgegeben.
5	LDAP_COMPARE_FALSCH	Zeigt keine Fehlerbedingung an. Gibt an, dass die Ergebnisse eines Vergleichsvorgangs „false“ sind.
6	LDAP_COMPARE_TRUE	Zeigt keine Fehlerbedingung an. Gibt an, dass die Ergebnisse eines Vergleichsvorgangs „true“ sind.
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	Gibt an, dass der Client während eines Bindungsvorgangs eine Authentifizierungsmethode angefordert hat, die vom LDAP-Server nicht unterstützt wird.
8	LDAP_Strong_Auth_Required	Gibt eine der folgenden Optionen an: In Bindungsanforderungen akzeptiert der LDAP-Server nur eine starke Authentifizierung. In einer Clientanforderung hat der Client einen Vorgang wie Löschen angefordert, der eine starke Authentifizierung erfordert. Bei einer unaufgeforderten Benachrichtigung über die Trennung der Verbindung erkennt der LDAP-Server, dass die Sicherheit der Kommunikation zwischen Client und Server unerwartet fehlgeschlagen ist oder gefährdet wurde.
9		Reserviert.
10	LDAP_REFERRAL	Zeigt keine Fehlerbedingung an. Gibt in LDAPv3 an, dass der Server nicht den Zieleintrag der Anforderung enthält,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
		die Server im Verweisfeld jedoch möglicherweise.
11	LDAP_ADMINLIMIT_ÜBERSCHREITUNG	Gibt an, dass ein von einer Verwaltungsbehörde festgelegter LDAP-Servergrenzwert überschritten wurde.
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Gibt an, dass der LDAP-Server eine Anforderung nicht erfüllen konnte, da mindestens eine kritische Erweiterung nicht verfügbar war. Entweder unterstützt der Server das Steuerelement nicht, oder das Steuerelement ist nicht für den Vorgangstyp geeignet.
13	LDAP_VERTRAULICHKEIT_ERFORDERLICH	Gibt an, dass die Sitzung nicht durch ein Protokoll wie Transport Layer Security (TLS) geschützt ist, das Sitzungsvertraulichkeit bietet.
14	LDAP_SASL_BIND_IN_PROGRESS	Zeigt keine Fehlerbedingung an, zeigt jedoch an, dass der Server für den nächsten Schritt im Prozess bereit ist. Der Client muss den gleichen SASL-Mechanismus an den Server senden, um den Prozess fortzusetzen.
15		Nicht verwendet.
16	LDAP_NO_SUCH_ATTRIBUTE	Gibt an, dass das im Änderungs- oder Vergleichsvorgang angegebene Attribut im Eintrag nicht vorhanden ist.
17	LDAP_UNDEFINIERTER_TYPE	Gibt an, dass das im Änderungs- oder Hinzufügen-Vorgang angegebene Attribut im Schema des LDAP-Servers nicht vorhanden ist.
18	LDAP_INFAST_MATCHING	Gibt an, dass die im Suchfilter angegebene Übereinstimmungsregel nicht mit einer Regel übereinstimmt, die für die Syntax des Attributs definiert ist.
19	LDAP_CONSTRAINT_VIOLATION	Gibt an, dass der Attributwert, der in einem DN-Vorgang zum Ändern, Hinzufügen oder Ändern angegeben ist, gegen die für das Attribut geltenden Einschränkungen verstößt. Die Einschränkung kann Größe oder Inhalt sein (nur Zeichenfolge, keine Binärdatei).
20	LDAP_TYPE_OR_VALUE_EXISTS	Gibt an, dass der in einem Änderungs- oder Hinzufügen-Vorgang angegebene Attributwert bereits als Wert für dieses Attribut vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
21	LDAP_INVALID_SYNTAX	Gibt an, dass der in einem Vorgang zum Hinzufügen, Vergleichen oder Ändern angegebene Attributwert eine nicht erkannte oder ungültige Syntax für das Attribut ist.
22–31		Nicht verwendet.
32	LDAP_NO_SUCH_OBJECT	Gibt an, dass das Zielobjekt nicht gefunden werden kann. Dieser Code wird bei folgenden Vorgängen nicht zurückgegeben: Suchvorgänge, die die Suchbasis finden, aber keine Einträge finden können, die dem Suchfilter entsprechen. Bindungsvorgänge.
33	LDAP_ALIAS_PROBLEM	Gibt an, dass beim Dereferenzieren eines Alias ein Fehler aufgetreten ist.
34	LDAP_INVALID_DN_SYNTAX	Gibt an, dass die Syntax des DN falsch ist. (Wenn die DN-Syntax korrekt ist, die Strukturregeln des LDAP-Servers den Vorgang jedoch nicht zulassen, gibt der Server Code 53 zurück: LDAP_UNWILLING_TO_PERFORM.)
35	LDAP_IS_LEAF	Gibt an, dass der angegebene Vorgang nicht für einen Blatteintrag ausgeführt werden kann. (Dieser Code ist derzeit nicht in den LDAP-Spezifikationen enthalten, aber für diese Konstante reserviert.)
36	LDAP_ALIAS_DEREF_PROBLEM	Gibt an, dass während eines Suchvorgangs entweder der Client keine Zugriffsrechte zum Lesen des Namens des Alias-Objekts hat oder eine Dereferenzierung nicht zulässig ist.
37–47		Nicht verwendet.
48	LDAP_INACPROPRIATE_AUTH	Gibt an, dass der Client während eines Bindungsvorgangs versucht, eine Authentifizierungsmethode zu verwenden, die der Client nicht ordnungsgemäß verwenden kann. Beispielsweise kann eine der folgenden Ursachen diesen Fehler verursachen: Der Client gibt einfache Anmeldeinformationen zurück, wenn starke Anmeldeinformationen erforderlich sind...ODER...Der Client gibt einen DN und ein Passwort für eine einfache Bindung zurück, wenn für den Eintrag kein Passwort definiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
49	LDAP_INVALID_CREDENTIALS	Gibt an, dass während eines Bindungsvorgangs einer der folgenden Fälle aufgetreten ist: Der Client hat entweder einen falschen DN oder ein falsches Passwort übergeben, oder das Passwort ist falsch, da es abgelaufen ist, eine Eindringlingserkennung das Konto gesperrt hat, oder aus einem ähnlichen Grund. Weitere Informationen finden Sie im Datencode.
49/52e	AD_INVALID-ANMELDINFORMATIONEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Fehler an, der zurückgegeben wird, wenn der Benutzername gültig ist, die Kombination aus Passwort und Benutzeranmeldeinformationen jedoch ungültig ist. Dies ist das AD-Äquivalent des LDAP-Fehlercodes 49.
49/525	BENUTZER NICHT GEFUNDEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, der zurückgegeben wird, wenn der Benutzername ungültig ist.
49/530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Gibt einen AcceptSecurityContext-Datenfehler in Active Directory (AD) an, bei dem es sich um einen Anmeldefehler handelt, der dadurch verursacht wird, dass sich der Benutzer zu diesem Zeitpunkt nicht anmelden darf. Wird nur zurückgegeben, wenn ein gültiger Benutzername und gültige Passwortanmeldeinformationen vorhanden sind.
49/531	EINGESCHRÄNKT_AUF_SPezifISCHE_GERÄTE	Gibt einen AcceptSecurityContext-Datenfehler in Active Directory (AD) an, bei dem es sich um einen Anmeldefehler handelt, der dadurch verursacht wird, dass sich der Benutzer nicht von diesem Computer aus anmelden darf. Wird nur zurückgegeben, wenn ein gültiger Benutzername und gültige Passwortanmeldeinformationen vorhanden sind.
49/532	PASSWORD_ABGELAUFEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, der einen Anmeldefehler darstellt. Das angegebene Account-Passwort ist abgelaufen. Wird nur zurückgegeben,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
		wenn ein gültiger Benutzername und ein gültiges Passwort vorhanden sind.
49/533	ACCOUNT_DISABLED	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, der einen Anmeldefehler darstellt. Der Account ist derzeit deaktiviert. Wird nur zurückgegeben, wenn ein gültiger Benutzername und ein gültiges Passwort vorhanden sind.
49/568	ERROR_TOO_VIELE_KONTEXT_IDS	Gibt an, dass während eines Anmeldeversuchs der Sicherheitskontext des Benutzers zu viele Sicherheits-IDs angesammelt hat. Dies ist ein Problem mit dem spezifischen LDAP-Benutzerobjekt/ -Account, das vom LDAP-Administrator untersucht werden sollte.
49/701	ACCOUNT_ABGELAUFEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, der einen Anmeldefehler darstellt. Der Account des Benutzers ist abgelaufen. Wird nur zurückgegeben, wenn ein gültiger Benutzername und ein gültiges Passwort vorhanden sind.
49/773	BENUTZER MUSS PASSWORD ZURÜCKSETZEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an. Das Passwort des Benutzers muss vor der ersten Anmeldung geändert werden. Wird nur zurückgegeben, wenn ein gültiger Benutzername und ein gültiges Passwort vorhanden sind.
50	LDAP_INSUFFICIENT_ACCESS	Gibt an, dass der Aufrufer nicht über ausreichende Rechte zum Ausführen des angeforderten Vorgangs verfügt.
51	LDAP_BELASTET	Gibt an, dass der LDAP-Server zu ausgelastet ist, um die Client-Anforderung zu diesem Zeitpunkt zu verarbeiten, aber wenn der Client wartet und die Anforderung erneut übermittelt, kann der Server sie dann möglicherweise verarbeiten.
52	LDAP_UNAVAILABLE	Gibt an, dass der LDAP-Server die Bindungsanforderung des Clients nicht verarbeiten kann, normalerweise weil er heruntergefahren wird.
52e	AD_INVALID-ANMELDINFORMATIONEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Fehler an, der zurückgegeben wird, wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
		der Benutzername gültig ist, die Kombination aus Passwort und Benutzeranmeldeinformationen jedoch ungültig ist. Dies ist das AD-Äquivalent des LDAP-Fehlercodes 49: LDAP_INVALID_CREDENTICALS.
53	LDAP_UNWILLING_TO_PERFORM	Gibt an, dass der LDAP-Server die Anforderung aufgrund serverdefinierter Einschränkungen nicht verarbeiten kann. Dieser Fehler wird aus den folgenden Gründen zurückgegeben: Die Anforderung zum Hinzufügen eines Eintrags verstößt gegen die Strukturregeln des Servers...ODER...Die Anforderung zum Ändern des Attributs gibt Attribute an, die Benutzer nicht ändern können...ODER...Passwortbeschränkungen verhindern die Aktion... ODER... Verbindungsbeschränkungen verhindern die Aktion.
54	LDAP_LOOP_DETECT	Gibt an, dass der Client einen Alias oder eine Verweisschleife erkannt hat und diese Anforderung daher nicht abschließen kann.
55–63		Nicht verwendet.
64	LDAP_BENAMUNG_VERSTÖSIGUNG	Gibt an, dass der Vorgang zum Hinzufügen oder Ändern von DNs gegen die Strukturregeln des Schemas verstößt. Beispiel: Die Anforderung ordnet den Eintrag einem Alias unter. Die Anforderung ordnet den Eintrag einem Container unter, der nach den Containment-Regeln verboten ist. Der RDN für den Eintrag verwendet einen verbotenen Attributtyp.
65	LDAP_OBJECT_CLASS_VIOLATION	Gibt an, dass der Vorgang zum Hinzufügen, Ändern oder Ändern des DN gegen die Objektklassenregeln für den Eintrag verstößt. Beispielsweise geben die folgenden Anforderungstypen diesen Fehler zurück: Der Vorgang zum Hinzufügen oder Ändern versucht, einen Eintrag ohne Wert für ein erforderliches Attribut hinzuzufügen. Beim Hinzufügen- oder Ändern-Vorgang wird versucht, einen Eintrag mit einem Wert für ein Attribut hinzuzufügen, das die Klassendefinition nicht enthält. Der Änderungsvorgang versucht, ein erforderliches Attribut

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
		zu entfernen, ohne die Hilfsklasse zu entfernen, die das Attribut als erforderlich definiert.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Gibt an, dass der angeforderte Vorgang nur für Blatteinträge zulässig ist. Beispielsweise geben die folgenden Arten von Anforderungen diesen Fehler zurück: Der Client fordert einen Löschvorgang für einen übergeordneten Eintrag an. Der Client fordert einen DN-Änderungsvorgang für einen übergeordneten Eintrag an.
67	LDAP_NOT_ALLOWED_ON_RDN	Gibt an, dass beim Änderungsvorgang versucht wurde, einen Attributwert zu entfernen, der den relativen eindeutigen Namen des Eintrags bildet.
68	LDAP_ALREADY_EXISTS	Gibt an, dass beim Hinzufügen-Vorgang versucht wurde, einen bereits vorhandenen Eintrag hinzuzufügen, oder dass beim Änderungsvorgang versucht wurde, einen Eintrag in den Namen eines bereits vorhandenen Eintrags umzubenennen.
69	LDAP_NO_OBJECT_CLASS_MODS	Gibt an, dass der Änderungsvorgang versucht hat, die Strukturregeln einer Objektklasse zu ändern.
70	LDAP_ERGEBNIS_TOO_LARGE	Reserviert für CLDAP.
71	LDAP_AFFECTS_MULTIPLE_DSAS	Gibt an, dass der Vorgang zum Ändern des DN den Eintrag von einem LDAP-Server auf einen anderen verschiebt und mehr als einen LDAP-Server erfordert.
72–79		Nicht verwendet.
80	LDAP_SONSTIGE	Zeigt eine unbekannte Fehlerbedingung an. Dies ist der Standardwert für NDS-Fehlercodes, die keinen anderen LDAP-Fehlercodes zugeordnet sind.
775	BENUTZER_ACCOUNT_GESPERRT	Gibt an, dass Benutzer sich nicht anmelden können, da das Benutzerkonto gesperrt ist.

Benutzerdefinierte Fehlercodes

Benutzerdefinierte LDAP-Fehlercodes

Fehler/Datencode	Text
10000	LDAP_ERROR_GENEREL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerdefinierte LDAP-Fehlercodes (Fortsetzung)

Fehler/Datencode	Text
10001	LDAP_ERROR_Mal_formed_URL
10002	LDAP_ERROR_UNAUTHENTICATED_BIND
10300	LDAP_ERROR_COMMUNICATION_EXCEPTION
10301	LDAP_FEHLER_Socket_Zeitüberschreitung
10302	LDAP_ERROR_CONNECTION_REFUSED
10303	LDAP_FEHLER_VERBINDUNG_ZURÜCKSETZEN
10304	LDAP_ERROR_NO_ROUTE
10305	LDAP_ERROR_UNKNOW_HOST
10400	LDAP_ERROR_SSL_EXCEPTION
10401	LDAP_ERROR_SSL_EMPTY_CERT_STORE
10402	LDAP_ERROR_SSL_CERT_NOT_FOUND
10403	LDAP_ERROR_SSL_CERT_ABGELAUFEN
10500	LDAP_ERROR_INVALID_SEARCH_FILTER_EXCEPTION

Senden Sie ein Einmalpasswort, wenn der LDAP-Server inaktiv ist

Eine LDAP-Eigenschaft ist verfügbar, um einem Benutzer ein Einmalpasswort zu senden, wenn sich der Benutzer nicht anmelden kann, weil der LDAP-Server ausgefallen ist. Sie können auch eine andere Eigenschaft konfigurieren, um zu steuern, wie lange das Passwort gültig ist.

Vorbereitungen

Erforderliche Rolle: admin

Um ein Einmalpasswort zu erhalten, muss der Benutzer in seinem Benutzerprofil Benachrichtigungen aktiviert haben. Die Benachrichtigung ist nur eine E-Mail-Nachricht. SMS-Nachrichten werden nicht unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Beide Eigenschaften sind standardmäßig aktiviert. Der Standardwert für die Eigenschaft, die die Passwortgültigkeit steuert, beträgt 10 Minuten.

Prozedur

1. Öffnen Sie die Liste der Systemeigenschaften, indem Sie `sys_properties.list` im Filter des Anwendungsnavigators eingeben.
2. Suchen Sie die Eigenschaft *`glide.ldap.onetime.password.enabled`*.
3. Legen Sie die Eigenschaft auf `true` fest.
4. Um die Gültigkeit des Passworts für einen Benutzer zu ändern, legen Sie die folgende Eigenschaft auf eine Ganzzahl in Minuten fest: *`glide.authenticate.onetime.password.validity`*.

Synchronisierung von LDAP-Datensätzen

Administratoren können inaktive, deaktivierte oder gelöschte LDAP-Datensätze mit ihren LDAP-Datensätzen synchronisieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei der LDAP-Datensatzsynchronisierung werden inaktive Datensätze auf dem LDAP-Server erkannt und die entsprechenden LDAP-Datensätze aktualisiert. Das Erkennen inaktiver LDAP-Datensätze umfasst die Definition konsistenter Datenindikatoren für jedes Benutzerobjekt, den Import von LDAP-Daten und die Auswertung der Datenindikatoren.

Ein Datenindikator kann sein:

- Ein Datumsfeld
- Mitgliedschaft in einer bestimmten OE (identifizieren durch Analysieren des Attributs *dn*) unter Verwendung des Attributs `useraccountcontrol` .
- Eine Kombination dieser Indikatoren

Importierte Daten gelangen über Import Set-Tabellen in die Instanz, in denen die Daten ausgewertet und verarbeitet werden können.

Der Importprozess kann LDAP-Aktualisierungsfilterfür mehrere Importaufträge verwenden, um verschiedene Arten von Benutzerdatensätzen aufzuteilen und Datensätze für die separate Verarbeitung zu trennen.

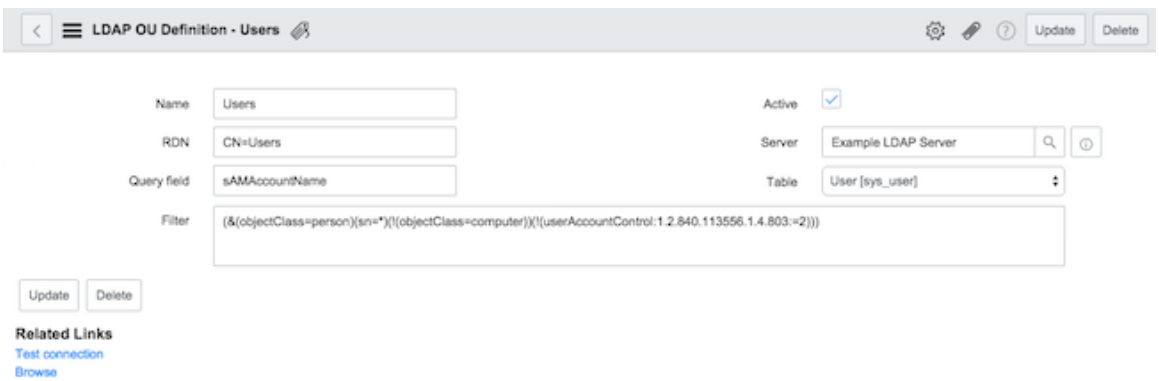
LDAP-Aktualisierungsfilter

Filter im LDAP-Aktualisierungsprozess können verwendet werden, um eine Verarbeitung anzugeben, die Einfügungen deaktivierter Benutzer ignoriert.

Sie können den LDAP-OE-Filter lockern, um alle Daten in Ihre Import Set-Tabelle aufzunehmen (einschließlich inaktiver Benutzer), und dann eine Verarbeitung angeben, die Einfügungen deaktivierter Benutzer ignoriert. Die Beispiel-OE-Definition „Benutzer“, die die Instanz in ihrem vordefinierten LDAP-Beispiel bereitstellt, enthält einen Filter.

Dieser Filter ist wichtig, da er definiert, welche Benutzerdatensätze in die auszuwertende Import Set-Tabelle übernommen werden. Während eine geringere Datenlast erreicht wird, besteht eine Einschränkung dieses Filters darin, dass inaktive Benutzer herausgefiltert werden, sodass die inaktiven Benutzerdatensätze nicht in die temporären Tabellen des Importsatzes importiert werden. Da die inaktiven Benutzerdatensätze nicht sichtbar sind, können die Datensatzindikatoren nicht ausgewertet werden.

LDAP-OU-Filter



Um die Filterung innerhalb des LDAP-Aktualisierungsprozesses zu verwenden, ändern Sie den Filter, um alle Benutzerdatensätze einzubeziehen. Das Ergebnis ist, dass alle Datensätze in die temporäre Tabelle des Importsatzes geladen werden, wo sie ausgewertet und transformiert werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Hier gibt es eine Vorsichtsmaßnahme: Da bei der Filterung alle Datensätze erfasst werden, erhalten Sie möglicherweise eine große Anzahl älterer inaktiver LDAP-Konten, die nicht in die Instanz eingefügt werden sollten. Ein Benutzerdatensatz sollte niemals für einen deaktivierten Benutzer erstellt werden.

LDAP-Extraktion

Ein LDAP-Extraktionsprozess kann implementiert werden, um deaktivierte Benutzer zu erkennen.

Ein Extrakt aus Ihrer LDAP-Quelle kann nach deaktivierten Benutzern mithilfe einer aktiven Kennzeichnung gefiltert werden, die für jeden Datensatz im Import auf „falsch“ festgelegt werden kann. Geben Sie („target.active=false“) an, und kopieren Sie sie in das **Skriptfeld** direkt im Datensatz der Tabellentransformationszuordnung.

Vorteile

Diese Methode bietet folgende Vorteile:

- Einfaches Skripting
- Vorhandene Benutzerdatensätze werden bei der Verarbeitung nicht berücksichtigt
- Inaktive Benutzer werden nicht in eine temporäre Importtabelle geladen
- Keine Auswirkungen auf die Leistung

Nachteile

Nachteile dieser Methode:

- Ein zusätzlicher Prozess wird erstellt
- Der Extraktsatz muss an einem Speicherort platziert werden, auf den Ihre Datenquelle zugreifen kann

Alternative Methode

LDAP-Aktualisierungsfilter Verwenden Sie mehrere Importaufträge, um verschiedene Arten von Benutzerdatensätzen aufzuteilen und Datensätze für die separate Verarbeitung zu trennen.

Inaktive LDAP-Benutzeraccounts

Erkennen, dass ein vorhandenes, aktuelles Benutzerkonto inaktiv ist oder deaktiviert oder aus einem Active Directory (AD) LDAP gelöscht wurde

Ein häufiges Problem bei der LDAP-Integration besteht darin, wie deaktivierte oder gelöschte Benutzer in einem Active Directory (AD) erkannt und dann in der Instanz deaktiviert werden. In einem Active Directory-LDAP wird normalerweise ein Filter festgelegt, um inaktive Benutzer bei der Aktualisierung auszuschließen, sodass die Instanz keine Benutzer erkennt, die in AD deaktiviert oder gelöscht sind. Das Problem besteht darin, wie erkannt werden kann, dass ein vorhandener aktueller Benutzer inaktiv ist oder aus AD gelöscht wurde.

Hinweis:
Der empfohlene Ansatz besteht darin, Benutzerdatensätze und alle anderen Arten von Datensätzen zu *deaktivieren* und nicht zu löschen. Jeder Datensatz ist mit anderen Datensätzen verknüpft, und durch das Löschen eines Datensatzes werden alle Beziehungen zu diesen anderen Datensätzen zerstört. Durch das Deaktivieren von Datensätzen bleiben diese Beziehungen bestehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchen Sie mithilfe des Felds userAccountControl nach inaktiven LDAP-Konten

Identifizieren, wenn ein Active Directory-Benutzer (AD) gelöscht (oder inaktiv gemacht) wird

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Eine Methode besteht darin, den aktiven Status von AD-Benutzern nachzuverfolgen und eine Geschäftsregel zu erstellen, um die entsprechenden Konten zu aktualisieren, wenn ein AD-Konto inaktiv ist.

Prozedur

1. Erstellen Sie ein neues Zeichenfolgenfeld in der Benutzertabelle [sys_user], um den Wert des Felds AD **userAccountControl nachzuverfolgen**.
   Beispiel: `u_ad_user_account`.
2. Erstellen Sie ein LDAP-Transformationsskript, um den Feldwert festzulegen.

   Example

   ```
   target.u_ad_user_account = source.userAccountControl
   ```

3. Aktualisieren Sie den LDAP-Filter, um deaktivierte AD-Konten anzuzeigen.

   Example
   Hier ist ein Beispiel für einen Filter.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   Hier ist ein Beispiel für einen Ersatzfilter, den Sie verwenden können.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. Erstellen Sie eine onChange-Geschäftsregel, um das aktive Feld auf „false“ zu setzen, wenn das Feld u_ad_user_account den Wert 514 hat.
   „514“ zeigt einen inaktiven Account an.

Beispiele für LDAP-Skripts

In den folgenden Skriptbeispielen wird davon ausgegangen, dass Sie Active Directory (AD) für Ihren LDAP-Server verwenden.

userAccountControl Attributwerte Skript

In diesem Beispiel wird die Quelle für die Attributwerte userAccountControl getestet, die einem deaktivierten Benutzer (514 oder 546) zugeordnet sind.

```
//Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol == '546'){
  target.active=false;
  target.locked_out=true;
}
```

Hier ein Beispiel mit einer Bit-weisen Prüfung:

```
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
if(source.u_useraccountcontrol & 2){
  active = false;
}
```

userAccountControl-Attributskript

In diesem Beispiel wird das Attribut userAccountControl untersucht, es wird jedoch nicht auf bestimmte Werte getestet. Sie enthält auch die Option zum erneuten Aktivieren von LDAP-Benutzerkonten.

```
/*
* Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
* Convert the userAccountControl attribute back to a hex value
*/
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
* The only digit we care about is the final one
* A final hex digit value of '2' in 'ctrl' means disabled
*/
if(ctrl.substr(-1) == "2"){

  //Deactivate and lock the user account
  target.active = false;
  target.locked_out = true;

  //Ignore any insert of a disabled record
  if(action == 'insert'){
    ignore = true;
  }
}
/* Optional: Uncomment else block to reactivate and unlock the user account
else {
  target.active = true;
  target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

onBefore-Transform Map-Skript

Hier ist ein Beispiel für ein onBefore-Transformationszuordnungsskript. Das Skript identifiziert deaktivierte Datensätze und Datensätze, die eingefügt werden. Wenn eine Einfügung eines deaktivierten Benutzers erfolgt, ignoriert die Vorgangstransformation den Datensatz.

```
//Ignore any insert of a disabled record as defined by the 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert'){
  ignore = true;
}
```

DN-Mitgliedsskript

Dieses Skriptbeispiel bietet Flexibilität, indem nicht auf die Werte 546 und 514 userAccountControl zurückgegriffen wird, sondern stattdessen überprüft wird, ob der Benutzer Mitglied eines bestimmten Distinguished Name (DN) ist. Sie können dieses Skript entweder im Feld „ **Skript** “ des Datensatzes „Tabellentransformationszuordnung“ oder in einem onBefore-Transformationszuordnungsskript verwenden.

```
//Deactivate LDAP-disabled users during transform based on OU membership in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1){
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  target.active = false;
  target.locked_out = true;
}
```

Active Directory-Anwendungsmodus (ADAM)

Active Directory Application Mode (ADAM) ist ein LDAP-konformer Verzeichnisdienst (Lightweight Directory Access Protocol).

Hinweis:
Für das Verständnis dieses Themas sind grundlegende Kenntnisse von Microsoft Windows Server und Active Directory erforderlich. Sie benötigen auch Administratorrechte für den Server, den Sie für ADAM konfigurieren.

Dies sind Beispielverfahren. Aufgrund von Installations- und Umgebungsvariationen können wir keinen direkten Support anbieten. Wir empfehlen die Zusammenarbeit mit einem Microsoft -Berater.

ADAM lässt sich einfach installieren und wird als Service unter Windows ausgeführt. Es kann vollständig angepasst und als Anwendungskomponente verteilt oder als eigenständiges LDAP-Verzeichnis verwendet werden. ADAM verwendet dieselben Technologien wie Active Directory-Domänencontroller (einschließlich Replikations- und Delegierungsfunktionen) und verfügt über eigene Verwaltungs- und Anpassungsfunktionen. Er kann als Windows -Service ausgeführt werden. ADAM kann unter den Betriebssystemen Windows XP, 2000, 2003 und 2008 installiert werden. ADAM ist in Windows Server 2003 R2 und Windows Server 2008 enthalten. Ein Download für frühere Betriebssysteme ist verfügbar unter http://www.microsoft.com/downloads http://www.microsoft.com/downloads.

Sicherheit

Einige Sicherheitsrichtlinien des Unternehmens verbieten externen Lieferanten und Partnern die direkte Verbindung mit einem Active Directory-Domänencontroller (AD). Wenn die Weitergabe bestimmter AD-Objekte oder -Attribute an einen externen Lieferanten oder Partner verboten ist, kann der Zugriff auf Objekte und Attribute mithilfe von AD-Sicherheitszugriffssteuerungseinträgen (ACE oder ACL) blockiert werden. Abhängig von den Sicherheitsanforderungen kann diese Methode die Integration komplex machen. Es wird empfohlen, mehrere Domänen und Gesamtstrukturen zu konsolidieren. Wenn alle LDAP-Importe und -Authentifizierungen über eine einzige Quelle geleitet werden müssen, kann ADAM als konsolidierte Quelle verwendet werden. Mit Release Windows 2008 wurde diese Funktionalität in Light-Weight-Directory Service, LDS umbenannt. Installation und Konfiguration ähneln denen von Windows Server 2003 R2.

Empfohlene Wissensartikel

Für diese Aufgabe müssen Sie AD, Objektklassen und Attribute verstehen. Für eine erfolgreiche Integration müssen Sie mit der aktuellen AD-Objektstruktur vertraut sein, mit Active Directory-Delegierungen vertraut sein und eine Strategie haben, wie und zu welchen Zwecken ADAM verwendet werden kann. Wenn Sie mit AD oder ADAM nicht vertraut sind, arbeiten Sie mit Ihrem AD-Administrator zusammen, um eine neue ADAM-Umgebung zu konfigurieren.

Treuhänder

Wenn *userProxy-* Objekte verwendet werden, muss der Computer, auf dem ADAM gehostet wird, Mitglied der Domäne mit den AD-Konten oder Mitglied einer vertrauenswürdigen Domäne sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Interne Konnektivität

Wenn `userProxy-` Objekte verwendet werden, muss der ADAM-Computer in der Lage sein, eine Verbindung zu den zugehörigen Domänencontrollern herzustellen, um die Proxy-Authentifizierung durchzuführen.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Instanz mit ADAM konfigurieren

Bei der ersten Installation werden die ADAM-Dateien auf Ihren Computer kopiert, die erforderlichen Komponenten werden registriert und die Anwendungsverknüpfungen erstellt.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden alle Anwendungsdateien im Verzeichnis %systemroot% \ADAMinstalliert.

- Windows Server 2003 R2 - ADAM kann mit installiert werden **Systemsteuerung > Software hinzufügen und entfernen > Manager für optionale Komponenten**.
- Windows Server 2000 und Windows XP – http://www.microsoft.com/downloads von Microsoft heruntergeladen.

Erstellen Sie den ersten Instanzservice, der als erster von ADAM gehosteter Verzeichnisdienst fungiert. Führen Sie einen der folgenden Schritte aus:

Prozedur

- Führen `Sie adaminstall.exe` aus dem ADAM-Ordner aus.
- Verwenden Sie die Verknüpfung **ADAM-Instanz erstellen** aus dem **Startmenü > Programme > ADAM** Ordner.

1. Wählen Sie die Installationsoption **Eine eindeutige Instanz** aus.

   Hinweis:
   Sie können diese Option verwenden, um ein Instanzreplikat auf einem zweiten Server zu installieren, um ein fehlersicheres System bereitzustellen.

2. Füllen Sie die Felder aus.

ADAM-Instanz

Feld	Beschreibung
Instanzname	Wird hauptsächlich zum Identifizieren des Windows Servicenamens und des Anzeigenamens verwendet
Ports	legt die Portnummern fest, die für LDAP- und LDAPS-Listener verwendet werden sollen. Der Standard-LDAP-Port ist 389, LDAPS ist 636. Wenn diese Ports auf dem Server verwendet werden, wählt der Setup-Assistent neue Ports aus. Arbeiten Sie mit Ihrem Netzwerkadministrator zusammen, um die besten zu verwendenden Ports zu ermitteln

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendungsverzeichnispartition	erstellt eine Anwendungsverzeichnispartition. In diesem Schritt nicht erforderlich. Wir empfehlen, die neue Partition jetzt zu erstellen. Es wird empfohlen, denselben eindeutigen Namen wie für die Gesamtstruktur oder Domäne zu verwenden, die Domäne der höchsten Ebene jedoch durch adam anstelle von com oder local zu ersetzen. Wenn Ihre Gesamtstrukturpartition beispielsweise *dc=myCompany,dc=com*ist, können Sie die ADAM-Partition als *dc=myCompany,dc=adam*erstellen.
Dateispeicherorte	wählt die Speicherorte für die ADAM-Partitionsdaten aus.
Auswahl des Servicekontos	wählt ein Servicekonto aus, unter dem die Instanz ausgeführt wird. Für eigenständige Services können Sie das standardmäßige Netzwerkservicekonto verwenden. Wenn Sie Replikate verwenden möchten, müssen Sie ein Konto verwenden, das Zugriff auf alle ADAM-Instanzen hat.
ADAM-Administratoren	die Delegierung im ADAM-Verzeichnis, die die integrierte Windows-Authentifizierung nutzt. So wird der anfängliche Zugriff für die Administration gewährt. Sobald dem ursprünglichen Konto Rechte gewährt wurden, delegiert dieser Benutzer oder diese Gruppe Rechte an andere Windows- oder ADAM-Benutzer. Sie können die Standardeinstellung auswählen, um nur dem aktuellen Benutzer Administratorzugriff zu gewähren, oder je nach Anforderungen einem anderen Benutzer oder einer anderen Gruppe Zugriff gewähren.
Importieren Sie LDIF-Dateien	die zu importierenden Dateien. MS-UserProxy ist die wichtigste zu importierende Datei, aber es lohnt sich, alle verfügbaren Dateien hinzuzufügen, da das Schema nur wenig Overhead hat und Sie sich keine Sorgen machen müssen, es später zu erweitern, wenn sich Ihre Anforderungen ändern. Bestätigen Sie die Details, und der Assistent schließt die Konfiguration ab.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Richten Sie die ADAM-Konsole ein

Richten Sie die ADAM-Konsole ein. Obwohl es viele Ähnlichkeiten zwischen ADAM und Active Directory gibt, kann die Verwaltung sehr unterschiedlich sein, da es keine Verwaltungskonsole für **Benutzer und Computer** gibt.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Der Großteil der allgemeinen Administration wird über die ADAM ADSI MMC-Konsole ausgeführt, die über das **ADAM** -Startmenü verfügbar ist. Wenn Sie die ADAM ADSI-Konsole zum ersten Mal ausführen, müssen Sie eine Verbindung zur von Ihnen erstellten Partition herstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das Element **ADAM ADSI-Bearbeitung** im linken Frame.
2. Geben Sie der neuen Verbindung einen Namen, und aktualisieren Sie die Felder „Servername“ und „Port“ mit den Informationen, die beim Erstellen der Instanz verwendet wurden.
3. Wählen Sie einen **eindeutigen Namen** oder **Benennungskontext** aus, und geben Sie den eindeutigen Namen der zuvor erstellten Anwendungspartition an.
   Sie können eine Verbindung zu den Partitionen *„Konfiguration“ und „Schema* “ herstellen, um erweiterte Konfigurationsoptionen zu erhalten.
   Sie sollten jetzt in der Lage sein, die Partition und die Standardcontainer für LostAndFound, NTDS-Kontingente und Rollen anzuzeigen. Der Rollencontainer wurde noch nicht konfiguriert.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Erstellen Sie Container und Organisationseinheiten für ADAM

Gruppieren Sie in ADAM gespeicherte Objekte logisch in Containern und Organisationseinheiten (OE), genau wie in Active Directory.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Stammpartition, und navigieren Sie zu **Neu** > **Objekt** > **organizationUnit**.

   Hinweis:
   Sie können auch die Liste der anderen verfügbaren Objekte anzeigen. Diese Liste variiert je nach den beim Import der LDF-Dateien installierten Schemaerweiterungen.

2. Wenn Sie zur Eingabe eines Werts aufgefordert werden, geben Sie den Namen der OE ein, z. B. Benutzer.
   Auf dem Bildschirm wird die Schaltfläche **Weitere Attribute** angezeigt.
3. Verwenden Sie die Schaltfläche, um zusätzlichen Attributen Werte zuzuweisen.
   Für die OEs und Container sind keine zusätzlichen Werte erforderlich.
   Nach dem Erstellen der OEs werden die neuen OEs als untergeordnete Elemente des Stammobjekts aufgelistet.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Delegierung mit ADAM

Sobald die OE-Struktur erstellt wurde, definieren Sie die Berechtigungsdelegierungen, um die Objekte ordnungsgemäß für eingeschränkte Benutzer zu sichern.

Wie bei Active Directory gibt es zwei allgemeine Möglichkeiten, Berechtigungen zu erteilen:

- Fügen Sie Benutzer zu einer Gruppe hinzu, der bereits die entsprechenden Berechtigungen zugewiesen sind.
- Definieren Sie neue Berechtigungen für die ADAM-Objekte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für diese Aufgabe besprechen wir Berechtigungen auf Objektebene. Weitere Informationen zu Gruppenmitgliedschaften finden Sie im Abschnitt „Gruppenadministration“.

Da es keine Benutzer- und Computerkonsole für ADAM gibt, werden alle Berechtigungen auf Objektebene mit dem Active Directory-Dienstprogramm *DSACLS.exe*definiert. Diese Datei befindet sich im ADAM-Programmverzeichnis. Beim Ausführen von ADAM-Dienstprogrammen ist es am besten, die Eingabeaufforderung für ADAM-Tools zu starten. Dadurch wird sichergestellt, dass die richtigen Versionen der Tools vorhanden sind. DSALCS wird zum Anzeigen und Festlegen von Objektzugriffsrechten verwendet.

Beispiel: "dsacls \\localhost:50010\dc=myCompany,dc=adam" zeigt die Berechtigungen an, die dem Stamm der Partition *dc=myCompany,dc=adam* zugewiesen sind, die auf dem lokalen Host, Port 50010, ausgeführt wird. DSACLS ist ein komplexes Tool zum Erstellen komplexer Delegierungen. *„DSACLS /?“ ausführen* für Nutzungshinweise.

Zugehörige Informationen

Erstellen Sie Container und Organisationseinheiten für ADAM

Verwenden Sie ADAMSync, um ADAM auszufüllen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM-Objekte werden ausgefüllt

ADAM-Objekte umfassen Benutzerobjekte, UserProxy-Objekte und Gruppenobjekte.

Benutzerobjekte

Benutzer können mit der ADAM-ADSI-Bearbeitungskonsole genau wie bei der Erstellung von OEs erstellt werden. Benutzer können auch mit AD-Befehlszeilentools verwaltet werden, was den Umfang dieses Dokuments sprengt. Das einzige obligatorische Attribut für neue Benutzerobjekte ist *cn*, ein Kurzname oder der vollständige Name des Benutzers. Es gibt auch eine Vielzahl optionaler Attribute, die den Active Directory-Benutzerattributen ähneln. Sie können auf die vollständige Liste der Attribute zugreifen, indem Sie Eigenschaften aus dem Benutzerobjekt auswählen.

UserProxy-Objekte

Für die ServiceNow LDAP-Integration empfehlen wir die Verwendung *von UserProxy-* Objekten in ADAM, wodurch ein Proxy-Account erstellt wird, der mit dem zugehörigen AD-Benutzeraccount verknüpft ist. Auf diese Weise kann ADAM Anmeldeinformationen mit AD-Benutzernamen und Passwörtern aus der Domäne authentifizieren, ohne dass ServiceNow eine direkte Verbindung zum Domänencontroller herstellt. *UserProxy-* Objekte sind AD- und ADAM-Benutzerobjekten sehr ähnlich, außer dass sie keine Passwörter speichern und über ein Attribut *objectSID verfügen*, das die SID aus dem verknüpften AD-Benutzerobjekt enthält. So funktioniert der Proxy. *UserProxy-* Objekte werden mit der *ADSIEdit* -Konsole oder mit Befehlszeilentools erstellt. Dies kann jedoch langwierig sein. Es wird empfohlen, einen automatisierten Prozess wie unten definiert zu verwenden.

Gruppenobjekte

Gruppen werden mit der ADSIEdit-Konsole und den AD-Befehlszeilentools erstellt. Gruppenkonzepte ähneln AD und werden verwendet, um Gruppen und Mitglieder in ServiceNowzu integrieren. Der größte Unterschied besteht darin, dass ADAM-Gruppen Mitglieder aus ADAM oder aus vertrauenswürdigen AD-Domänen enthalten können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisierung der ADAM-Objekterstellung

Wenn Sie Active Directory-Konten mit ADAM synchronisieren möchten, empfehlen wir Ihnen die Verwendung von Microsoft *ADAMSync* Tool. Dies ist die häufigste Verwendung von ADAM für die ServiceNow LDAP-Integration.

Über Berechtigungsdelegierung

ADAM enthält einige integrierte Gruppen mit Standardberechtigungen. Diese Gruppen befinden sich im Container `cn=roles,dc=myCompany,dc=adam`. Diese ähneln Gruppen auf Domänenebene und haben Rechte für Objekte in der aktuellen Partition. Ähnlich wie bei AD-Gesamtstrukturen können Sie auch eine höhere Berechtigungsebene festlegen, indem Sie die Standardgruppen in `cn=roles,cn=configuration,dc=myCompany,dc=adam verwenden`. Sie müssen eine Verbindung zur Konfigurationspartition in `ADSIEdit herstellen`. Die Gruppe „Administratoren“ enthält standardmäßig das während des Setups angegebene Konto. Dieses Mitglied ist nicht immer sichtbar, da es über die Konfigurationsgruppen geerbt wird. Administratoren haben die vollständige Kontrolle über alle Partitionsobjekte. Die Gruppe „Leser“ enthält standardmäßig keine Mitglieder und hat Lesezugriff auf alle Objekte in der Partition. Die Benutzergruppe ist eine dynamische Gruppe, genau wie in Active Directory. Vorübergehend enthält sie alle in der Partition erstellten ADAM-Benutzer.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Test und Problembehandlung des ADAM-Setups

Das primäre Tool zum Testen ist LDP. Auf diese Weise können Sie die Benutzerauthentifizierung vollständig testen.

Der Großteil der Objektverwaltung kann über die ADAM-ADSI-Bearbeitungskonsole durchgeführt werden, die Zugriff auf die gesamte Sammlung von Objekten und Attributen bietet. Die höchste Stufe der Steuerung und Problembehandlung von ADAM-Services ist die Verwendung des Windows -Service, der während des Instanz-Setups erstellt wurde. Der Servicename variiert und hängt vom Namen der erstellten Instanz ab. Dieser Service muss ausgeführt werden, damit der ADAM-Service ausgeführt werden kann. Wenn Verbindungsprobleme auftreten, sollten Sie die Netzwerkkonfigurationen überprüfen, um sicherzustellen, dass Sie über den erforderlichen Netzwerkzugriff verfügen, um eine Verbindung zum Server und ADAM-Port herzustellen. Für jede installierte ADAM-Instanz wird ein Windows-Ereignisprotokoll erstellt. Dies ist auch ein großartiges Tool für die Problembehandlung von ADAM-Services.

Das Windows Sicherheitsereignisprotokoll ist auch hilfreich bei der Problembehandlung `von userProxy-` Authentifizierungen. Alle `userProxy-Anmeldeversuche` werden im Sicherheitsprotokoll protokolliert und verweisen auf die Remote-Client-Geräteadresse, den eindeutigen Namen des Benutzers, der sich anmelden möchte, und das Ergebnis oder den Statuscode.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Sicherung und Wiederherstellung mit ADAM

Alle ADAM-Daten können mit standardmäßigen Dateisystem-Sicherungsmethoden gesichert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Redundanz

ADAM verfügt über integrierte Replikationsdienstprogramme, die auf derselben Technologie wie AD basieren. Ein vollständiges Lese- und Schreibreplikat einer ADAM-Partition kann auf demselben oder einem anderen Computer vorhanden sein. Sie können dieses Replikat auf verschiedene Arten verwenden, um eine fehlersichere LDAP-Integration mit der Instanz bereitzustellen. Eine Möglichkeit besteht darin, beide Partitionen für die Instanz durch die Firewall verfügbar zu machen und beide Server im Feld LDAP-Eigenschaftenserver zu definieren.

Zugehörige Informationen

Active Directory-Anwendungsmodus (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Verwenden Sie LDAPS mit ADAM

Die Standardkonfiguration für *die userProxy-* Objektauthentifizierung besteht darin, die LDAPS-Kommunikation (sichere LDAP) zu erzwingen. LDAPS erfordert SSL-Zertifikate, um den Netzwerkverkehr zu sichern.

Um diese Anforderung zu entfernen, nehmen Sie die folgende Änderung vor, indem Sie die *ADSIEdit* -Konsole verwenden, die mit der Konfigurationspartition verbunden ist.

```
Object: CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

Starten Sie den ADAM-Service neu, um die neue Einstellung zu verwenden.

Um sichere Bindungen zu unterstützen und die übertragenen Benutzer- und Passwortinformationen zu verschlüsseln, muss auf dem Server und jedem LDAP-Client ein SSL-Zertifikat installiert sein. Da der ADAM-Service nur begrenzt und kontrolliert verwendet werden kann, ist es möglich, ein selbstsigniertes Zertifikat zu verwenden, das die Anforderungen erfüllt, ohne Zertifikatkosten zu verursachen oder eine Zertifizierungsstellen-Infrastruktur (CA) aufzubauen. Wenn Sie bereits eine Zertifizierungsstelle haben, können Sie ein Zertifikat ausstellen. Erstellen Sie andernfalls ein selbstsigniertes Zertifikat.

Erstellen eines selbstsignierten Zertifikats

Zur Verwendung des Dienstprogramms *selfssl* muss Internet Information Services (IIS) installiert sein. Dieser Service kann entfernt werden, nachdem Sie das Zertifikat generiert haben. Sie können das Dienstprogramm selfssl.exe aus dem IIS Resource Kit abrufen. Wenn IIS bereits installiert ist, erstellen Sie eine neue Website, damit die aktuellen Websites während der Zertifikatgenerierung nicht betroffen sind. SelfSSL muss das neue selbst ausgestellte Zertifikat vorübergehend an eine gültige Website anhängen.

Selfssl ist ein Befehlszeilentool und verfügt über die folgenden allgemeinen Parameter.

Selfssl-Parameterbeschreibungen

Parameter	Beschreibung
/T	Fügt das Zertifikat zu „Vertrauenswürdige Zertifikate“ auf dem lokalen Computer hinzu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Selfssl-Parameterbeschreibungen (Fortsetzung)

Parameter	Beschreibung
/N:cn	Legen Sie den allgemeinen Namen des Zertifikats fest. Dieser muss mit dem vollständig qualifizierten Domänennamen des Servers übereinstimmen, der den Webservice mit dem Zertifikat ausführt
/K	Legt die Stärke der Schlüsselgröße in Bits fest
/V	Anzahl der Tage, die das Zertifikat gültig ist
/S	ID der Website, an die das Zertifikat angehängt werden soll
/P	IP-Port des Webservice

Das Attribut des allgemeinen Namens muss mit dem externen Namen oder der Adresse übereinstimmen, die die Instanz für die Verbindung mit Ihrem ADAM-Computer verwendet. Sie müssen die Site-ID der IIS-Website abrufen, es sei denn, Sie verwenden die Standardwebsite, die 1 ist und nicht im selfssl-Befehl definiert werden muss. Ein Beispielbefehl zum Generieren eines Zertifikats für myCompany wäre:

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /P:50001 /T
```

Diese Anweisung erstellt ein Zertifikat, das 10 Jahre lang gültig ist. Legen Sie den Wert auf eine beliebige Dauer fest. Beachten Sie jedoch, dass das neue Zertifikat generiert und an die Instanz übermittelt werden muss, bevor das alte abläuft. Wir empfehlen, das Ablaufdatum auf dem Zertifikat zu notieren.

Sobald das Zertifikat generiert wurde, können Sie es von der Website entfernen oder die gesamte Website löschen, wenn Sie eine temporäre Website erstellt haben.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Weisen Sie das Zertifikat ADAM zu

Installieren Sie ein SSL-Zertifikat auf dem Server und einem beliebigen LDAP-Client, um sichere Bindungen zu unterstützen und die übertragenen Benutzer- und Passwortinformationen zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Da der ADAM-Service nur begrenzte und kontrollierte Verwendungszwecke bietet, ist es möglich, ein selbstsigniertes Zertifikat zu verwenden, um Ihre Anforderungen zu erfüllen, ohne Zertifikatkosten zu verursachen oder eine Zertifizierungsstellen-Infrastruktur (CA) aufzubauen.

Prozedur

1. Öffnen Sie die MMC-Konsole für Zertifikate, und erstellen Sie zwei Konsolenverbindungen, eine für lokale Computerzertifikate und eine für lokale Computerservices-Zertifikate im neuen ADAM-Service.
   Das neue Zertifikat finden Sie unter Zertifikate (Lokaler Computer)\Personal\Certificates.
2. Kopieren Sie das Zertifikat in den Container für den ADAM-Service Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name\Trusted Root Certificates\Certificates, und kopieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie das Zertifikat nach Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name \Personal\Certificates.

3. Öffnen Sie die Registerkarte „Details“ für das kopierte Zertifikat, notieren Sie den Datumsstempel Gültig ab, und weisen Sie Lesezugriff auf die Zertifikatschlüsseldatei zu.
   Wechseln Sie zu C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Microsoft \Crypto\RSA\MachineKeys, und identifizieren Sie das Zertifikat mit dem entsprechenden Zeitstempel.
   Weisen Sie dem Servicekonto, auf dem ADAM ausgeführt wird, Lese- und Ausführungsrechte zu. Standardmäßig ist dies **Netzwerkservice**.
4. Starten Sie den ADAM-Service neu, um das neue Zertifikat zu aktivieren.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Exportieren Sie das Zertifikat des öffentlichen Schlüssels

LDAPS-Clients, einschließlich der -Instanz, benötigen das Zertifikat des öffentlichen Schlüssels, um eine sichere Verbindung zu ADAM herzustellen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Exportieren Sie aus den oben verwendeten Serverzertifikatkonsolen einen öffentlichen Schlüssel, der von den Clients verwendet werden soll.

Prozedur

1. Wählen Sie das Zertifikat aus, klicken Sie mit der rechten Maustaste, und wählen Sie **alle Aufgaben/ Export**aus.
   Exportieren Sie den privaten Schlüssel nicht. Wählen Sie das standardmäßige DER-codierte binäre X.509-Format aus, und geben Sie den Namen der Exportdatei an.
2. Installieren Sie das öffentliche Zertifikat auf den LDAP-Clients, die über LDAPS eine Verbindung zum Server herstellen.
   Wenn Sie dazu aufgefordert werden, fügen Sie das Zertifikat dem Speicher der *`vertrauenswürdigen Stammzertifizierungsstellen`* hinzu.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Zugriffskonto für Active Directory-Anwendungsmodus (ADAM).

Das System erfordert ein Benutzerkonto, um die Objektinformationen des Active Directory-Anwendungsmodus (ADAM) zu lesen, die in die Anwendungsinstanz importiert werden.

Erstellen Sie das Konto mit einer der folgenden Methoden:

- Erstellen Sie ein lokales ADAM-Benutzerkonto, weisen Sie ihm ein Passwort zu und weisen Sie ihm Berechtigungen zu.
- Weisen Sie einem Domänenkonto Windows in der ADAM-Partition eine Berechtigung zu.
- Verwenden Sie ein *`userProxy-`* Konto.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie ADAM als LDAP-Quelle verwenden, müssen Sie den vollständig qualifizierten eindeutigen Namen (FQDN) des ADAM-Kontos im Feld „ **Eindeutiger Anmeldename** “ des LDAP-Servers der Instanz angeben.

Zugehörige Informationen

Active Directory-Anwendungsmodus (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Testen Sie die LDAPS-Verbindungen

Testen Sie die LDAPS-Verbindungen. Es gibt zwei Konsolenverbindungen, eine für lokale Computerzertifikate und die andere für lokale Computerservices-Zertifikate im neuen ADAM-Service.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Führen `Sie LDP.exe` aus dem ADAM-Installationsordner c:\windows\adamaus.
   Vergewissern Sie sich, dass die ADAM-Version ausgewählt ist, da dies nicht der standardmäßige Windows LDP-Client ist.
2. Öffnen Sie eine neue Verbindung über das Menü **Verbindung/Verbinden**.
   Der Servername muss mit dem CN übereinstimmen, der dem Zertifikat zugewiesen ist.
3. Geben Sie den **LDAPS-Port** ein, und aktivieren Sie das Kontrollkästchen **SSL**.
   Das Ergebnis einer erfolgreichen Verbindung sind einige allgemeine Serverinformationen und keine Fehler.
4. Binden Sie sich an den Service an (melden Sie sich an).
   Um typische LDAP-Client-Verbindungen zu replizieren, wählen Sie die Option Einfache Bindung aus. Geben Sie einen gültigen eindeutigen ADAM-Benutzer- oder `userProxy-` Namen in das Benutzerfeld und das zugehörige Passwort ein.
   Wenn die Meldung „Authentifiziert als:…“ zurückgegeben wird. dann haben Sie erfolgreich eine Verbindung über LDAPS hergestellt.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Verwenden Sie ADAMSync, um ADAM auszufüllen

Administratoren verwenden MS ADAMSync, um LDAP-Verzeichnisse auszufüllen, die MS ADAM verwenden.

Hinweis:

In diesem Dokument wird davon ausgegangen, dass Sie mindestens über grundlegende Kenntnisse von Microsoft Windows Server, Active Directory und ADAM verfügen und bereits eine funktionsfähige Active Directory-Anwendungsmodus (ADAM) Instanz mit einer Partition haben.

Dies sind Beispielverfahren. Aufgrund der Komplexität und der Tatsache, dass sie in Ihrer Umgebung ausgeführt wird, können wir keinen direkten Support bieten. Wir empfehlen Ihnen, mit Microsoft oder einem Microsoft -Berater zusammenzuarbeiten, wenn Probleme auftreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald ADAM installiert und die erste Partition erstellt wurde, können Sie sie mit Objekten ausfüllen.

Die folgenden Optionen sind verfügbar:

- Manuelle Objekterstellung mit GUI oder Skripts. Diese Option ist ineffizient und langsam.
- Integrieren Sie mit Active Directory mithilfe von Microsoft Integration Information Server. Diese Option bietet letztendlich die meiste Flexibilität und Funktionalität, erfordert jedoch einige erweiterte Konfigurationen. Es ist eine kostenlose Version von MIIS verfügbar, die mit Active Directory, ADAM undMicrosoft Globale Adresslisten von Exchange kompatibel ist. Sofern Sie nicht bereits Erfahrung mit MIIS haben, empfehlen wir Ihnen, nicht zu versuchen, eine neue Umgebung nur für die LDAP-Integration zu implementieren.
- Verwenden Sie ADAMSync, ein Synchronisierungstool, das Microsoft mit ADAM bereitstellt. Dies ist die Option, die hier erläutert wird.

Definieren Sie ADAM-Benutzerkonten

Definieren Sie Benutzerkonten in ADAM. Ein Benutzeraccount wird für die Instanz verwendet, mit der eine Verbindung hergestellt werden soll, und der andere Benutzeraccount ist für ADAMSync.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Konten können lokale ADAM-Benutzerobjekte, UserProxy-Objekte oder ein Windows-Konto aus einer vertrauenswürdigen Domäne sein.

Das Konto *ADAM User* erfordert schreibgeschützten Zugriff auf die Verzeichnisstruktur, die Sie in Ihre Instanz importieren. Die beste Möglichkeit, dies zu erreichen, besteht darin, den Account dem Mitgliedsattribut in der Lesergruppe hinzuzufügen, die sich in cn=roles,dc=myCompany,dc=adam befindet.

Neue ADAM-Benutzerkonten sind standardmäßig deaktiviert. Sie müssen die neuen Konten aktivieren und ein Passwort festlegen.

Prozedur

1. Aktivieren Sie Benutzer, indem Sie das Attribut msDS-UserAccountDisabled in FALSCH ändern.
2. Klicken Sie mit der rechten Maustaste auf das Benutzerobjekt, und setzen Sie das Passwort zurück.
3. Testen Sie die neuen Konten mithilfe des in Active Directory-Anwendungsmodus (ADAM) definierten LDP, um sicherzustellen, dass sie eine Verbindung herstellen können.
   Verwenden Sie den **LDAP** > **Ansicht/Struktur** Option, wobei Basis-DN leer gelassen wird, um sicherzustellen, dass Sie die Objekte im Verzeichnis mit den neuen Konten anzeigen können. Die Konfiguration, das Schema und die Domänenpartition sollten im linken Bereich sichtbar sein. Durchläuft die Domänenpartition. Wenn Sie ein neues lokales ADAM-Konto verwenden, wird „Keine untergeordneten Elemente“ angezeigt, was bedeutet, dass Sie keinen Lesezugriff auf die Objekte haben. Überprüfen Sie die Setup-Gruppenmitgliedschaften, und wiederholen Sie den Test.

   ADAMSync verwendet das Konto *ADAMSync User*, um Objekte in der ADAM-Partition zu verwalten. Für diesen Account sind Rechte auf Administratorebene erforderlich, da er ADAM-Objekte erstellt, aktualisiert und löscht.

   ADAMSync verwendet das Konto *ADAMSync AD*, um die AD-Objekte zu lesen, die mit ADAM synchronisiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie ADAMSync ein

ADAMSync ist in Windows Server 2003 R2 enthalten. Laden Sie ADAMSync herunter, und installieren Sie es, wenn Sie ein anderes Betriebssystem verwenden.

Erweitern des Schemas

Das ADAM-Schema muss erweitert werden, um ADAMSync zu unterstützen.

1. Führen Sie den folgenden Befehl aus c:\windows\adam aus, um die ADAMSync-Schemaerweiterungen zu importieren. Möglicherweise müssen Sie den server:port ändern und Anmeldeinformationen hinzufügen, wenn der aktuelle Benutzer keinen Zugriff hat. Weitere Informationen finden Sie in der Datei „AdaSyncMetadata.ldf“.

```
ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
#configurationNamingContext
```

2. Machen Sie dasselbe mit MS-AdamSchemaW2k3.ldf, um Windows 2003-Attribute zu unterstützen.

```
ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
#configurationNamingContext
```

Empfohlene Schemaänderungen

Hier sind einige zusätzliche Schemaänderungen, die wir empfehlen.

1. Öffnen Sie eine neue MMC-Konsole, und fügen Sie das ADAM-Schema-Snap-in hinzu.
2. Stellen Sie eine Verbindung zur ADAM-Instanz her.
3. Erweitern Sie den Ordner Klassen, suchen Sie die Klasse userProxy, und öffnen Sie **Eigenschaften**.
4. Überprüfen Sie die folgenden optionalen Attribute auf der Registerkarte Attribute, und fügen Sie alle hinzu, die noch nicht vorhanden sind.
   - Unternehmen
   - department
   - gegebenNane
   - E-Mail
   - PhysicalDeliveryOfficeName
   - sAMAccountName
   - sn
   - phoneNumber
   - Titel
   - userAccountControl
   - userPrincipalName
5. Starten Sie den ADAM-Service neu, um die neuen Einstellungen zu aktivieren.

Installieren Sie die ADAM-Konfigurationsdatei

Installieren Sie die ADAM-Konfigurationsdatei über die Windows-Befehlszeile.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Installieren Sie die Konfigurationsdatei.

```
C:\WINDOWS\adam>adamsync /install localhost:50000 MS-AdamSyncConf-SNC.XML
```

2. Führen Sie die Synchronisierungsdatei aus, um sich bei der Konsole anzumelden.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. Überprüfen Sie die Ergebnisse mithilfe der ADSIEdit-Konsole.
   Sie sollten die neuen Objekte und Attribute sehen, die von ADAMSync erstellt wurden.
4. Führen Sie ldap aus, um die UserProxy-Authentifizierung zu testen.
   Automatisierung des Synchronisierungsprozesses

   Richten Sie den Synchronisierungsprozess als Windows geplante Aufgabe ein. Sie müssen die Anmeldeinformationen entweder in der Konfigurationsdatei oder in der Befehlszeile angeben oder die geplante Aufgabe mit einem Konto ausführen, das Zugriff hat.

   Spezielle Hinweise

   - Sie können mehrere Konfigurationsdateien und regelmäßige Aufgaben erstellen, um ADAM aus mehreren Quellen zu synchronisieren.

     In diesem Beispiel wird das Attribut sAMAccountName importiert, das als Anwendungsanmeldung verwendet werden kann. Wenn Sie die Quelle synchronisieren, müssen Sie sicherstellen, dass Sie über einen eindeutigen Attributwert verfügen, der für die Anmeldeinformationen verwendet werden kann. sAMAccountName ist innerhalb einer Domäne garantiert eindeutig, jedoch nicht über mehrere Domänen hinweg.

   - Wenn Sie Microsoft Exchange verwenden, empfehlen wir, cn=SystemMailbox*-Objekte als Teil der Objektfilterkonfiguration auszuschließen.

Beispiel für ADAM-Konfigurationsdateien

Alle Konfigurationen für ADAMSync werden in XML-Dateien gespeichert.

Standardkonfigurationsdatei mit Kommentaren

Die Standardkonfigurationsdatei MS-AdamSyncConf.xml ist in der ADAMSync-Installation enthalten. Erstellen Sie eine Kopie dieser Datei, damit Sie ein Basisbeispiel haben, auf das Sie in Zukunft zurückgreifen können. Dieses Beispiel zeigt die Standardkonfigurationsdatei mit hinzugefügten Kommentaren.

```
<?xml version="1.0"?>
<doc>
 <configuration>
<!-- Sync File Description -->
<description>MyCompany ADAMSync Configuration</description>
  <security-mode>object</security-mode>;
<!-- source-ad-name = fqdn of the domain controller -->;
  <source-ad-name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
<!-- source-ad-partition = root AD domain partition -->;
  <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<!-- source-ad-account = use this to specify an account to connect to AD -->;
<!-- if not used, the current user will be used  -->;
 <source-ad-account>;</source-ad-account>;
 <account-domain>;</account-domain>;
<!-- target-dn = target ADAM OU -->;
 <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
 <query>;
<!-- base-dn = should be the root AD partition if you want all users -->;
  <base-dn>;dc=myCompany,dc=com</base-dn>;
<!-- object-filter = standard ldap query format, this will grab all users -->;
<!-- need to review results to see if you should modify this filter -->;
  <object-filter>;(objectCategory=person)</object-filter>;
  <attributes>;
<!-- include=userproxy requires objectSID to link back to the AD account -->;
   <include>;objectSID</include>;
   <include>;givenName</include>;
   <include>;sn</include>;
   <include>;description</include>;
   <include>;title</include>;
   <include>;company</include>;
   <include>;department</include>;
   <include>;mail</include>;
   <include>;physicalDeliveryOfficeName</include>;
   <include>;telephoneNumber</include>;
   <include>;sAMAccountName</include>;
  </attributes>;
 </query>;
<!-- map for user-to-userproxy object types -->;
 <user-proxy>;
  <source-object-class>;user</source-object-class>;
  <target-object-class>;userProxy</target-object-class>;
 </user-proxy>;
 <schedule>;
  <aging>;
   <frequency>;0</frequency>;
   <num-objects>;0</num-objects>;
  </aging>;
  <schtasks-cmd>;</schtasks-cmd>;
 </schedule>;
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdatei für LDAP-Filter

Sie können eine beliebige Filterebene im Wert object-filter in der Konfigurationsdatei angeben. Verwenden Sie die standardmäßige LDAP-Abfragesyntax mit den folgenden XML-Escape-Zeichen anstelle der Standardoperatoren.

- AND = "&" ersetzen durch &
- ODER = „|“ (senkrechte Linie) ersetzen durch |
- NOT = „!“ Ersetzen durch !

Referenzkonfigurationsdatei

Hier ist eine tatsächliche Konfigurationsdatei, die als Beispiel referenziert werden kann.

```
<?xml version="1.0"?>;
<doc>;
 <configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
  <security-mode>;object</security-mode>;
  <source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
  <source-ad-partition>;dc=service-now,dc=com</source-ad-partition>;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
  <target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>;
  <query>;
   <base-dn>;dc=service-now,dc=com</base-dn>;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;userAccountControl</include>;
   </attributes>;
  </query>;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
   <aging>;
    <frequency>;0</frequency>;
    <num-objects>;0</num-objects>;
   </aging>;
   <schtasks-cmd>;</schtasks-cmd>;
  </schedule>;
 </configuration>;
 <synchronizer-state>;
  <dirsync-cookie>;</dirsync-cookie>;
  <status>;</status>;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```

Konfigurieren Sie Microsoft Active Directory für die sichere LDAPS-Kommunikation

Verwenden Sie Zertifikatpaare, um die Microsoft Active Directory (AD) LDAPS-Kommunikation zu aktivieren.

Hinweis:
Diese Verfahren wurden mit Windows 2003 R2 Standard Edition entwickelt und getestet und funktionieren mit allen Versionen von Windows 2003.

Die sichere LDAP-Kommunikation (LDAPS) ähnelt der SSL-Kommunikation (HTTPS), bei der die Daten zwischen Servern und Clients verschlüsselt werden. Um dies zu erreichen, verwenden Server und Clients gemeinsame Informationen über Zertifikatpaare. Der Server enthält das Zertifikat des privaten Schlüssels und die Clients das Zertifikat des öffentlichen Schlüssels. Diese Zertifikate sind erforderlich, um die LDAPS-Kommunikation mit Microsoft Active Directory (AD) zu ermöglichen.

Um LDAPS für Active Directory zu konfigurieren, müssen Sie:

- Stellen Sie sicher, dass die Active Directory-Domäne eingerichtet ist und die Instanz über die Firewall eine Verbindung zum Active Directory-Server herstellen kann.
- Stellen Sie sicher, dass eine Zertifizierungsstelle (CA) vorhanden ist, die ein Zertifikat für den Domänencontroller (DC) ausstellen kann. Wenn Sie noch keine CA-Infrastruktur haben, gibt es zwei Optionen.
  - Richten Sie eine eigenständige Zertifizierungsstelle ein, um das Zertifikat auszustellen
  - Fordern Sie ein Drittparteizertifikat an
- Wenn Sie bereits eine Zertifizierungsstelle haben, können Sie ein Zertifikat von einer internen Zertifizierungsstelle generieren.

Alle Zertifikate haben ein definiertes Ablaufdatum, das in den Zertifikateigenschaften angezeigt werden kann. Wenn das Zertifikat abläuft, schlägt der gesamte LDAPS-Datenverkehr fehl, und Ihre Benutzer können sich nicht mehr bei der Instanz anmelden. Um dies zu beheben, muss ein neues Zertifikat ausgestellt und in Ihrer Instanz installiert werden.

Der Standardablauf für Microsoft CA-Zertifikate beträgt ein Jahr. Externe CA-Zertifikate werden normalerweise in Schritten von einem Jahr erworben. Notieren Sie, wann Ihr Zertifikat abläuft, oder verwenden Sie die Ablaufbenachrichtigungsfunktion der Anwendung (befindet sich in). **System-LDAP** > **Zertifikate**) an. Stellen Sie sicher, dass Sie ein neues Zertifikat bereit haben, bevor das alte abläuft. So haben Sie Zeit, das neue Zertifikat zu installieren und zu testen, bevor das alte abläuft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie eine eigenständige Zertifizierungsstelle für Active Directory ein

Der erste Schritt zur Konfiguration von Microsoft Active Directory für den SSL-Zugriff besteht in der Einrichtung einer eigenständigen Zertifizierungsstelle (Certificate Authority, CA).

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Machen Sie sich keine Sorgen über die zusätzliche Ressourcennutzung, da beide erforderlichen Services (IIS und CA) nach der Ausstellung der Zertifikate deaktiviert werden können.

Prozedur

1. Installieren Sie Internet Information Server (IIS).
2. Installieren Sie Zertifizierungsstellendienste im eigenständigen Modus.
3. Vergewissern Sie sich, dass die Webanwendung „Zertifikatsservices“ installiert und aktiv ist.

Nächste Maßnahme
Erweitern Sie in der IIS-Managerkonsole den lokalen Computer, und wählen Sie *Website*saus. Der Status der **Standard-Website** muss „ *Wird*ausgeführt“ sein. Unter der **Standardwebsite** sollte auch eine Anwendung vom *Typ „CertSrv“ angezeigt*werden. Wenn die Site nicht ausgeführt wird oder die Anwendung fehlt, müssen Sie das Problem beheben, bevor Sie fortfahren.

Generieren Sie ein Zertifikat von einer internen Zertifizierungsstelle

Wenn Sie Microsoft Active Directory für den SSL-Zugriff konfigurieren, müssen Sie ein internes Zertifikat generieren und das externe Zertifikat anfordern.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Schritte gelten für Microsoft CA-Services. Wenn Sie eine andere interne CA-Plattform haben, wenden Sie sich an Ihren lokalen CA-Administrator.

Prozedur

1. Navigieren Sie auf dem Domänencontroller (DC), für den Sie ein Zertifikat erstellen möchten, zu `http://localhost/certsrv`, oder geben Sie den Namen des CA-Servers an, wenn er sich auf einem Remote-Server befindet.
2. Klicken Sie auf der Willkommensseite auf **Zertifikat***anfordern, und wählen Sie erweiterte Zertifikatsanforderung aus*.
3. Wählen Sie auf der Seite „Erweiterte Zertifikatanforderung“ die Option **Erstellen** aus, und senden Sie eine Anforderung an diese Zertifizierungsstelle.
4. Schließen Sie die erweiterte Zertifikatsanforderung wie folgt ab:

Erweiterte Zertifikatanforderungsfelder

Feld	Eintrag
Name	Der vollständig qualifizierte Domänenname (FQDN) des Domänencontrollers, der das Zertifikat anfordert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eintrag
E-Mail	Die E-Mail-Adresse der Person, die für das Zertifikat verantwortlich ist.
Unternehmen	Ihr Unternehmensname.
Einstellungen für Schlüsseloptionen	
Erstellen Sie einen neuen Schlüsselsatz	Wählen Sie es aus.
CSR	Kryptografischer Anbieter des Microsoft RSA-Kanals.
Schlüsselnutzung	Exchange
Schlüsselgröße	1024 wird empfohlen. Die Instanz unterstützt bis zu 2048.
Name des automatischen Schlüsselcontainers	Wählen Sie es aus.
Speichern Sie das Zertifikat im Zertifikatspeicher des lokalen Computers	Wählen Sie es aus.

5. Klicken Sie auf **Absenden**.
   Sie werden auf eine Seite weitergeleitet, die Ihre **Anforderungs-ID**bereitstellt. Notieren Sie sich diese ID.
6. Führen Sie die folgenden Schritte aus, um die ausstehende Anforderung zu verarbeiten:
   a. Öffnen Sie die Verwaltungskonsole der Zertifizierungsstelle.
   b. Erweitern Sie den Serverknoten, und wählen Sie **Ausstehende Anforderungen**aus.
   c. Suchen Sie die Anforderungs-ID für die Anforderung, die Sie gerade übermittelt haben, klicken Sie mit der rechten Maustaste, und wählen Sie *Alle Aufgaben/Problem aus, um die Anforderung zu genehmigen und das Zertifikat auszustellen*.
7. Führen Sie die folgenden Schritte aus, um das ausgestellte Zertifikat abzurufen:
   a. Navigieren Sie vom Domänencontroller, von dem aus Sie die Anforderung gestellt haben, zu `http://localhost/certsrv`, oder geben Sie den Namen des CA-Servers an, wenn er sich auf einem Remote-Server befindet.
   b. Wählen Sie `Status einer ausstehenden Zertifikatsanforderung anzeigen aus`.
   c. Klicken Sie auf den Link zum neuen Zertifikat.
   d. Klicken Sie auf den Link **Dieses Zertifikat installieren**.

Nächste Maßnahme
Sie müssen ein Drittparteizertifikat anfordern. Zertifikate von externen Zertifizierungsstellen können für nur 30 USD pro Jahr erworben werden. Ausführliche Informationen zum Anfordern eines Zertifikats von einer externen Zertifizierungsstelle finden Sie im Microsoft-Artikel 321051 . Nachdem es empfangen, installiert und getestet wurde, folgen Sie dem Exportverfahren.

Testen Sie die LDAPS-Konnektivität lokal

Testen Sie die LDAPS-Konnektivität nach der Installation der internen Zertifikate und Zertifikate von Drittparteien, wenn Sie Microsoft Active Directory für den SSL-Zugriff konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Stellen Sie sicher, dass Windows-Supporttools auf dem Domänencontroller (DC) installiert sind.
   Das Support-Tools-Setup (suptools.msi) befindet sich im Verzeichnis `\Support\Tools` auf Ihrer Windows Server-CD.
2. Navigieren zu **Starten** > **Alle Programme** > **Windows-Supporttools** > **Befehlszeile**.
   Geben Sie in der Befehlszeile `ldp` ein, um das Tool zu starten.
3. *Wählen* Sie im LDP-Fenster aus **Verbindung** > **Connect** und geben den lokalen FQDN und die Portnummer (636) an.
   Wählen Sie auch *SSL*aus.
   Bei Erfolg wird ein Fenster angezeigt, in dem Informationen zur Active Directory-SSL-Verbindung aufgelistet werden. Wenn die Verbindung nicht erfolgreich hergestellt werden kann, versuchen Sie, Ihr System neu zu starten, und wiederholen Sie diesen Vorgang.

Exportieren Sie das Zertifikat des öffentlichen Schlüssels, um dem LDAP-Zertifikat zu vertrauen

Exportieren Sie das Zertifikat des öffentlichen Schlüssels, und importieren Sie es in die Anwendung, wenn Sie Microsoft Active Directory für den SSL-Zugriff konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Ihre Zertifizierungsstelle kein vertrauenswürdiger Drittanbieter ist, müssen Sie das Zertifikat für die ausstellende Zertifizierungsstelle exportieren, damit wir ihr und durch Zuordnung auch dem LDAP-Serverzertifikat vertrauen können. Benutzer von MS Certificate Services können den Zertifikatpfad anzeigen, indem sie das Zertifikat in der für den Export verwendeten Konsole anzeigen. Wählen Sie die Registerkarte **Zertifikatpfad** aus. Sie müssen alle Zertifikate in der Kette exportieren. Sie finden das CA-Zertifikat im selben Ordner wie das LDAP-Zertifikat, indem Sie im Zertifikatpfad nach dem Namen suchen. Senden Sie alle Zertifikate für den Import in Ihre Instanz.

Prozedur

1. Fügen Sie über eine aktuelle oder neue MMC-Konsole das Snap-in „Zertifikat (lokaler Computer)“ hinzu.
2. Öffnen Sie den Ordner `Persönlich/Zertifikate`.
3. Suchen Sie das neue Zertifikat.
   Die Spalte Ausgestellt an zeigt den FQDN des Domänencontrollers an.
4. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie *Alle Aufgaben/Export*aus.
5. Exportieren Sie in das DER- oder Base64-Format.
   Benennen Sie die Datei im Format `MyCompany.cer`. Dies ist das Zertifikat des öffentlichen Schlüssels, das in der Instanz für eine sichere Kommunikation mit Ihrem Domänencontroller verwendet werden muss.
6. Testen Sie LDAPS lokal, bevor Sie das Zertifikat an die Instanz senden.

Nächste Maßnahme
Importieren Sie nach Abschluss dieses Verfahrens das Zertifikat des öffentlichen Schlüssels in die Anwendung.
Informationen zum Hochladen des Zertifikats in die Anwendung finden Sie unter Installieren Sie das LDAP X.509-SSL-Zertifikat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwendung des globalen LDAP-Katalogs

Einem DC kann die Rolle „Globaler Katalog“ (GC) zugewiesen werden. Die Rolle „Globaler Katalog“ (GC) ist ein LDAP-konformes Verzeichnis, das aus einer teilweisen Darstellung jedes Objekts aus jeder Domäne innerhalb einer Gesamtstruktur besteht.

Administratoren konfigurieren Active Directory so, dass LDAP-Verzeichnisinformationen (Lightweight Directory Access Protocol) mit einer der folgenden Hosting-Methoden gehostet werden.

- Die übliche Methode zum Hosten von LDAP-Verzeichnisinformationen besteht in der Verwendung des Standard-LDAP oder LDAPS (sicheres LDAP) an den Ports 389 oder 636. Diese Standard-LDAP-Ports sind immer auf einem Domänencontroller (DC) vorhanden und werden selten geändert. Der Zugriff auf diese Verzeichnispartition bietet Zugriff auf alle Objekte in der Domäne, die auf dem DC gehostet wird. Es gibt keine Möglichkeit, mit dieser Methode auf Objekte aus anderen Domänen zuzugreifen.
- Einem RZ kann auch die Rolle „Globaler Katalog“ (GC) zugewiesen werden. Die Rolle „Globaler Katalog“ (GC) ist ein LDAP-konformes Verzeichnis, das aus einer teilweisen Darstellung jedes Objekts aus jeder Domäne innerhalb der Gesamtstruktur besteht. Auf dieses LDAP-Verzeichnis kann über Port 3268 zugegriffen werden, mit LDAPS über Port 3269. Die Zertifikatanforderungen für LDAPS- und Standard-LDAP-Ports sind identisch.

Globale Katalog-LDAP-Abhängigkeiten

- Für den Domänencontroller, mit dem Ihre Instanz eine Verbindung herstellt, muss die Rolle „Globaler Katalog“ aktiviert sein.
- Firewall-Regeln müssen eingehenden Datenverkehr an den Domänencontroller an Port 3268 (LDAP) oder 3269 (LDAPS) zulassen.

Spezielle Hinweise

- Nicht alle Attribute werden in die GC-Partition repliziert. Allgemeine Attribute wie Vorname, Nachname, E-Mail, Telefonnummer, Beschreibung und Adresse sind enthalten. Zusätzliche Attribute können dem GC hinzugefügt werden, sollten jedoch begrenzt werden, um die Auswirkungen auf den Replikationsdatenverkehr der Gesamtstruktur zu minimieren.
- Standard-LDAP-Integrationen verwenden sAMAccountName normalerweise als UserID der Instanz und als Zusammenfügungsschlüssel in der LDAP-Importzuordnung, da dieser innerhalb einer Domäne garantiert eindeutig ist. Dieses Attribut ist nicht mehr eindeutig, wenn eine gesamte Gesamtstruktur von Domänen angezeigt wird. Ein neues eindeutiges Attribut muss identifiziert werden, und zwar die Benutzer-ID und der Zusammenfügungsschlüssel. Diese müssen nicht dasselbe Attribut sein und können je nach Gesamtstrukturdesign variieren. Wenden Sie sich an Ihren Active Directory-Administrator. Normalerweise ist userPrinicpalName ein eindeutiges Attribut über Domänen hinweg. Dies ist jedoch möglicherweise kein benutzerfreundlicher Name für die Anmeldung, kann jedoch für den eindeutigen Bezeichner bei Importen verwendet werden. Ein allgemeines Attribut, das für die Benutzer-ID verwendet wird, ist die E-Mail-Adresse. Diese Entscheidungen wirken sich auf die LDAP-Eigenschaften und die LDAP-Zuordnung aus.
- Der für den Zusammenfügungsschlüssel in der LDAP-Importzuordnung verwendete Wert muss eindeutig sein und für jedes zu importierende Objekt vorhanden sein. Wenn sie nicht eindeutig ist oder nicht vorhanden ist, werden falsche Datensätze mit Änderungen aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie bereits eine LDAP-Integration haben und diese in einen GC ändern möchten, ändern Sie den Zusammenfügungsschlüssel für den Import. Die neuen Schlüsselwerte müssen importiert werden, bevor Sie den Zusammenfügungsschlüssel ändern können.
- Wenn Sie Änderungen an Ihrer LDAP-Integration vornehmen, die Ihre Integration unterbrechen, sollte Ihr erster Schritt darin bestehen, diese Änderungen rückgängig zu machen. Wenden Sie sich danach an Kundenservice und Support, um vollständige Informationen darüber zu erhalten, was Sie versuchen.

OpenLDAP-Nebenschema-Änderung

In OpenLDAP 2.3-Systemen, die back-bdb (Berkley-Backend) verwenden, nehmen Administratoren geringfügige Änderungen an ihrem Schema vor, um die Integration zu erleichtern.

Warnung:
Die hier beschriebene Anpassung wurde für die Verwendung in bestimmten Fällen entwickelt und wird von Now Support nicht unterstützt. Diese Methode wird wie sie ist zur Verfügung gestellt und sollte vor der Implementierung gründlich getestet werden. Veröffentlichen Sie alle Fragen und Kommentare zu dieser Anpassung in unserem Community-Forum .

In OpenLDAP 2.3 bietet back-bdb eingeschränkte Unterstützung für die Ungleichheitsindizierung (Reihenfolge). Sie ist nur für die Syntax „generalizedTime“ und „ChangeSequenceNumber“ implementiert. Sie kann nicht für eine Syntax unterstützt werden, die Teilzeichenfolgen unterstützt. Suchfilter, die Ungleichungen enthalten, werden anhand des Anwesenheitsindex verarbeitet.

Wir empfehlen, zu diesem Zweck ein benutzerdefiniertes Attribut zu erstellen, anstatt zu ändern, was bereits indiziert oder im Schema vorhanden ist (z. B. `servnowid`).

Ändern Sie das OpenLDAP-Schema

Ändern Sie das OpenLDAP-Schema. Diese Schritte beschreiben eine von einem unserer Kunden bereitgestellte Schemaänderung an OpenLDAP 2.3, die ihnen bei der Integration mit ihrer Instanz geholfen hat.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Warnung:
Die hier beschriebene Anpassung wurde für die Verwendung in bestimmten Fällen entwickelt und wird von Now Support nicht unterstützt. Diese Methode wird wie sie ist zur Verfügung gestellt und sollte vor der Implementierung gründlich getestet werden. Veröffentlichen Sie alle Fragen und Kommentare zu dieser Anpassung in unserem Community-Forum .

So ändern Sie das OpenLDAP-Schema für die Integration mit der -Instanz:

Prozedur

1. Erstellen Sie ein benutzerdefiniertes Attribut.

Example

```
attribute ( 1.3.6.1.4.1.3403000.2.1.8

    NAME 'servnowid'
 ORDERING caseIgnoreOrderingMatch
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
EQUALITY caseIgnoreMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

2. Fügen Sie das Attribut in die ausgewählte Objektklassen-OID ein.

Example

```
objectclass ( 1.3.6.1.4.1.3403000.2.2.1
    NAME 'BcfUserIdentifiers' SUP top AUXILIARY
 MAY ( uniqid $ unixid $ servnowid ) )
```

In OpenLDAP 2.3 können Sie die Serverkonfigurationen dynamisch ändern, Sie können jedoch nur das Schema erweitern. Sie können das vorhandene Schema nicht ändern oder löschen. Anstatt eine weitere Objektklasse für dieses Attribut in der dynamischen Konfiguration zu erstellen, verwenden Sie die statische Konfigurationsdatei slapd.conf.

3. Fügen Sie in slapd.conf die Indizierung für das neue Attribut im bdb-Abschnitt Ihres Hauptdatenbank-Back-Ends hinzu.

Example

```
database bdb (configs here) ....

index servnowid pres

(other indexes here) .....
```

4. Führen Sie als Stamm den Befehl slapindex aus, um dieses Attribut zu indizieren und in Suchfiltern verfügbar zu machen.
Stellen Sie sicher, dass der OpenLDAP-Daemon nicht ausgeführt wird oder sich im schreibgeschützten Modus befindet, bevor Sie slapindex starten.

Datensatz-LDAP-Löschungen

Standardmäßig löscht die Instanz keine Einträge, nachdem sie aus LDAP entfernt wurden.

Durch das Löschen eines Eintrags, der auch als *Datensatz*bezeichnet wird, werden auch der gesamte Verlauf und Verweise auf den gelöschten Eintrag gelöscht.

Zum Beispiel haben Konfigurationselemente (Configuration Items, CIs), SLA-Vereinbarungen, Softwarelizenzen, Bestellungen und Servicekatalogeinträge alle einen Verweis auf die Abteilung. Wenn eine Abteilung gelöscht wird, löscht die Integration alle Verweise auf die Abteilung. Außerdem führt das Löschen eines Benutzers dazu, dass der gesamte Verlauf der Aktionen dieses Benutzers verloren geht.

Entscheiden Sie, ob alle Datensätze aus einer Tabelle beibehalten oder gelöscht werden sollen, je nach den Anforderungen Ihrer Organisation.

Begrenzen Sie gleichzeitige Sitzungen

Sie können die Anzahl der gleichzeitigen interaktiven Sitzungen für einen Benutzer oder eine Rolle in einer Instanz auf allen Knoten begrenzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

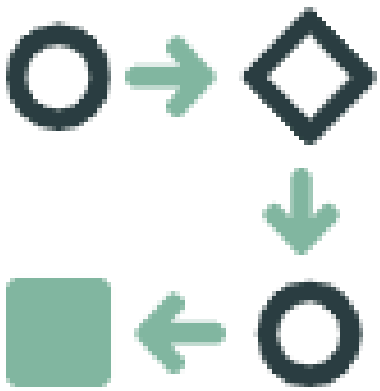
Erkunden

Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen der Begrenzung gleichzeitiger Sitzungen.

Aktivieren

Machen Sie sich damit vertraut, wie Sie die Beschränkung gleichzeitiger Sitzungen aktivieren.

Satz



Legen Sie das Limit für gleichzeitige Sitzungen für einen Benutzer oder eine Rolle fest.

Deaktivieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informieren Sie sich, wie Sie die Begrenzung gleichzeitiger Sitzungen deaktivieren können.

Erkundung gleichzeitiger Sitzungen begrenzen

Sie können die Anzahl der gleichzeitigen interaktiven Sitzungen für einen Benutzer oder eine Rolle in einer Instanz auf allen Knoten begrenzen.

Gleichzeitige interaktive Sitzungen beziehen sich auf die Anzahl der Sitzungen, die ein Benutzer pro Instanz von ServiceNow haben kann. Eine aktive Instanzsitzung tritt bei jeder neuen Anmeldung bei einer bestimmten ServiceNow -Instanz auf. Standardmäßig gibt es keine Beschränkungen für die Anzahl der aktiven Instanzsitzungen, die ein Benutzer haben kann.

Mit dem Jakarta-Release können Sie die Anzahl der aktiven gleichzeitigen Sitzungen pro Benutzer begrenzen. Wenn sich der Benutzer nach Erreichen der maximalen Anzahl aktiver Sitzungen anmeldet, wird die älteste aktive Sitzung beendet, und eine neue interaktive Sitzung wird aktiv. Wenn ein Benutzer versucht, über einen Browser auf eine geschlossene Sitzung zuzugreifen, wird er zur Anmeldeseite weitergeleitet.

Hinweis:
Das Plugin „ **Gleichzeitige Sitzungen** begrenzen“ muss aktiv sein, um ein maximales Sitzungslimit zu aktivieren. Grenzwerte werden über die Eigenschaft glide.authenticate.max.concurrent.interactive.sessions festgelegt. Ein maximaler Grenzwert gilt für alle Benutzer oder Rollen, für die die Eigenschaft „limit“ aktiv ist. Für einen Benutzer oder eine mit dem Benutzer verbundene Rolle muss der Wert limit_concurrent_sessions auf true gesetzt sein, damit die Anzahl der zu initiierenden Sitzungen begrenzt ist. Beim Release Jakarta unterstützt diese Funktion keine Sitzungen, die über die native mobile App oder nicht interaktive Mechanismen erstellt wurden.

Ein typischer Anwendungsfall, wenn eine maximale gleichzeitige Sitzung von 1 festgelegt ist:

1. Der Benutzer greift über Chrome auf die anfängliche Instanz ServiceNow zu.
2. Nachdem sich der Benutzer erfolgreich angemeldet hat, erstellt ServiceNow Sitzung 1 (S1) für den Benutzer.
3. Der Benutzer beschließt, einen weiteren Zugriff auf die Instanz ServiceNow über Firefox zu initiieren.
4. Nachdem sich der Benutzer erfolgreich angemeldet hat, erstellt ServiceNow Sitzung 2 (S2) für den Benutzer.
5. Da der Benutzer eine maximale Anzahl gleichzeitiger Sitzungen von 1 hat, wird die S1-Sitzung ungültig, wenn S2 erstellt wird.
6. Wenn der Benutzer erneut über Chrome auf die S1-Instanz ServiceNow zugreift, wird er zur Anmeldeseite weitergeleitet, da S1 ungültig ist.

Grenzwerte für gleichzeitige Sitzungen funktionieren mit allen ServiceNow -Authentifizierungsmechanismen: SAML, LDAP und lokale Datenbankauthentifizierung. Sie funktioniert auch mit der Multifaktor-Authentifizierung und allen interaktiven ServiceNow -Authentifizierungsmechanismen. Die Quelle der Sitzung kann über die Tabelle **sys_user_session** unter der Spalte **Typ**angezeigt werden. Die Werte können sein:

- Webbrowser
- Mobiler Browser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ServiceNow Mobile-App
- Nicht interaktiv (SOAP, WSDL, OAuth)

Plugin „Gleichzeitige Sitzungen begrenzen“ aktivieren und konfigurieren

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „Gleichzeitige Sitzungen begrenzen“ (com.glide.limit.concurrent.sessions) aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**.
2. Suchen und klicken Sie auf das Plugin „Gleichzeitige Sitzungen begrenzen“.
3. Überprüfen Sie im System-Plugin-Formular die Plugin-Details, und klicken Sie dann auf den zugehörigen Link **Aktivieren/Aktualisieren**.
4. Klicken Sie auf **Aktivieren**.
5. Um diese Funktion zu aktivieren und eine maximale Anzahl gleichzeitiger Sitzungen festzulegen, wechseln Sie zur Registerkarte Plugin-Dateien, suchen Sie die folgenden Eigenschaften, und ändern Sie die Einstellungswerte:

Option	Bezeichnung
glide.authenticate.limit.concurrent.interactive-.sessions	Sie können die Funktion zum Begrenzen gleichzeitiger Sitzungen aktivieren, indem Sie den Wert auf **True festlegen**. Standardmäßig ist diese Eigenschaft auf **False**festgelegt, was bedeutet, dass die Anzahl der interaktiven Sitzungen, die ein Benutzer aktiv haben kann, unbegrenzt ist. **Hinweis:** Um diese Funktion zu deaktivieren, setzen Sie diese Eigenschaft zurück auf **False**.
glide.authenticate.max.concurrent.interactive-.sessions	Sie können die maximale Anzahl gleichzeitiger aktiver interaktiver Sitzungen festlegen, die ein Benutzer in der Instanz auf allen Knoten haben kann.

6. **Wahlweise:** Bei Bedarf können Sie auch die folgenden Eigenschaften ändern:

Option	Bezeichnung
glide.authenticate.session.types.to.limit.concurrency	Diese Eigenschaft schränkt Sitzungstypen ein. Standardmäßig haben nur die Webbrowsersitzungen ein Limit. Zu den Sitzungstypen gehören: ○ Webbrowser (1) ○ Mobiler Browser (2)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	○ ServiceNow Mobile-App (3) ○ Nicht interaktiv (10) Sie können den Wert für Webbrowser auf „1“, für mobile Browser auf „2“ oder für beide auf „1,2“ festlegen. **Hinweis:** Nur Web- und Mobile-Browsersitzungen können ein Limit haben. Es gibt keine Grenzwerte für Sitzungen, die aus der Mobile-App ServiceNow stammen, oder für nicht interaktive Sitzungen.
glide.authenticate.limit.concurrent.sessions.across.all.nodes	Diese Eigenschaft schränkt das Limit gleichzeitiger Sitzungen pro Knoten ein, anstatt sie auf alle Knoten einer ServiceNow -Instanz zu beschränken. Standardmäßig ist der Wert auf „true“ festgelegt, wodurch Benutzersitzungen auf allen Knoten eingeschränkt werden. Wenn die Eigenschaft auf „false“ festgelegt ist, unterliegen nur die Sitzungen auf diesem Knoten und nicht die Sitzungen auf den anderen Knoten der Begrenzung.

7. Klicken Sie auf **Aktualisieren**, damit die Einstellungen wirksam werden.

Nächste Maßnahme

Festlegen eines Grenzwerts für gleichzeitige Sitzungen nach Benutzer oder Rolle.

Zugehörige Informationen

Liste der Plugins (Washington DC)

Festlegen eines Grenzwerts für gleichzeitige Sitzungen nach Benutzer oder Rolle

Sie können ein Limit für gleichzeitige Sitzungen für einen bestimmten Benutzer oder eine bestimmte Rolle festlegen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Benutzer** oder **Benutzeradministration** > **Rollen**.
2. Wählen Sie einen Benutzer oder eine Rolle aus, für die Sie ein **Limit für gleichzeitige Sitzungen festlegen möchten, aktivieren Sie das Kontrollkästchen Gleichzeitige Sitzungen** begrenzen, und klicken Sie auf **Aktualisieren**.
   Der Benutzer oder die Rolle hat ein Limit dafür, wie viele Sitzungen gleichzeitig geöffnet sein können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Deaktivieren eines Grenzwerts für gleichzeitige Sitzungen nach Benutzer oder Rolle

Sie können eine Beschränkung gleichzeitiger Sitzungen für einen bestimmten Benutzer oder eine bestimmte Rolle deaktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Benutzer** oder **Benutzeradministration** > **Rollen**.
2. Wählen Sie einen Benutzer oder eine Rolle aus, für die Sie die Begrenzung gleichzeitiger Sitzungen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gleichzeitige Sitzungen** begrenzen, und klicken Sie auf **Aktualisieren**.
   Der Benutzer oder die Rolle unterliegt keiner Begrenzung, wie viele gleichzeitige Sitzungen gleichzeitig geöffnet sein können.

Multifaktor-Authentifizierung (MFA)

Erfahren Sie, wie Sie die Multifaktor-Authentifizierung aktivieren und konfigurieren.

Erkunden

Lernen Sie die Funktionen und den Geschäftsnutzen von MFA kennen.

Aktivieren

Machen Sie sich mit der Aktivierung von MFA vertraut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden

Konfigurieren und verwenden Sie die MFA.

MFA mit Single Sign-on (SSO)

Erfahren Sie, wie Sie MFA mit Single Sign-on (SSO) konfigurieren.

Multifaktor-Authentifizierung erkunden

Erfahren Sie, wie Sie die Multifaktor-Authentifizierung aktivieren und konfigurieren.

MFA-Aktivierung

Aktivieren Sie das Plugin „ **Integration – Multifactor Authentication** “ (com.snc.integration.multifactor.authentication), um mit der Verwendung von MFA für eine Instanz zu beginnen. Für die Aktivierung dieses Plugins ist die Administratorrolle erforderlich. Details zu diesem Vorgang finden Sie unter Aktivieren Sie das MFA-Plugin.

Multifaktor-Kriterien

Verwenden Sie Multifaktor-Kriterien, um zu bestimmen, welche Benutzer und Rollen die zweistufige Multifaktor-Überprüfung verwenden müssen. Sie können eines dieser Kriterien oder eine Kombination davon verwenden, um Ihren Geschäftsanforderungen gerecht zu werden.

Benutzerbasierte Multifaktor-Kriterien

Verwenden Sie benutzerbasierte Multifaktor-Kriterien, um einzelne Benutzer auszuwählen, die sich mit MFA anmelden müssen. Administratoren aktualisieren das Feld **Multifaktor-Authentifizierung** aktivieren in einem Benutzerdatensatz, um die MFA-Anforderungen für einen Benutzer zu aktivieren oder zu deaktivieren. Details zu diesem Vorgang finden Sie unter Konfigurieren Sie benutzerbasierte Multifaktor-Kriterien.

Rollenbasierte Multifaktor-Kriterien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie rollenbasierte Multifaktor-Kriterien, um die MFA-Anmeldung für alle Benutzer zu erfordern, die einer bestimmten Rolle zugewiesen sind. Der Datensatz „Rollenbasierte Multifaktor **-Authentifizierung** “ in der Tabelle „Multifaktor **-Kriterien** “ [multi_factor_criteria] enthält die Liste der Rollen, die eine MFA-Anmeldung erfordern. Weitere Informationen zum Verwalten dieser Liste finden Sie unter Konfigurieren Sie rollenbasierte Multifaktor-Kriterien.

Richtlinienbasierte Multifaktor-Kriterien für adaptive Authentifizierung

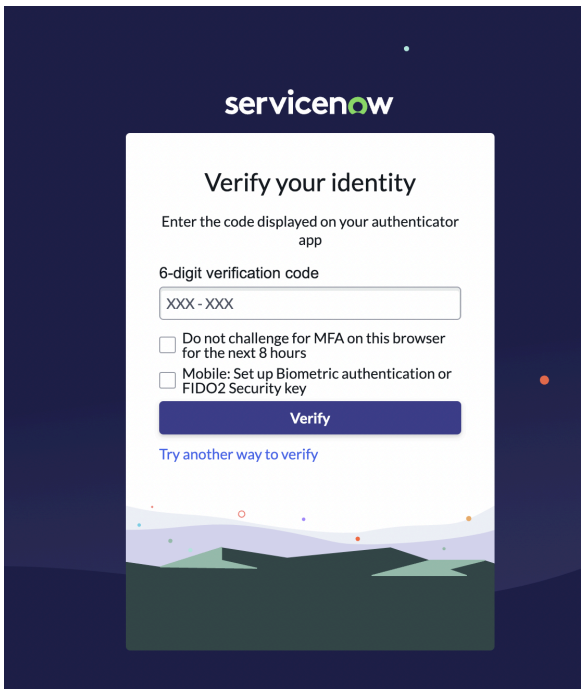
Verwenden Sie die adaptive Authentifizierung, um zu bestimmen, wann Ihre Instanz MFA erfordert. Die adaptive Authentifizierung verwendet Authentifizierungsrichtlinien, um Kriterien wie die IP-Adresse eines Benutzers oder Benutzergruppen auszuwerten. Weitere Informationen zur adaptiven Authentifizierungsfunktion finden Sie unter Adaptive Authentifizierung.

Methoden der Multifaktor-Authentifizierung

Benutzer können zusätzlich zu ihrem Benutzernamen und ihrem Passwort die folgenden Optionen verwenden, um die Anforderungen der Multifaktor-Authentifizierung zu erfüllen.

Authentifikatoranwendungen

Eine Authentifikatoranwendung ist Software einer Drittpartei, die temporäre Passcodes generiert. Benutzer können diese Passcodes zusammen mit ihrem Passwort verwenden, um sich bei einer Instanz anzumelden, die eine Multifaktor-Authentifizierung (MFA) erfordert. Weitere Informationen zu diesen Anwendungen finden Sie unter Authentifikatoranwendungen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Biometrische Scanner

Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Benutzer zu identifizieren. Ihre Benutzer können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Weitere Informationen zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

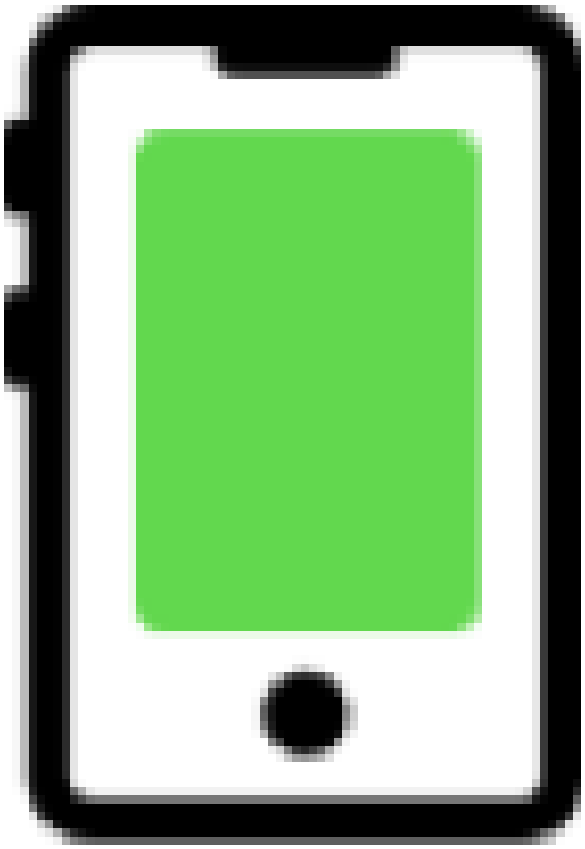
Hardwareschlüssel

Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden zur Authentifizierung in einen Port Ihres Geräts eingefügt. Weitere Informationen zur Registrierung von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SMS



Der Administrator kann die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden, erforderlich sind.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die OTP-SMS an die Mobiltelefonnummer gesendet, die dem sys_user-Datensatz zugeordnet ist. Benutzer können den sechsstelligen Überprüfungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.

Weitere Informationen finden Sie unter Multifaktor-Authentifizierung mit SMS.

E-Mail

Der Administrator kann die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden, erforderlich sind.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird E-Mail-OTP an die E-Mail-Adresse des Benutzers gesendet. Benutzer können den sechsstelligen Überprüfungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und ihre Identität überprüfen.

Weitere Informationen finden Sie unter Multifaktor-Authentifizierung mit E-Mail.

Eigenschaften Multifaktor-Authentifizierung

Verwenden Sie die Eigenschaften der Multifaktor-Authentifizierung, um MFA in Ihrer Instanz zu aktivieren, zu deaktivieren und zu konfigurieren. Weitere Informationen zu diesen Eigenschaften finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

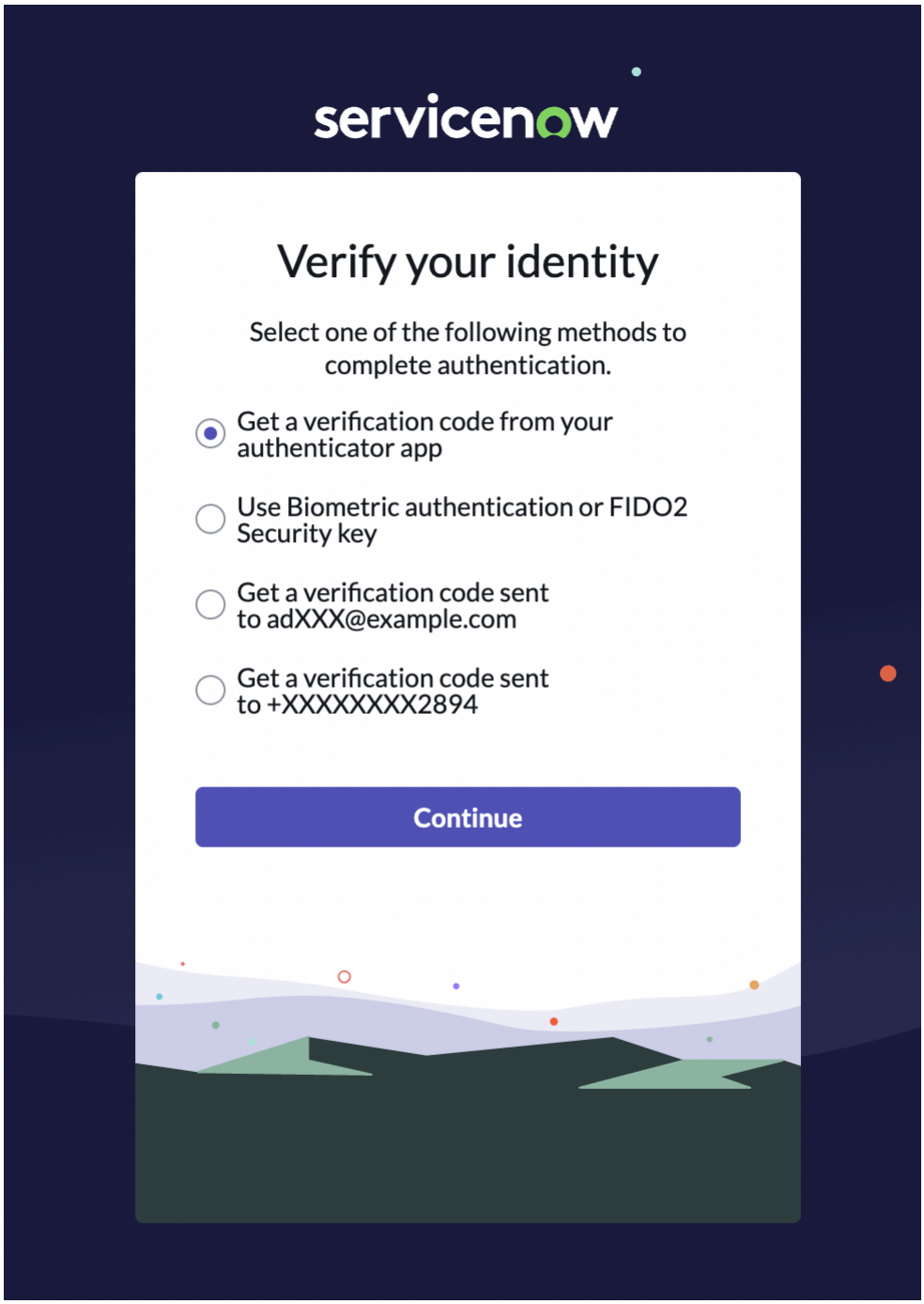
MFA-Aktivierung, unterstützte Methoden und Workflow

MFA, auch bekannt als zweistufige Überprüfung, ist eine Sicherheitsanforderung, bei der Benutzer mehr als einen Satz von Anmeldeinformationen eingeben müssen, um auf eine Instanz zuzugreifen.

Die Basisebene der Authentifizierung bei einer Instanz ist die lokale Datenbankauthentifizierung, bei der ein Benutzer eine Kombination aus Benutzername und Passwort eingibt. Mit MFA können Administratoren und Benutzer eine zweite Authentifizierungsebene anfordern. Diese zweite Authentifizierung kann sein:

- Ein Passcode aus einer Authentifizierungs-App
- Ein Hardwareschlüssel
- Ein biometrischer Authentifikator, z. B. ein Fingerabdruckleser oder eine Gesichtserkennung.
- Eine SMS oder E-Mail

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Als Administrator können Sie MFA für einzelne Benutzer oder alle Benutzer in einer bestimmten Rolle anfordern. Sie können Ihren Benutzern auch ermöglichen, sich für MFA zu entscheiden und es zu verwenden.

Aktivierung

Das Plugin *`Integration - Multifactor Authentication`* (com.snc.integration.multifactor.authentication) wird standardmäßig in Ihrer Instanz installiert, muss jedoch von einem Administrator mithilfe einer Systemeigenschaft aktiviert werden. Details finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Nach dem Klonen einer Instanz müssen Sie MFA für die geklonte Instanz erneut aktivieren. Weitere Informationen finden Sie in den KB-Artikeln KB0657100 , KB0860689 ,KB0825390 , KB0779908 , KB0717367 , KB0727991 .

Unterstützte Authentifizierungsmethoden

Sie können MFA mit den folgenden Authentifizierungsmethoden verwenden:

- Lokale Datenbankauthentifizierung (native ServiceNow Authentifizierung)
- LDAP-Integration
- SSO-SAML
- SSO-OIDC

Hinweis:
Benutzer müssen eine Authentifikatoranwendung einrichten, bevor sie einen Hardwareschlüssel oder biometrischen Authentifikator konfigurieren. Weitere Informationen zum Einrichten der Authentifikatoranwendung finden Sie unter Richten Sie die Multifaktor-Authentifizierung für Ihr Benutzerprofil ein.

Workflow für Multifaktor-Authentifizierung einrichten

Der Administrator aktiviert die Multifaktor-Authentifizierung

Das Plugin „ **Integration – Multifactor Authentication** “ (com.snc.integration.multifactor.authentication) ist standardmäßig in Ihrer Instanz aktiviert. Um MFA zu verwenden, müssen Administratoren MFA mit einer Systemeigenschaft aktivieren. Nach der Aktivierung wählen Administratoren Benutzer oder Rollen aus, für die MFA-Anmeldungen erforderlich sind.

Weitere Informationen zum Administrator-Setup für MFA finden Sie unter Multifaktor-Authentifizierung (MFA).

Benutzer melden sich mit einer Authentifizierungs-App an

Ihre Benutzer werden bei der ersten Anmeldung aufgefordert, eine Authentifikator-App zu verwenden. Dieser Schritt ist auch dann erforderlich, wenn Ihre Benutzer Biometrie oder einen Hardwareschlüssel verwenden. Benutzer, die sich anmelden, sehen einen QR-Code, den sie scannen können, um schnell eine Authentifikator-App einzurichten. Dieser erste Anmeldevorgang wird in Richten Sie die Multifaktor-Authentifizierung für Ihr Benutzerprofil einbeschrieben.

Authentifizierungs-Apps sind als mobile Anwendungen verfügbar. Einige Authentifizierungs-Apps sind als Erweiterungen für Desktop-Browser für Benutzer verfügbar, die keinen Zugriff auf ein Mobilgerät haben.

Nach der ersten Anmeldung können Benutzer zusätzliche Authentifikatoren konfigurieren

Nach der ersten Anmeldung können Benutzer Hardwareschlüssel oder biometrische Authentifikatoren registrieren.

Weitere Informationen zu diesen und anderen benutzerseitigen Konfigurationen für MFA finden Sie unter Multifaktor-Authentifizierung (MFA) verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Webauthentifizierung

Aktivieren Sie *Integration - Web Authentication* (com.snc.integration.webauthn), um die Authentifizierung mit Hardwareschlüsseln oder biometrischen Lesern in Ihrer Instanz zu ermöglichen.

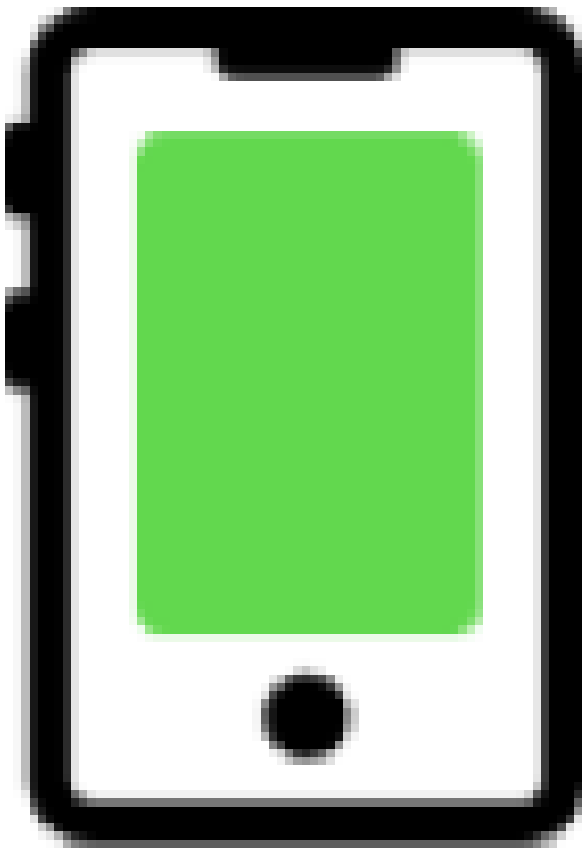
Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden zur Authentifizierung in einen Port Ihres Geräts eingefügt. Weitere Informationen zur Registrierung von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.

Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Benutzer zu identifizieren. Ihre Benutzer können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Weitere Informationen zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SMS oder E-Mail (Einmalpasswort)

Damit sich Benutzer unterwegs bei einer ServiceNow -Instanz anmelden und die Experience reibungsloser gestalten können, wird MFA mit SMS und E-Mail unterstützt.



Der Administrator kann die Instanz ServiceNow so konfigurieren, dass Benutzer erforderlich sind, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die OTP-SMS an die Mobiltelefonnummer gesendet, die dem sys_user-Datensatz zugeordnet ist. Der Benutzer kann den sechsstelligen Überprüfungscode eingeben, der an das Mobilgerät gesendet wurde, und seine Identität überprüfen.

Weitere Informationen finden Sie unter Multifaktor-Authentifizierung mit SMS.

Der Administrator kann die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden, erforderlich sind.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird E-Mail-OTP an die E-Mail-Adresse gesendet, die dem Benutzer zugeordnet ist. Der Benutzer kann den sechsstelligen Überprüfungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und seine Identität überprüfen.

Weitere Informationen finden Sie unter Multifaktor-Authentifizierung mit E-Mail.

Aktivieren Sie das MFA-Plugin

Das Plugin „Integration – Multifactor Authentication“ ist standardmäßig aktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „ **Integration – Multifactor Authentication** “ (com.snc.integration.multifactor.authentication).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Konfigurieren Sie benutzerbasierte Multifaktor-Kriterien

Verwenden Sie benutzerbasierte Multifaktor-Kriterien, um MFA für einen Benutzer zu aktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Benutzer**.
2. Konfigurieren Sie die Liste so, dass die Spalte **Multifaktor-Authentifizierung aktivieren angezeigt** wird.
3. Ändern Sie die Werte der Spalte **Multifaktor-Authentifizierung** aktivieren für die ausgewählten Benutzer in **true**.

   Wenn sich der Benutzer mit seinem Benutzernamen und Passwort anmeldet, wird er aufgefordert, die Multifaktor-Authentifizierung einzurichten.

Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Verwenden Sie rollenbasierte Multifaktor-Kriterien, um die Multifaktor-Authentifizierung für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Multifaktor-Kriterien**.
2. Öffnen Sie in der Liste **„Multifaktor-Kriterien** “ den Datensatz **„Rollenbasierte Multifaktor-Authentifizierung** “.
3. Verwenden Sie die Liste **„Multifaktor-Rollen** “, um Rollen hinzuzufügen oder zu entfernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Eine Rolle hinzufügen	Doppelklicken Sie auf **Neue Zeile einfügen...**, und geben Sie einen Rollennamen ein, oder wählen Sie einen aus. Klicken Sie auf das **Speichern**-Symbol ( ), um den Eintrag zu speichern.
Entfernen Sie eine Rolle	Klicken Sie auf das Löschsymbol ( ), um eine Rolle aus der Liste zu entfernen.

4. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Ihre Instanz erzwingt die Multifaktor-Authentifizierung für alle Benutzer, die Mitglieder der in der Liste **„Multifaktor-Rollen“** aufgeführten Rollen sind.

Wichtig:
Der Datensatz muss aktiv sein, um die rollenbasierte Multifaktor-Authentifizierung zu erzwingen.

Setzen Sie die Multifaktor-Authentifizierung (MFA) für Benutzer zurück

Administratoren können MFA für Benutzer zurücksetzen, die die App gelöscht haben, den Zugriff auf das Gerät verloren haben oder ihrem Gerät keine alternative MFA zugeordnet haben.

Vom Administrator unterstützte Multifaktor-Authentifizierung zurückgesetzt

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt, wie ein ServiceNow® -Administrator die MFA-Validierung zurücksetzen kann, um Benutzer zu entsperren und ihnen die erneute Registrierung von MFA zu ermöglichen.

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Anwendereinrichtung**.
2. Suchen Sie in der Benutzertabelle nach dem Benutzer, den Sie entsperren möchten.
3. Legen Sie Validieren auf **false**fest.
   Wenn Sie den Wert in „ **false** “ ändern, wird der Benutzer entsperrt und kann MFA erneut registrieren. Wenn der entsperrte Benutzer die Anmeldeinformationen eingibt und sich anmeldet, wird die Seite **Multifaktor-Authentifizierung (MFA)** aktivieren angezeigt. Benutzer können die Schritte auf der Seite ausführen, um MFA erneut zu registrieren.

Konfigurieren Sie richtlinienbasierte Multifaktor-Kriterien für die adaptive Authentifizierung

Verwenden Sie adaptive Richtlinien, um zu bestimmen, welche Benutzer die zweistufige Multifaktor-Überprüfung (MFA) verwenden müssen.

Vorbereitungen

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Diese Option wird nur angezeigt, wenn das **Multi-Provider-SSO-Plugin** in Ihrer Instanz aktiv ist. Weitere Informationen zu dieser Funktion finden Sie unter Externes Single Sign-on (SSO).
- Wenn die Standardrichtlinie **Step-Up-MFA-Richtlinie**ist, werden Anwender mit Multifaktor-Authentifizierung angezeigt, wenn die in der **Step-Up-MFA-** Richtlinie konfigurierte Richtlinie als „wahr“ ausgewertet wird. Die Richtlinie hat Vorrang vor der anwender- oder rollenbasierten Konfiguration.
- MFA mit SSO-Anmeldung ist nur verfügbar, wenn die Eigenschaft „ glide.authenticate.mfa.with.multisso.enabled“ auf „wahr“ festgelegt ist.
- Sie können zum Datensatz „Authentifizierungsrichtlinie“ navigieren, um die Richtlinieneingabe(n) im referenzierten Richtlinienfeld (**Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie**) hinzuzufügen oder zu bearbeiten.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **MFA-Kontext**.
   Der Kontextdatensatz der **MFA-Kontextrichtlinie** wird geöffnet.
2. Wählen Sie die Standardrichtlinie im Feld **Standardrichtlinie** aus.
   Diese Auswahl bestimmt, wie Ihre Instanz die Richtlinienbedingungen verwendet, um zu bestimmen, ob MFA erforderlich ist.

Standardrichtlinien

Standardrichtlinie	Definition
Step-Up-MFA-Richtlinie	Wählen Sie diese Option aus, um MFA zu erzwingen, wenn die in der **Step-Up-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
Step-Down-MFA-Richtlinie	Wählen Sie diese Option aus, um MFA zu umgehen, wenn die in der **Step-Down-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

3. Wählen Sie im Feld **Step-Up-MFA-Richtlinie** eine Richtlinie aus, die mit diesem Kontext verwendet werden soll.
   Weitere Informationen zu Richtlinien und Richtlinienkonfigurationen finden Sie unter
4. Klicken Sie auf **Aktualisieren**.
   Nach dem Speichern des Datensatzes werden die Listen „ **Richtlinieneingabe“** und **„Richtlinienbedingungen“** aktualisiert, um die Richtlinieneingaben und Bedingungen anzuzeigen, die der im Feld **Step-Up-MFA-Richtlinie** ausgewählten Richtlinie zugeordnet sind.

Systemeigenschaften der Multifaktor-Authentifizierung

Verwenden Sie Systemeigenschaften, um MFA zu aktivieren und an Ihre Sicherheitsanforderungen anzupassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften Multifaktor-Authentifizierung

Eigenschaft	Beschreibung
Multifaktor-Authentifizierung aktivieren (*glide.authenticate.multifactor*)	Option, mit der Benutzer und Administratoren diese Funktion verwenden können. Der Standardwert ist aktiviert. Weitere Informationen zu dieser Eigenschaft finden Sie unter Multi-Faktor-Authentifizierung (MFA) aktivieren in Härtungseinstellungen für Instanzsicherheit.
Anzahl, die angibt, wie oft ein Benutzer die Multifaktor-Authentifizierung umgehen kann (*glide.authenticate.multifactor.setup.bypass.count*)	Anzahl der Fälle, in denen ein Benutzer das Setup von MFA überspringen kann. Benutzer können sich auch dann bei der Instanz anmelden, wenn sie ihr Mobilgerät nicht dabei haben. Wenn Sie diese Funktion deaktivieren und sie dann erneut aktivieren, beginnt der Zähler erneut. Der Standardwert ist 3.
Die Zeit in Minuten, zu der der an die E-Mail-Adresse des Anwenders gesendete Einmalcode gültig ist (*glide.multifactor.onetime.code.validity*)	Anzahl der Minuten, die der Rücksetzungscode gültig ist. Weitere Informationen finden Sie unter Melden Sie sich mit Multifaktor-Authentifizierung an. Der Standardwert ist 10.
Zusätzliche Zeit in Sekunden, für die der Code gültig ist, um den Taktversatz zu berücksichtigen. Der maximale Wert beträgt 60 Sekunden. (*glide.authenticate.multifactor.clock_skew*)	Anzahl der zusätzlichen Sekunden, für die der Rücksetzungscode gültig ist. Der Höchstwert beträgt 60. Der Standardwert ist 10. Die Instanz validiert den vom Benutzer eingegebenen Code anhand des einzelnen App-generierten Codes, der zum aktuellen Zeitpunktgeneriert wird. Sie können das Zeitfenster mit dieser Eigenschaft verzerren und zulassen, dass ein oder mehrere Codes während eines Zeitfensters generiert werden, um als gültig angesehen zu werden. Der Wert der Eigenschaft wird in der folgenden Berechnung verwendet: aktuelle Zeit - X/2 und aktuelle Zeit + X/2, wobei X der Wert dieser Eigenschaft ist. Wenn Sie beispielsweise den Wert 10verwenden, berücksichtigt die Instanz alle Codes, die die App innerhalb des Zeitbereichs [Aktuelle Zeit - 5 Sekunden] und [Aktuelle Zeit + 5 Sekunden] generiert, als gültig. Verwenden Sie diese Eigenschaft, um Anmeldeprobleme zu vermeiden, bei denen der Benutzer in der standardmäßig zugewiesenen Zeit nicht den richtigen Code eingeben kann.
Aktivieren Sie die Funktion zum Speichern des Browsers für die Multifaktor-Authentifizierung. (*glide.authenticate.multifactor.remember.browser.enable*)	Legen Sie Ihre Instanz so fest, dass ein Benutzer zur Eingabe von MFA aufgefordert wird, wenn er sich von einem neuen Gerät oder Browser aus anmeldet. Der Standardwert ist ja.
Gültigkeit des Browser-Fingerabdrucks in Stunden.	Nachdem MFA den Browser gespeichert hat, wird der Benutzer für diese Dauer nicht mehr zur MFA im

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften Multifaktor-Authentifizierung (Fortsetzung)

Eigenschaft	Beschreibung
(*glide.authenticate.multifactor.browser.fingerprint.validity*)	selben Browser aufgefordert. Der Standardwert ist 8 Stunden.
Maximale Anzahl von Browsern, die sich ein Benutzer merken kann. (*glide.authenticate.multifactor.remembered.browser.max.count*)	Die Anzahl der Browser, die MFA für diesen Anwender speichert.
Standardwert der Checkbox „Browser speichern“ auf der Seite „Multifaktor validieren“. (*glide.authenticate.multifactor.remember.browser.default*)	Standardwert des Kontrollkästchens „recall-browser“ auf der Seite „Multifaktor validieren“.
Aktivieren Sie die auf der Webauthentifizierung (FIDO2) basierende MFA. (*glide.webauthn.enabled*)	Option zum Aktivieren passwortloser Authentifizierungsmethoden wie Hardwareschlüssel und biometrische Authentifizierung.

Konfigurieren Sie MFA mit Biometrie

Administratoren können die Liste „Öffentliche Benutzeranmeldeinformationen“ verwenden, um vom Benutzer erstellte Anmeldeinformationen anzuzeigen und zu verwalten.

Wenn ein Benutzer eine Authentifikatoranwendung, biometrische Authentifizierung oder einen Hardwareschlüssel registriert, erstellt Ihre Instanz einen Datensatz in der Tabelle „ **Öffentliche Benutzeranmeldeinformationen**“ [sys_user_public_credential]. Verwenden Sie diese Tabelle, um anzuzeigen, welche Benutzer einen Authentifikator registriert haben, welche Typen und wann sie registriert und verwendet wurden. Sie können diese Datensätze auch als inaktiv markieren, um zu verhindern, dass Benutzer diese Anmeldeinformationen verwenden können.

Formular „Öffentliche Anmeldeinformationen“ des Benutzers

Feld	Beschreibung
Kurzname der Anmeldeinformationen	Kurzname für die Anmeldeinformationen. Dieser Kurzname wird vom Benutzer bei der Registrierung eines Authentifikators ausgewählt.
Benutzer	Benutzer, der den Anmeldeinformationen zugeordnet ist
Aktiv	Gibt an, ob die Anmeldeinformationen aktiv sind. Administratoren können einen Datensatz auf inaktiv setzen, um zu verhindern, dass sich ein Benutzer mit diesen Anmeldeinformationen authentifiziert.
Authentifikator	Der Typ des vom Benutzer registrierten Authentifikators.
Registrierungszeit	Das Datum und die Uhrzeit, zu der der Benutzer diese Anmeldeinformationen erstellt hat
Zuletzt verwendet um	Datum und Uhrzeit der letzten Anmeldung des Benutzers mit diesen Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte Authentifikatortypen

Wenn Sie eine Authentifizierungsmethode eingeschränkt haben, z. B. biometrische Authentifikatoren, können Benutzer keine neuen Anmeldeinformationen dieses Typs erstellen. Alle Anmeldeinformationen, die vor dieser Einschränkung erstellt wurden, funktionieren jedoch weiterhin. Sie können Datensätze in der Tabelle „ **Öffentliche Benutzeranmeldeinformationen** “ deaktivieren, um zu verhindern, dass diese Anmeldeinformationen verwendet werden, nachdem sie erstellt wurden.

Konfigurationsoptionen für den Authentifikator

Verwenden Sie die Seite „Authentifikatorkonfiguration“, um Authentifikatoroptionen für Ihre Instanz zu verwalten.

Navigieren zu **Multi-Faktor-Authentifizierung** > **Webauthentifizierung** > **Konfiguration des Authentifikators** , um die Standardkonfigurationsoptionen anzuzeigen und zu bearbeiten.

Formular „Authentifikatorkonfiguration“

Feld	Beschreibung
Zulässiger Authentifikatortyp	Typ der Authentifikatoren, die registriert werden dürfen. Wählen Sie aus: • **Plattformauthentifizierer** sind an ein Gerät angehängt oder in dieses integriert. Unter diese Kategorie fallen Fingerabdruckleser oder die auf Mobilgeräten verfügbare Gesichtserkennung (z. B. Apple FaceID oder TouchID). • **Roaming** -Authentifikatoren können von einem Computer oder einem anderen Clientgerät entfernt und an anderer Stelle verwendet werden. Hardwareschlüssel fallen unter diese Kategorie.
Nachweistyp	Wenn der Wert auf „direkt“ oder „indirekt“ festgelegt wird, müssen Authentifikator-Metadaten importiert werden, um die Herkunft eines Authentifikators während der Registrierung nachzuweisen. • Keine • Direkt • Indirekt
Plattform-Selbstnachweis	Gibt an, ob der Selbstnachweis für Plattformauthentifizierer aktiviert ist.
Plattformübergreifender Selbstnachweis	Ob der Selbstnachweis für Roaming-Authentifikatoren aktiviert ist.
Anwenderverifizierung	Wählen Sie zwischen **Bevorzugt** und **Erforderlich**. Bei Bedarf fordert der Webauthentifizierungs-Flow Benutzer zur Verifizierung mit PIN oder Biometrie auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Authentifikatorkonfiguration“ (Fortsetzung)

Feld	Beschreibung
Benutzerpräsenz verifizieren	Ob der Webauthentifizierungs-Flow die Verifizierung der Benutzerpräsenz erfordert.
Residenter Schlüssel	Wählen Sie zwischen **Bevorzugt** und **Erforderlich**. Bei Bedarf behält der Authentifikator die Anmeldeinformationen des öffentlichen Schlüssels im Authentifikatorspeicher bei.
Zeitüberschreitung (in ms)	Maximales Zeitlimit für den Abschluss der Registrierung und Authentifizierung der Webauthentifizierung. Die Zeit wird in Millisekunden angegeben.

Multifaktor-Authentifizierung mit SMS

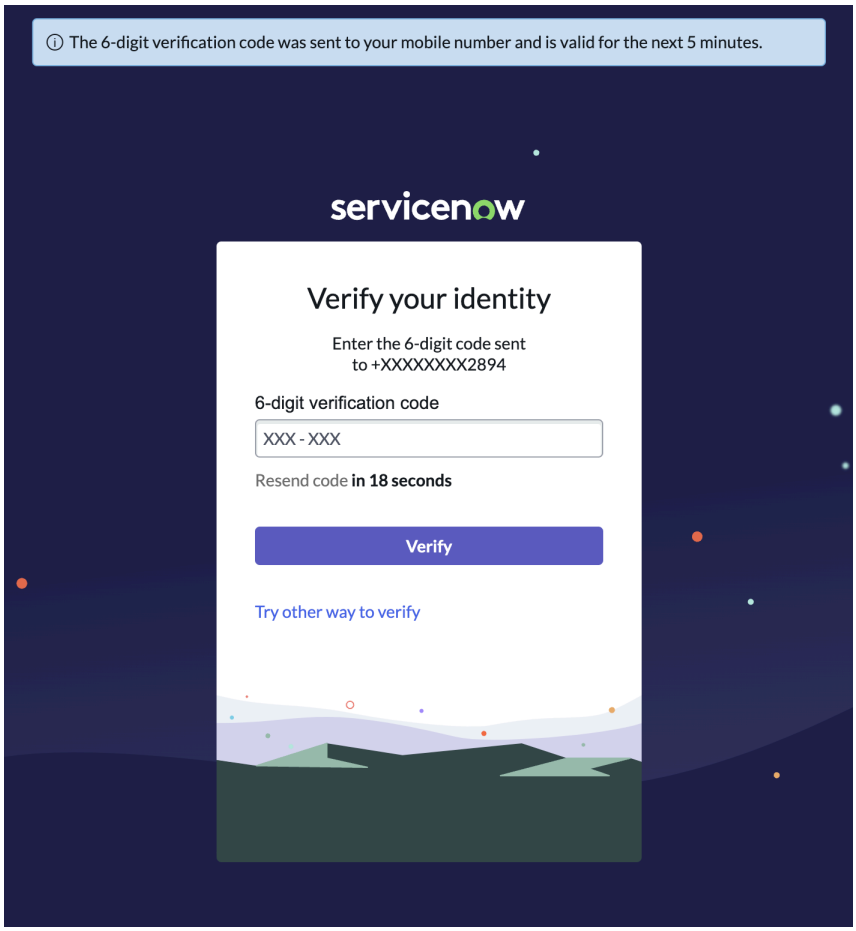
Multifaktor-Authentifizierung (MFA) mit SMS als Faktor für die Authentifizierung.

Der Administrator kann die Instanz ServiceNow so konfigurieren, dass Benutzer erforderlich sind, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die OTP-SMS an die Mobiltelefonnummer gesendet, die dem sys_user-Datensatz zugeordnet ist. Der Benutzer kann den sechsstelligen Überprüfungscode eingeben, der an das Mobilgerät gesendet wurde, und seine Identität überprüfen.

Sie können MFA mit SMS auch mit dem vordefinierten Twilio konfigurieren. Weitere Informationen finden Sie unter Multifaktor-Authentifizierung Provider.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Darüber hinaus kann die MFA mit SMS basierend auf der Richtlinieneingabe und den Bedingungen mithilfe von Filterkriterien gesteuert werden. Im Folgenden sind die Arten von Filterkriterien aufgeführt:

- IP-Filterkriterien
- Rollen-Filterkriterien
- Gruppenfilterkriterien

Aktivieren Sie das MFA mit SMS-Plugin

Installieren Sie für MFA mit SMS das Plugin „Multifaktor-Authentifizierung mit SMS“ (com.snc.authentication.sms_mfa).

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit der Multifaktor-Authentifizierung mit SMS installiert:

- Adaptive Authentifizierung (com.snc.adaptive_authentication
- Notify – Twilio Direct-Treiber (com.snc.notify.twilio_direct)

Abhängiges Plugin: Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können die Demodaten bei der Installation des Plugins laden, wenn Sie einen benutzerdefinierten Provider für die Generierung der SMS konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Multifaktor-Authentifizierung mit SMS“ (com.snc.authentication.sms_mfa).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Konfigurieren Sie SMS als MFA-Faktor

Konfigurieren Sie die Richtlinieneingabe und -bedingung, um SMS-OTP als MFA-Faktorrichtlinie für die Authentifizierung anzuzeigen.

Vorbereitungen

Erforderliches Plugin: Multifaktor-Authentifizierung mit SMS (com.snc.authentication.sms_mfa).

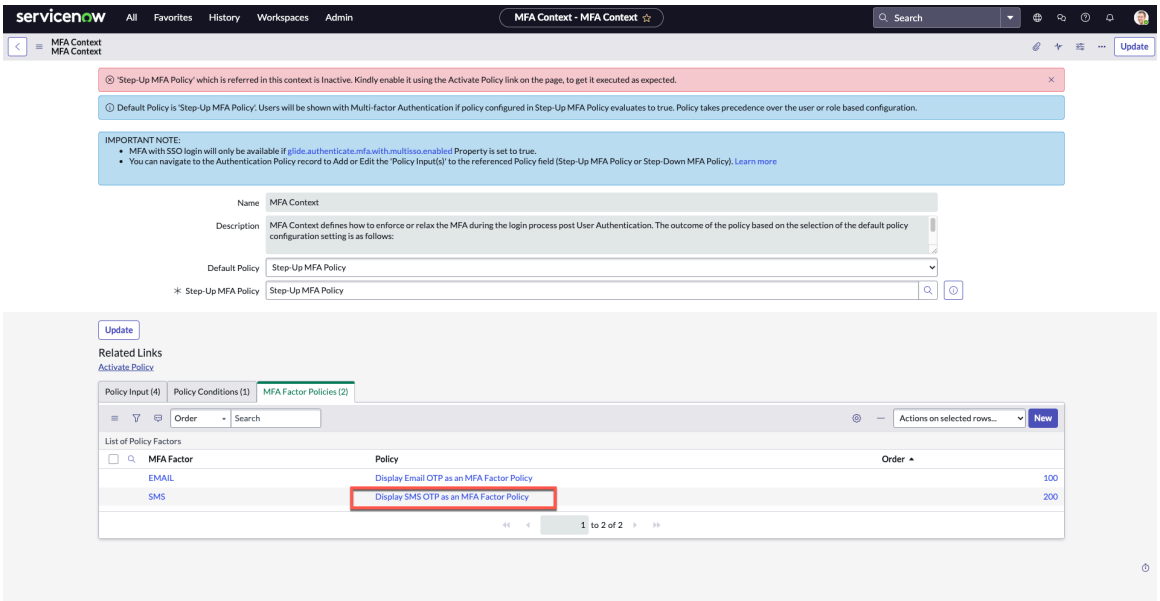
Erforderliche Rolle: admin

Hinweis:
Die MFA-Kontextrichtlinie muss als „ `true` “ ausgewertet werden, um die SMS-Faktorrichtlinie anzuwenden.

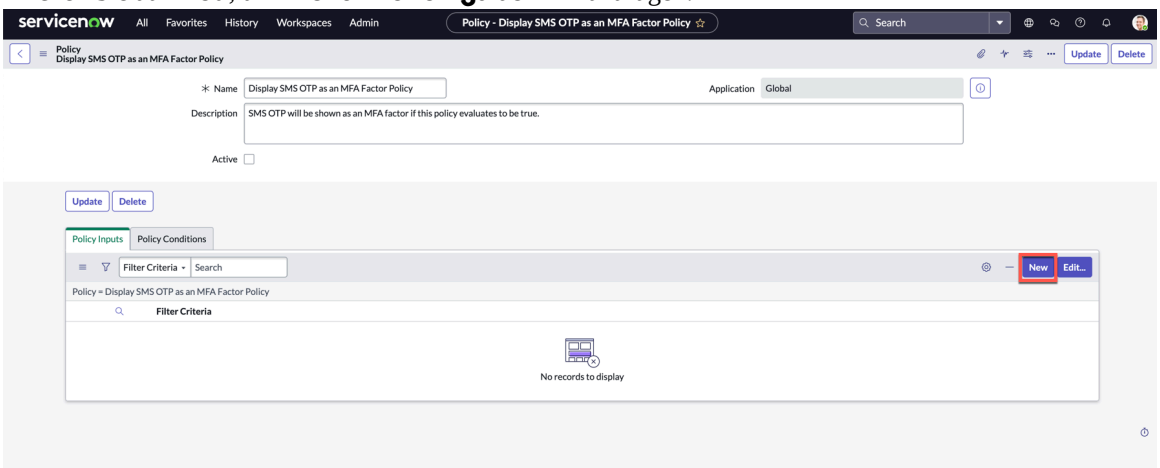
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**.
2. Klicken Sie auf die Registerkarte **MFA-Faktorrichtlinien**.
3. Wählen Sie **SMS-OTP als MFA-Faktorrichtlinie anzeigen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Neu**, um **Richtlinieneingaben**hinzuzufügen.

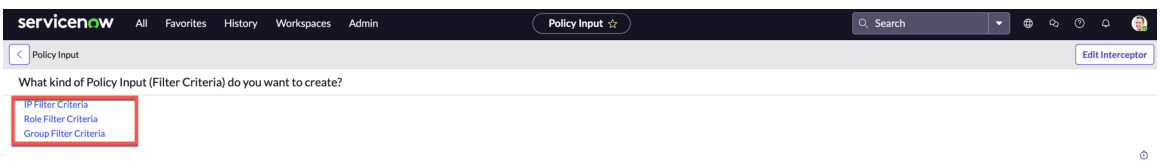


5. Wählen Sie die Filterkriterien aus, die Sie erstellen möchten.

Im Folgenden sind die Arten von Filterkriterien aufgeführt:

- IP-Filterkriterien
- Rollen-Filterkriterien
- Gruppenfilterkriterien

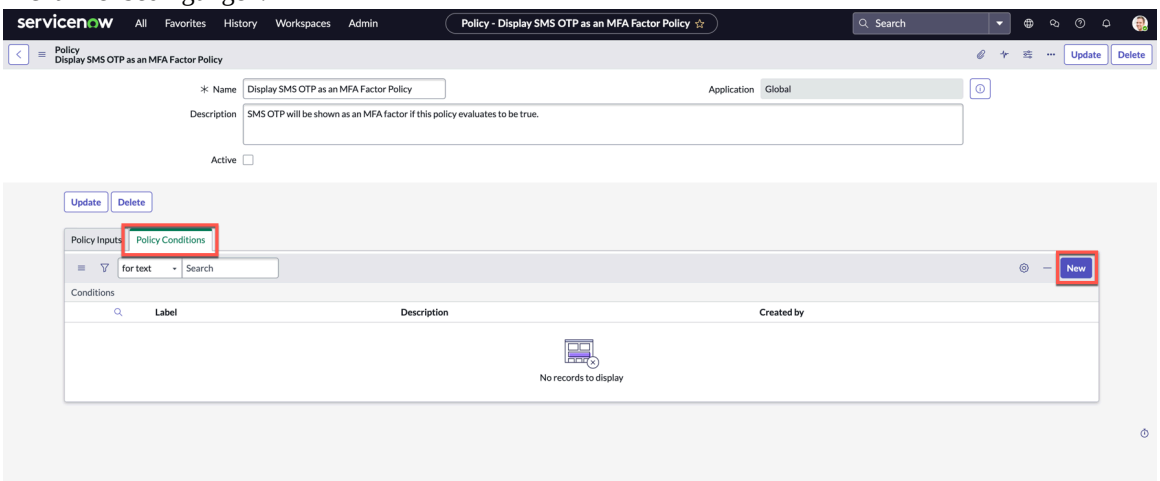
Beispiel: Rollenfilterkriterien.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie **auf Rollenfilterkriterien**.
7. Füllen Sie die Felder für die Rollenfilterkriterien aus, und übermitteln Sie den Datensatz.
   Die neue Richtlinie wird erstellt. Weitere Informationen finden Sie unter Rollenfilterkriterien.
8. Klicken Sie auf der Seite „Richtlinie – SMS-OTP als MFA-Faktorrichtlinie anzeigen“ auf Richtlinienbedingungen.



9. Klicken Sie auf **Neu**, um **Richtlinienbedingungen**hinzuzufügen.
10. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination mehrerer Richtlinieneingaben (Filterkriterien), die zum Auswerten von Authentifizierungsanforderungen verwendet wird. Wählen Sie die rollenbasierte Filterkriterienrichtlinie aus, die für die Bedingung erstellt wurde.

11. Klicken Sie auf **Absenden**.
12. **Wahlweise:** Wiederholen Sie Schritt 8, um zusätzliche Richtlinienbedingungen zu erstellen.

Hinweis:
Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen OR-Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „wahr“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

Basierend auf der Rollenfilterrichtlinie (Benutzer) und den für die Rolle angegebenen Bedingungen wird „SMS als MFA-Faktor“ als Optionen für die Authentifizierung für die Benutzer angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multifaktor-Authentifizierung Provider

Verwenden Sie MFA-Provider, um die SMS- und E-Mail-basierte Authentifizierung zu konfigurieren, um sicherzustellen, dass sich jeder Benutzer sicher anmelden kann.

Auf der Now Platformkönnen Sie MFA-Provider mit dem Mechanismus der Verwendung von Multifaktor-Authentifizierung wie E-Mail und SMS konfigurieren.

Sie können die folgende Providerkonfiguration verwenden, die für MFA in Now Platformverfügbar ist:

- Konfiguration des E-Mail-Anbieters
- Konfiguration des Twilio-Providers
- InfoBIP-Provider-Konfiguration

Hinweis:
Twilio und Infobip Provider-Konfiguration werden automatisch ausgefüllt, indem „Demodaten laden“ bei Installation der Plugins „Multifaktor-Authentifizierung mit SMS“ (com.snc.authentication.sms_mfa) und „Notify – Twilio Direct“-Treiber (com.snc.notify.twilio_direct) aktiviert wird.

Sie können auch eine eigene Anbieterkonfiguration erstellen, um die Multifaktor-Authentifizierung mit SMS und E-Mail zu aktivieren.

Hinweis:
Die InfoBIP-Provider-Konfiguration wird als Teil der Demodaten bereitgestellt. Sie können die Felder basierend auf Ihren Anforderungen für die Konfiguration Ihres eigenen Providers bearbeiten.

Konfigurieren Sie den MFA-Provider

Konfigurieren Sie SMS und E-Mail mit dem Provider, um sicherzustellen, dass sich jeder Benutzer sicher anmelden kann.

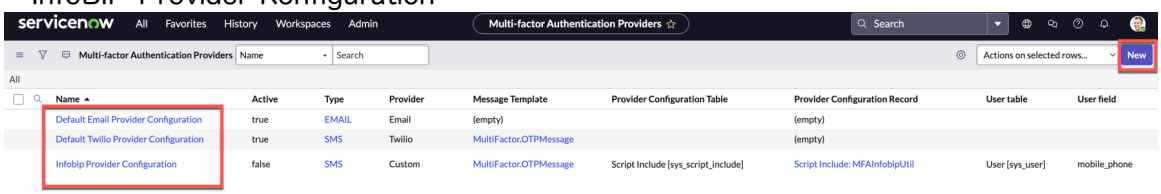
Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Anbieter**.

   Die folgenden Anbieterkonfigurationen sind für MFA innerhalb von Now Platformverfügbar:

   - Konfiguration des E-Mail-Anbieters
   - Konfiguration des Twilio-Providers
   - InfoBIP-Provider-Konfiguration



2. Um einen neuen Provider zu erstellen, klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Name	Name des Datensatzes.
Typ	Beschreibung des Datensatzes.
Anbieter	Wählen Sie **Twilio** oder **Benutzerdefiniert**aus. **Hinweis:** Informationen zur Konfiguration von Twilio finden Sie unter Notify mit Twilio konfigurieren . Wenn Sie **Benutzerdefiniert**auswählen, müssen Sie die folgenden Felder angeben: ○ Konfigurationstabelle des Anbieters ○ Konfigurationsdatensatz des Anbieters ○ Skript ○ Anwendertabelle ○ Benutzerfeld
Nachrichtenvorlage	Die Nachrichtenvorlage für den Datensatz.
Aktiv	Option zum Aktivieren der Provider-Konfiguration.

4. Klicken Sie auf **Absenden**.

Basierend auf der Nachrichtenvorlage und den Anbieterkonfigurationen wird die SMS oder E-Mail als Faktor für die Authentifizierung während des Anmeldevorgangs an Benutzer gesendet.

Benutzerdefinierte Konfiguration des Vonage-Providers (Tutorial)

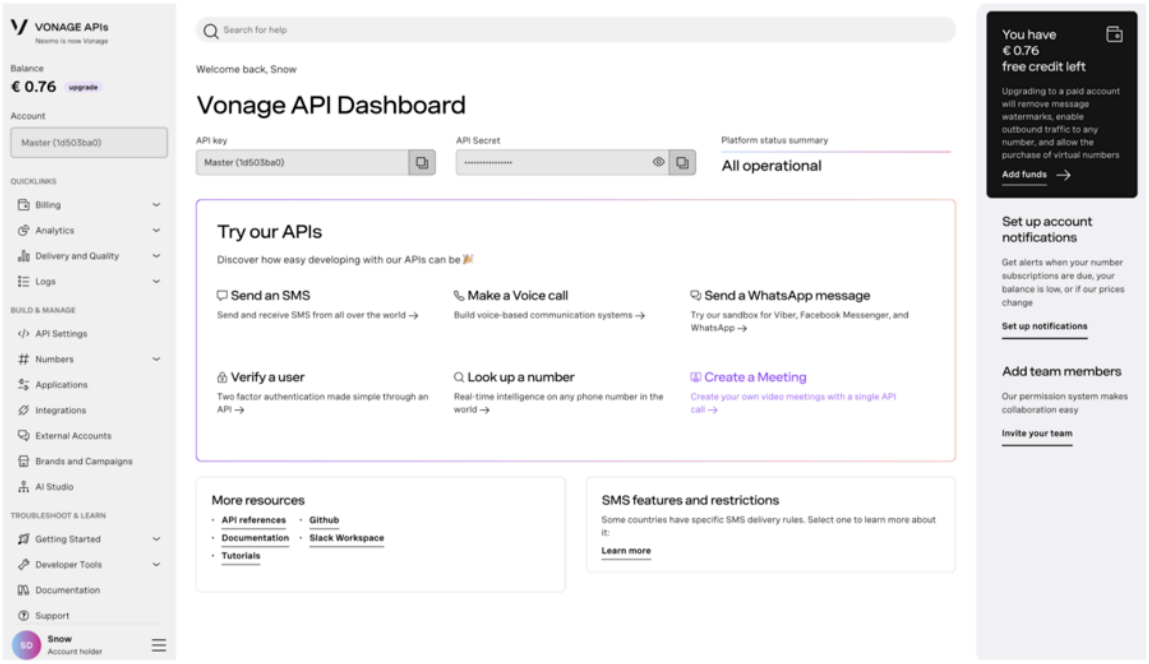
Konfigurieren Sie eine SMS mit dem Vonage-Provider, um sicherzustellen, dass sich jeder Benutzer sicher anmelden kann.

Vorbereitungen
Erforderliche Rolle: admin

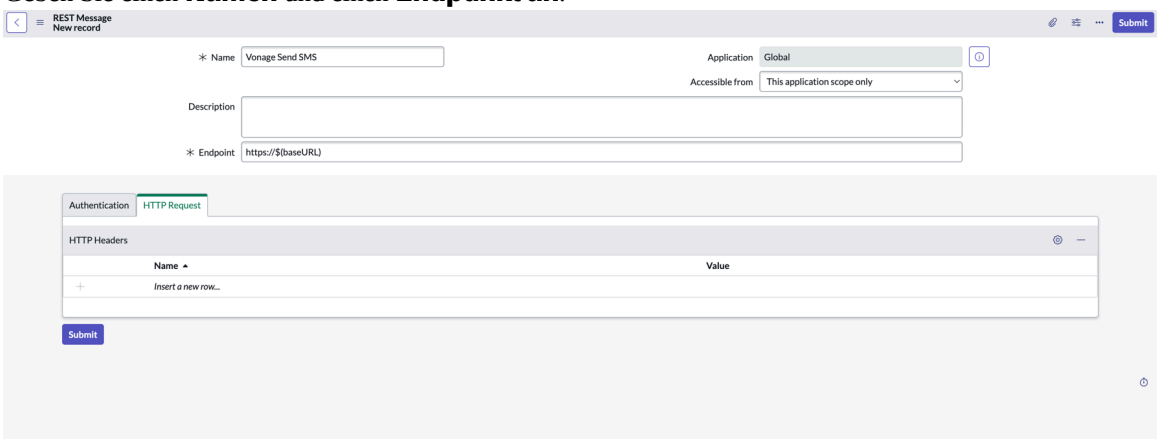
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **Ausgehend** > **REST-Nachricht** und führen die REST-Nachrichtenkonfiguration basierend auf den Informationen aus dem Vonage API-Dashboard durch.



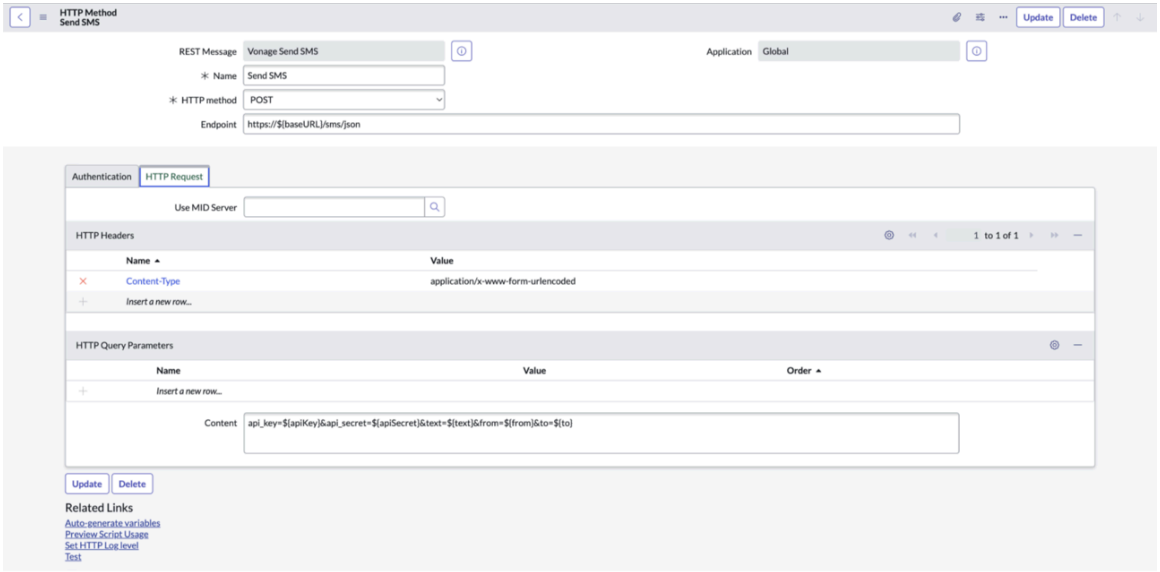
2. Klicken Sie auf **Neu**, um eine neue **REST-Nachricht**zu erstellen.
3. Geben Sie einen **Namen** und einen **Endpunkt an**.



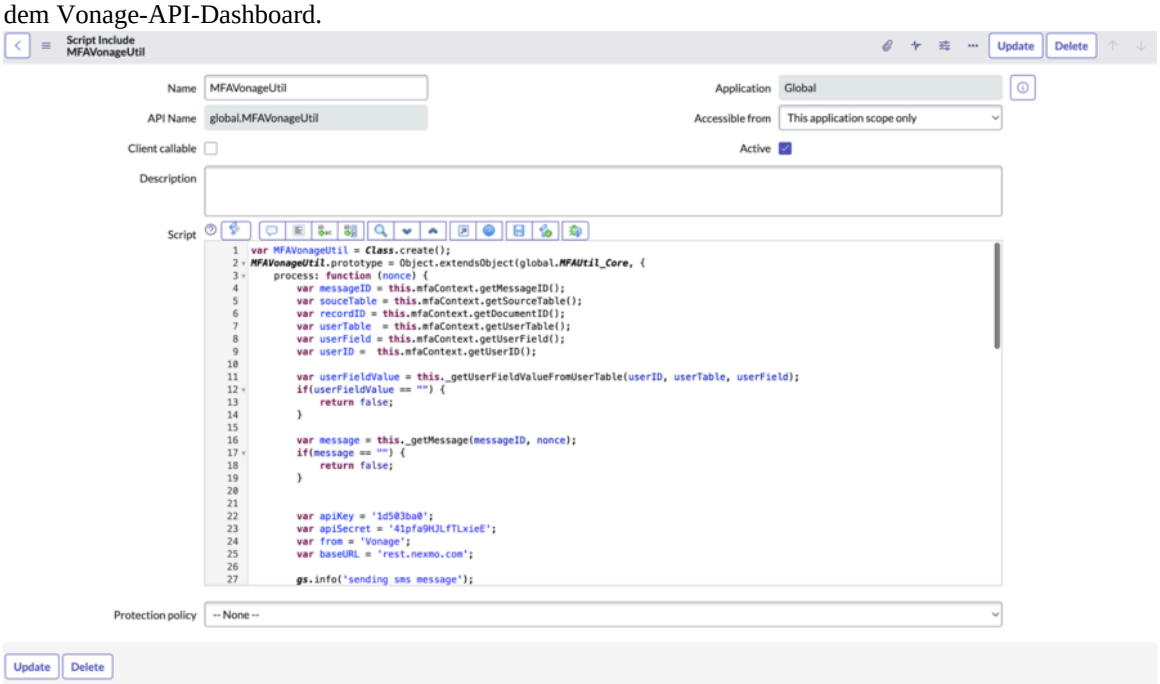
4. Klicken Sie auf **Absenden**.
5. Öffnen Sie den erstellten Datensatz, klicken Sie in der zugehörigen Liste **HTTP-Methoden** auf **Neu**, und wählen Sie die HTTP-Methode als **POST aus**.
6. Füllen Sie die folgenden Felder aus:
   - Endpunkt: `https://${baseURL}/sms/json`
   - Inhalt:`api_key=${apiKey}&api_secret=${apiSecret}&text=${text}&from=${from}&to=${to}`
   - Inhaltstyp: `application/x-www-form-urlencoded`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

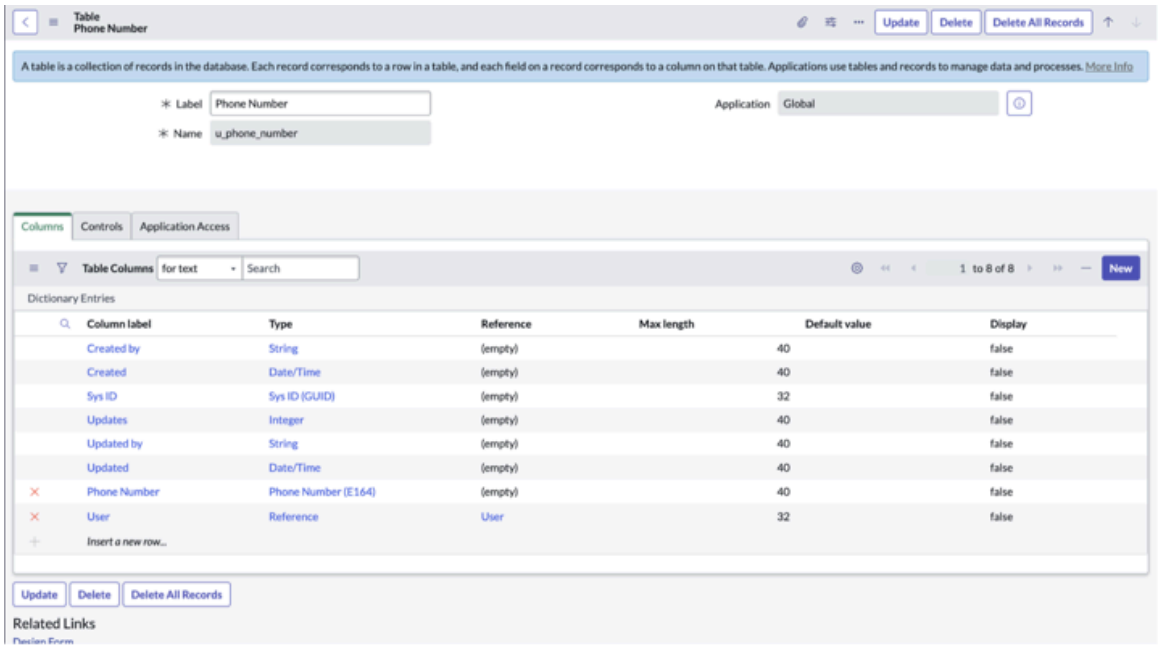


7. Aktualisieren Sie den Datensatz.
8. Klicken Sie im Abschnitt „ **Zugehörige Links** “ auf **Variablen automatisch generieren**.
9. Importieren Sie die im Ordner freigegebene SI, und kopieren Sie den apiKey und den geheimen Schlüssel aus dem Vonage-API-Dashboard.

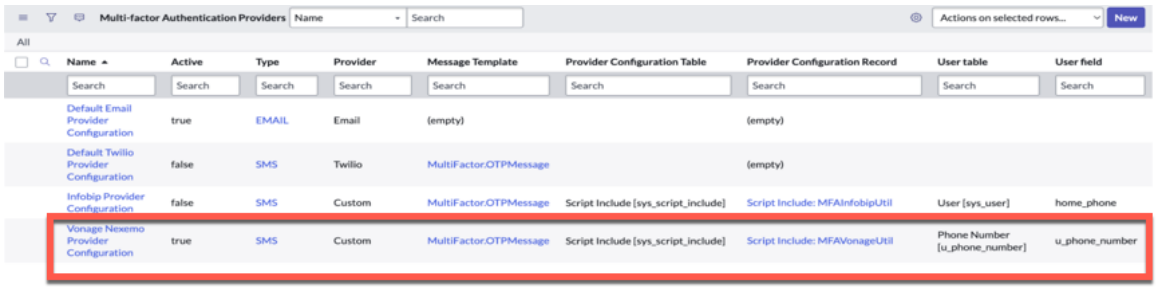


10. Erstellen Sie eine benutzerdefinierte Tabelle „Telefonnummern“ mit zwei Spalten, z. B.:
    - **Spaltenbezeichnung**: Benutzer, **Typ**: Referenz, **Referenz**: Benutzer (sys_user).
    - **Spaltenbezeichnung**: Telefonnummer, **Typ**: Telefonnummer (E164).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Erstellen Sie einen benutzerdefinierten Provider in der Multifaktor-Provider-Tabelle.



Weitere Informationen zur Provider-Konfiguration finden Sie unter Konfigurieren Sie den MFA-Provider.

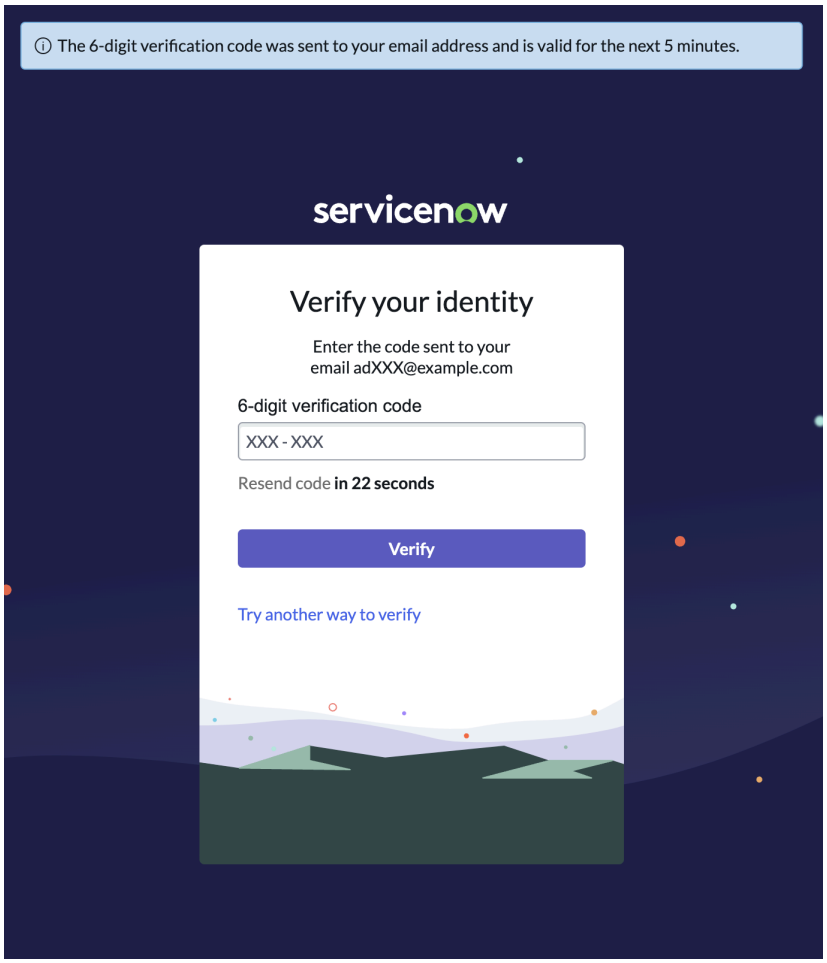
Multifaktor-Authentifizierung mit E-Mail

Multifaktor-Authentifizierung (MFA) mit E-Mail als Faktor für Ihre Authentifizierung.

Der Administrator kann die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden, erforderlich sind.

Hinweis:
MFA mit E-Mail wird standardmäßig mit dem Plugin „Integration - Multifactor Authentication“ (com.snc.integration.multifactor.authentication) aktiviert. Sie müssen die Richtlinieneingaben und -bedingungen konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die OTP-E-Mail an die zugeordnete E-Mail-Adresse gesendet. Der Benutzer kann den sechsstelligen Überprüfungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und seine Identität überprüfen.

Konfigurieren Sie E-Mail als MFA-Faktor

Konfigurieren Sie die Richtlinieneingabe und -bedingung, um E-Mail-OTP als MFA-Faktorrichtlinie für die Authentifizierung anzuzeigen.

Vorbereitungen
Erforderliche Rolle: admin

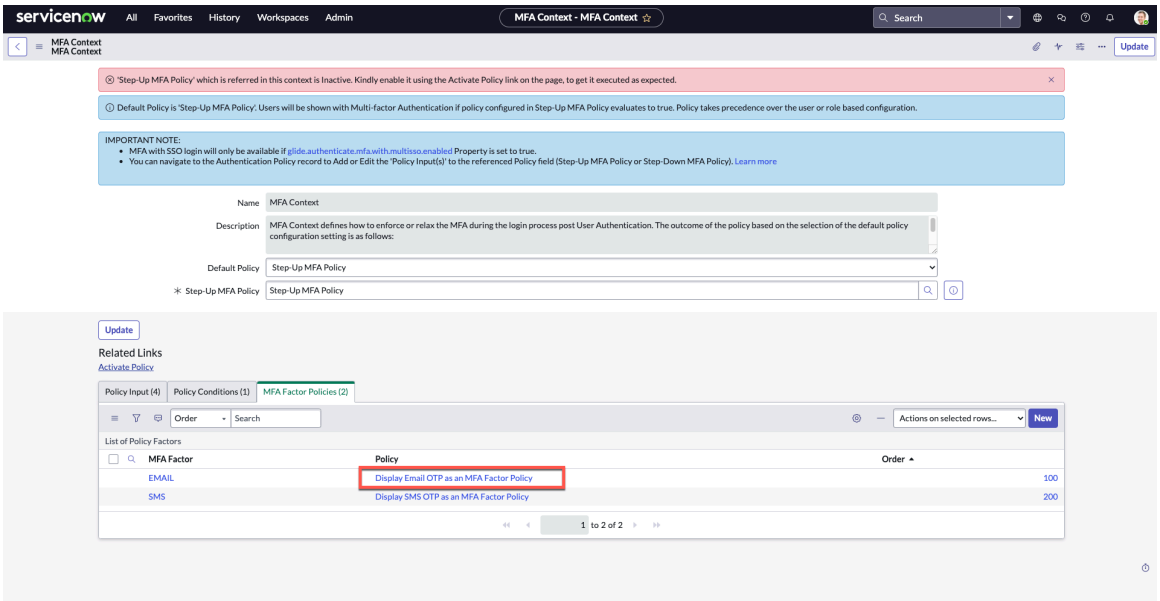
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**.
2. Klicken Sie auf die Registerkarte **MFA-Faktorrichtlinien**.

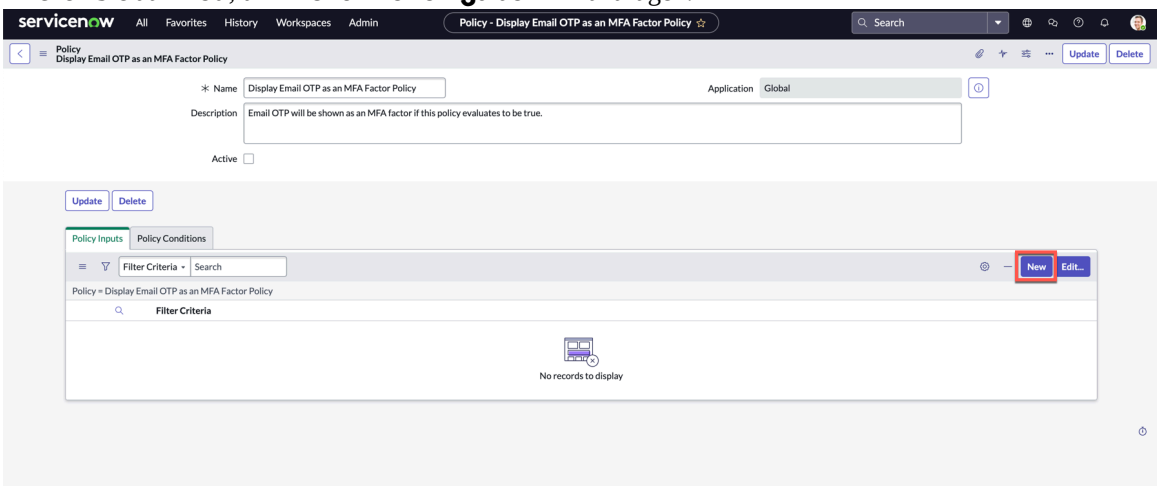
> **Hinweis:**
> E- **Mail** als **MFA-Faktor mit einer Richtlinie** ist standardmäßig verfügbar. Sie können die Richtlinie bearbeiten und die Richtlinieneingaben und -bedingungen angeben.

3. Wählen Sie das **OTP „E-Mail anzeigen“ als MFA-Faktorrichtlinie aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Neu**, um **Richtlinieneingaben**hinzuzufügen.



5. Wählen Sie die Filterkriterien aus, die Sie erstellen möchten.

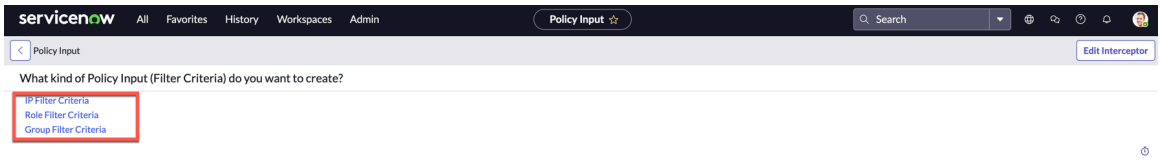
   Im Folgenden sind die Arten von Filterkriterien aufgeführt:

   - IP-Filterkriterien
   - Rollen-Filterkriterien
   - Gruppenfilterkriterien

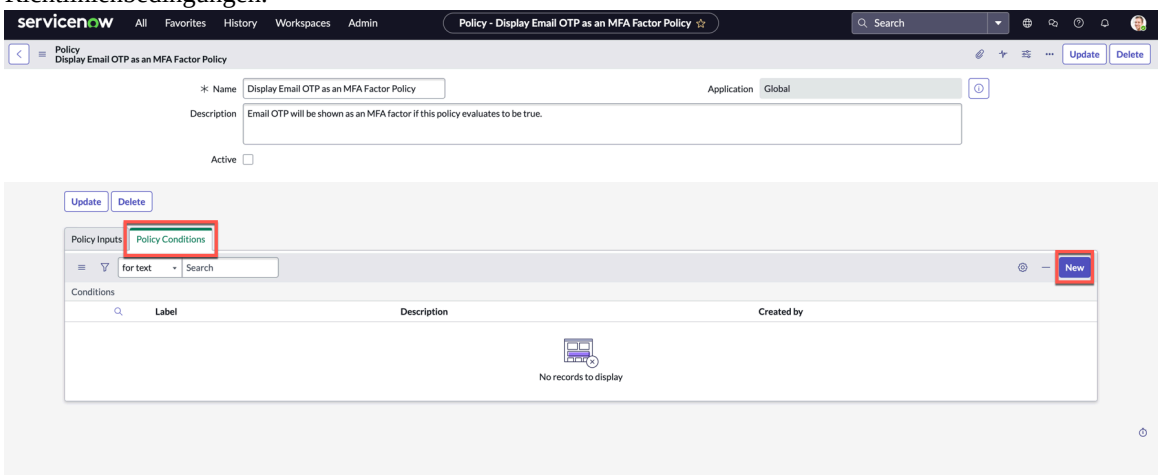
   Beispiel: Rollenfilterkriterien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie **auf Rollenfilterkriterien**.
7. Füllen Sie die Felder für die Rollenfilterkriterien aus, und übermitteln Sie den Datensatz.
   Die neue Richtlinie wird erstellt. Weitere Informationen finden Sie unter Rollenfilterkriterien
8. Klicken Sie auf der Seite „Richtlinie – E-Mail-OTP als MFA-Faktorrichtlinie anzeigen“ auf Richtlinienbedingungen.



9. Klicken Sie auf **Neu**, um **Richtlinienbedingungen**hinzuzufügen.
10. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination mehrerer Richtlinieneingaben (Filterkriterien), die zum Auswerten von Authentifizierungsanforderungen verwendet wird. Wählen Sie die rollenbasierte Filterkriterienrichtlinie aus, die für die Bedingung erstellt wurde.

11. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. **Wahlweise:** Wiederholen Sie Schritt 8, um zusätzliche Richtlinienbedingungen zu erstellen.

Hinweis:
Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen OR-Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „wahr“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

Basierend auf der Rollenfilterrichtlinie (Benutzer) und den für die Rolle angegebenen Bedingungen wird der E-Mail-MFA-Faktor als Optionen für die Authentifizierung für die Benutzer angezeigt.

Multifaktor-Authentifizierung (MFA) verwenden

Erfahren Sie, wie Sie mit Tools für die Multifaktor-Authentifizierung sicher auf Ihre Instanz zugreifen können.

Melden Sie sich mit MFA an

ServiceNow erfordert Authentifikatoranwendungen, die zeitbasierte Einmalpasswörter (TOTP) unterstützen. ServiceNow testet MFA mit den folgenden Authentifikatoren:

- Google Authentifikator
- Microsoft Authentifikator
- LastPass-Authentifikator
- Auth
- FreeOTP
- Duo
- Okta Verifizieren

Hinweis:
Andere nicht aufgeführte Authentifikatoren sind möglicherweise ebenfalls kompatibel, werden jedoch nicht von ServiceNowgetestet.

Hinweis:
Informationen zu browserspezifischen Verhaltensänderungen finden Sie in diesem KB-Artikel .

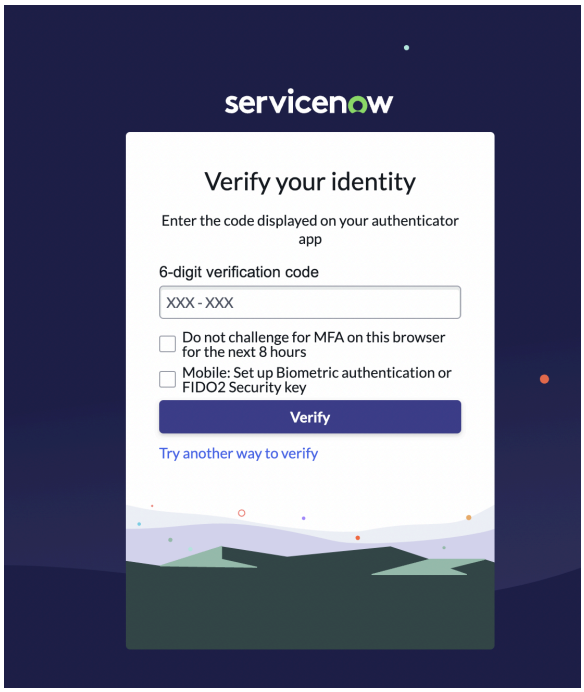
Wenn Ihr Administrator die Multifaktor-Authentifizierung (MFA) für Ihre Instanz aktiviert hat, werden Sie nach der Eingabe Ihres Benutzernamens und Passworts zu einer zweiten Authentifizierung aufgefordert. Weitere Informationen zum MFA-Anmeldevorgang finden Sie unter Melden Sie sich mit Multifaktor-Authentifizierung an

Validierung mit Authentifikator-App

Wenn Sie keine zweite Authentifizierungsform konfiguriert haben, wird nach der Anmeldung eine Konfigurationsseite angezeigt, die Sie durch die Einrichtung einer Authentifizierungs-App führt. Weitere Informationen zu diesem Setup finden Sie unter Richten Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Multifaktor-Authentifizierung bei der ersten Anmeldung ein.



Geben Sie den in Ihrer Authentifikator-App angezeigten Code ein, um sich anzumelden.

Registrieren Sie ein Authentifizierungsgerät

Nachdem Sie eine Authentifizierungs-App konfiguriert haben, können Sie andere Methoden für die Authentifizierung registrieren.

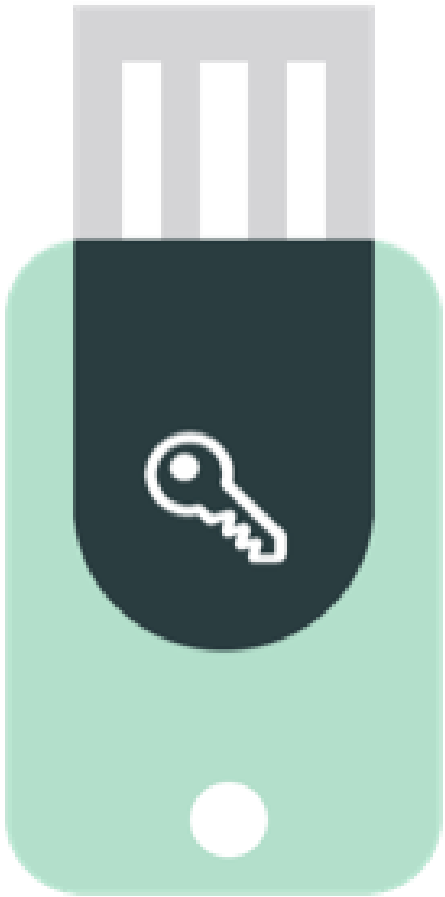
Biometrische Authentifikatoren

Als zweite MFA-Authentifizierung können Sie biometrische Authentifikatoren wie Fingerabdruck oder Gesichtserkennung verwenden. Wenn Ihr Administrator diese Option zulässt, können Sie biometrische Authentifikatoren mithilfe der Schritte in Registrieren Sie einen biometrischen Authentifikatorkonfigurieren.

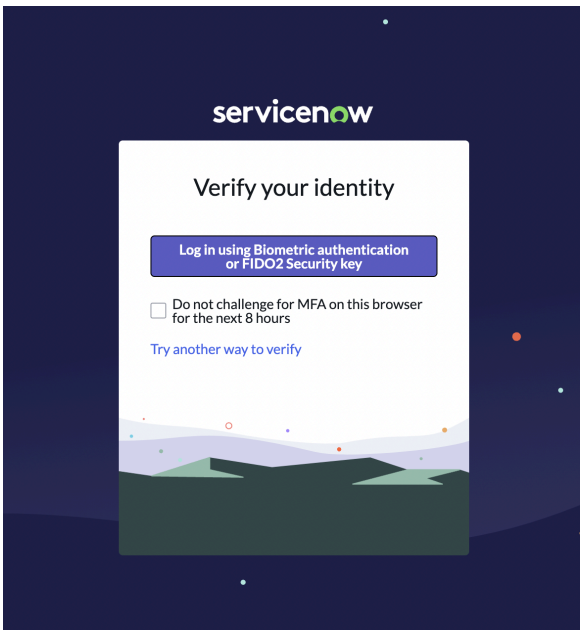
Hardwareschlüssel-Authentifikatoren

Hardwareschlüssel sind physische Sicherheitsgeräte, die Sie zur Authentifizierung verwenden können. Sie können ein Hardwaregerät für die Verwendung mit Ihrer Instanz mithilfe der Schritte in Registrieren Sie einen Hardware-Sicherheitsschlüsselregistrieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Validierung mit Biometrie oder Hardwareschlüssel



Verwenden Sie den Biometrie- oder Sicherheitsschlüssel, um sich anzumelden.

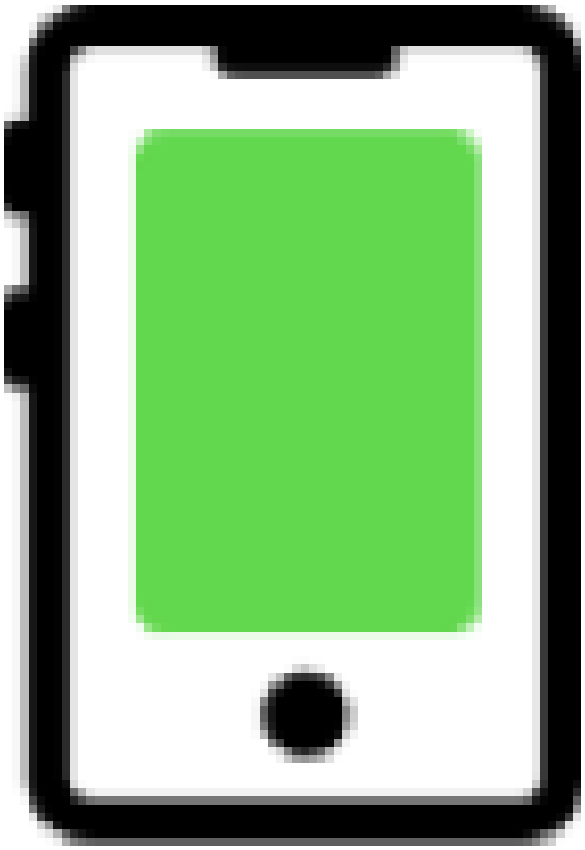
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie eine Telefonnummer für OTP

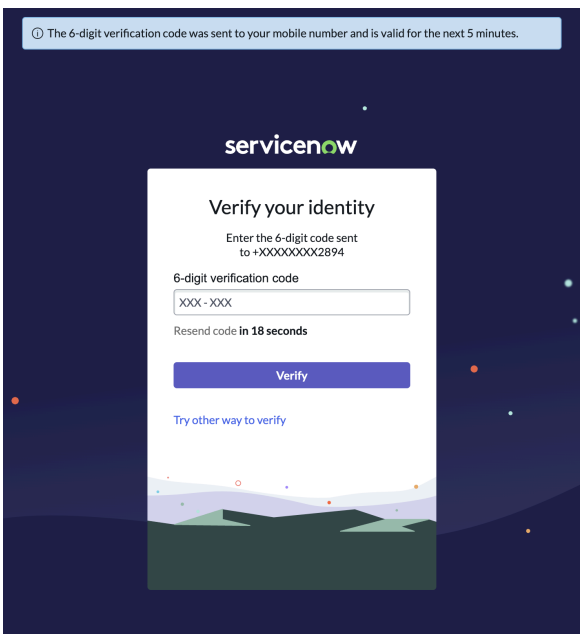
SMS

Der Administrator konfiguriert die Instanz ServiceNow so, dass Benutzer, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden, erforderlich sind.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die OTP-SMS an die Mobiltelefonnummer gesendet, die dem sys_user-Datensatz zugeordnet ist. Benutzer können den sechsstelligen Überprüfungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.



Validierung mit SMS



Geben Sie den sechsstelligen Code ein, der an die Mobiltelefonnummer gesendet wurde, um sich anzumelden. Der gesendete Code ist für die nächsten 5 Minuten gültig. Sie können Code erneut senden verwenden, um den Code erneut zu senden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

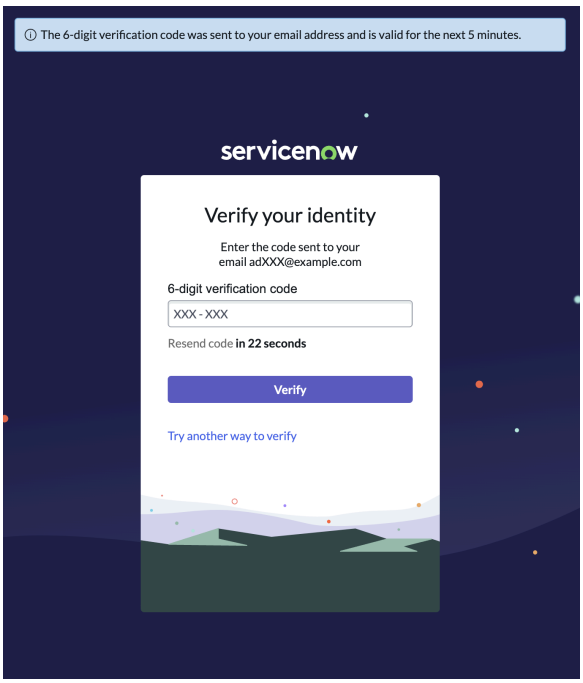
Registrieren Sie eine E-Mail-Adresse für OTP

E-Mail-Adresse

Der Administrator konfiguriert die Instanz ServiceNow so, dass Benutzer erforderlich sind, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird E-Mail-OTP an die E-Mail-Adresse gesendet, die dem Benutzer zugeordnet ist. Der Benutzer kann den sechsstelligen Überprüfungscode eingeben, der an das Mobilgerät gesendet wurde, und seine Identität überprüfen.

Validierung mit E-Mail



Geben Sie den sechsstelligen Code ein, der an die E-Mail-Adresse gesendet wurde, um sich anzumelden. Der gesendete Code ist für die nächsten 5 Minuten gültig. Sie können Code erneut senden verwenden, um den Code erneut zu senden.

Richten Sie die Multifaktor-Authentifizierung bei der ersten Anmeldung ein

Wenn Ihr Administrator die Multifaktor-Authentifizierung für Ihr Profil aktiviert hat, Sie die Anwendung jedoch noch nicht eingerichtet haben, können Sie sie bei der Anmeldung einrichten.

Vorbereitungen

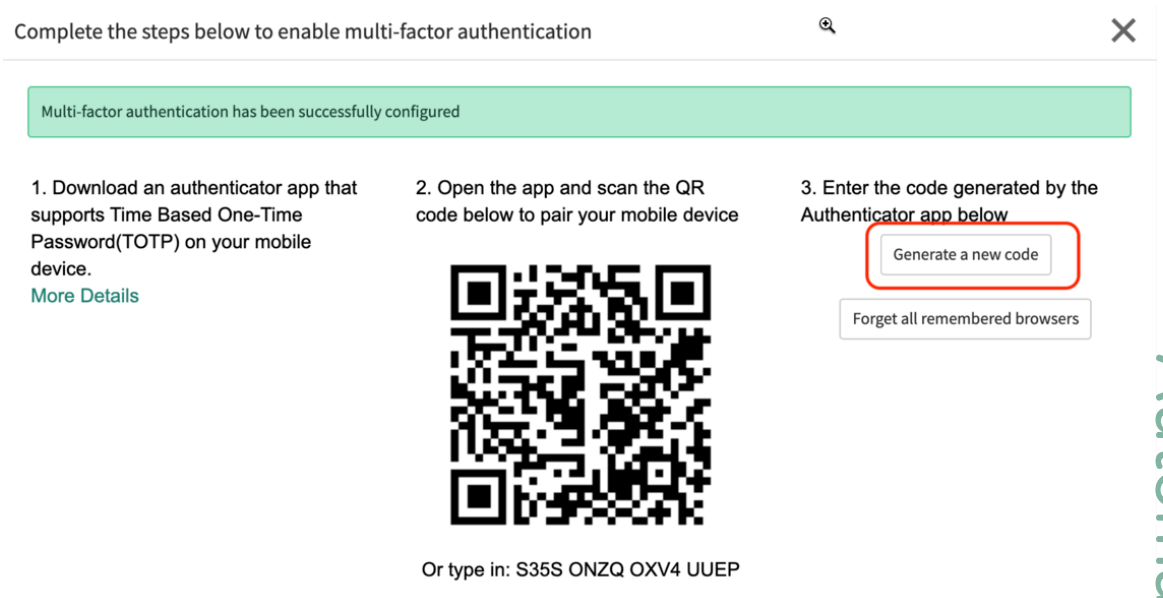
Erforderliche Rolle: keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrer Instanz an.
   Der Setup-Bildschirm der Multifaktor-Authentifizierung erfasst Ihre Anmeldung.



2. Wenn Sie die jetzt eingerichtete Authentifizierung überspringen möchten, klicken Sie auf **Setup umgehen**.
   Sie können die Multifaktor-Authentifizierung für eine begrenzte Anzahl von Malen umgehen, die Ihr Administrator zulässt. Schließlich müssen Sie die Multifaktor-Authentifizierung konfigurieren.
3. Machen Sie ein Foto des QC-Codes mit der Anwendung Google Authenticator, oder geben Sie die Zeichenfolge manuell in die Anwendung ein.
4. Geben Sie den Code ein, und klicken Sie auf **Gerät koppeln und anmelden**.

   Die Anwendung antwortet mit einem sechsstelligen Code, der alle 30 Sekunden aktualisiert wird. Wenn Sie den richtigen Code eingegeben haben, wird eine Meldung angezeigt, die Sie darüber informiert, dass die Multifaktor-Authentifizierung eingerichtet ist. Wenn Sie einen ungültigen Code eingegeben haben, suchen Sie auf Ihrem Mobilgerät erneut nach dem Code, da er möglicherweise aktualisiert wurde, und geben Sie den angezeigten Code ein.

   Hinweis:
   Damit der Code ordnungsgemäß funktioniert, muss sich die Systemzeit auf Ihrem Computer in derselben Zeitzone befinden wie die Zeit auf Ihrem Mobilgerät.

Richten Sie die Multifaktor-Authentifizierung für Ihr Benutzerprofil ein

Aktivieren Sie die Multifaktor-Authentifizierung für Ihren Account in Ihren Benutzerprofileinstellungen.

Vorbereitungen
Erforderliche Rolle: keine

Die Multifaktor-Authentifizierung muss für Ihre Instanz aktiviert sein.

Automatische Übersetzung

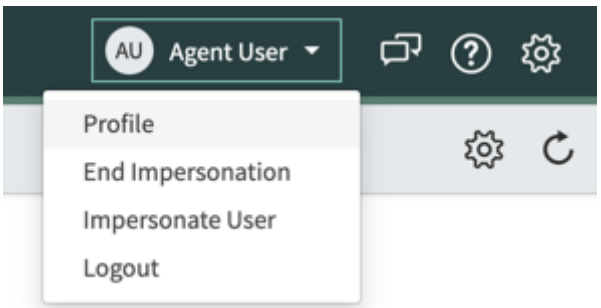
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ihr Administrator verlangt möglicherweise die Verwendung der Multifaktor-Authentifizierung. In diesem Fall werden Sie bei der Anmeldung automatisch aufgefordert. Weitere Informationen finden Sie unter Richten Sie die Multifaktor-Authentifizierung bei der ersten Anmeldung ein. Gehen Sie wie folgt vor, wenn Ihr Administrator Ihnen erlaubt, sich für die Multifaktor-Authentifizierung zu entscheiden.

Prozedur

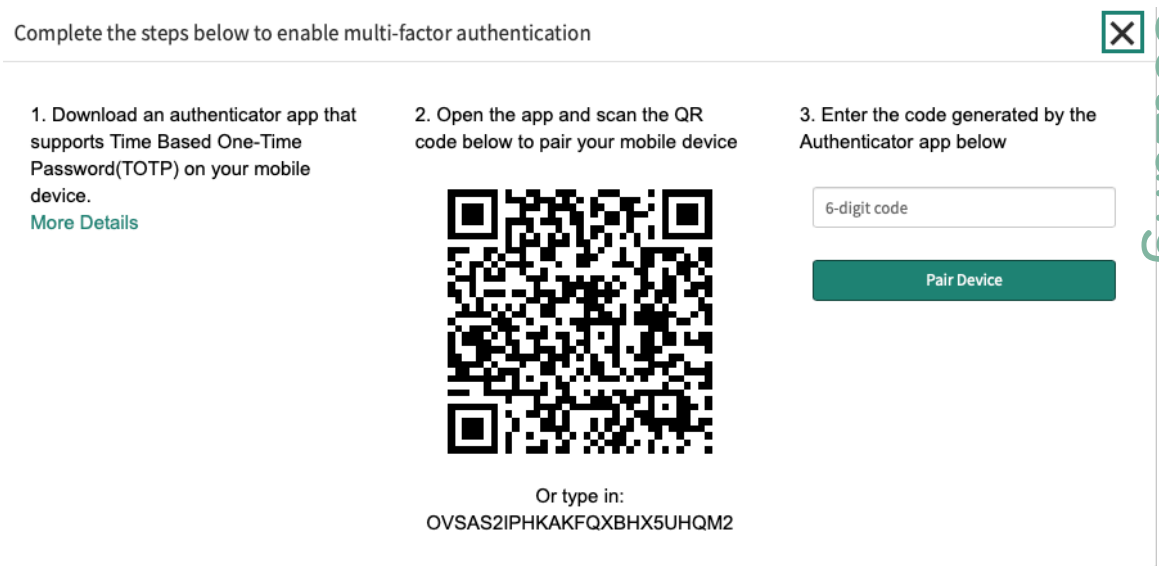
1. Navigieren zu **Alle** > **Selfservice** > **Mein Profil**.

Hinweis:
Sie können Ihr Profil auch aufrufen, indem Sie im Instanz-Header auf Ihren Benutzernamen klicken.



2. Klicken Sie in Ihrem Benutzerprofil im Abschnitt „ **Zugehörige Links** “ auf **Muti-Faktor-Authentifizierung** oder **Accountwiederherstellung aktivieren**.
3. Befolgen Sie die Anweisungen auf dem Bildschirm, um eine Authentifikator-App zu registrieren. ServiceNow unterstützt Authentifikatoren für Mobile-Apps und Browsererweiterungen. Weitere Informationen zu diesen Apps finden Sie unter Authentifikatoranwendungen.

Hinweis:
Auch wenn Sie sich mit einem Biometrie- oder Hardwareschlüssel authentifizieren möchten, müssen Sie zuerst eine Authentifikator-App registrieren.



Ergebnisse

Die Multifaktor-Authentifizierung ist für Ihr Benutzerkonto aktiviert. Bei der nächsten Anmeldung werden Sie aufgefordert, die Multifaktor-Authentifizierung zu verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können die Multifaktor-Authentifizierung für Ihren Account nicht deaktivieren, nachdem Sie sie aktiviert haben. Wenn Sie die Multifaktor-Authentifizierung deaktivieren müssen, wenden Sie sich an Ihren Administrator.

Nächste Maßnahme

Wenn Sie für die Anmeldung bei Ihrer Instanz einen Hardwareschlüssel oder biometrischen Authentifikator verwenden möchten, können Sie diese Authentifikatoren jetzt registrieren. Weitere Informationen finden Sie unter Registrieren Sie einen biometrischen Authentifikator und Registrieren Sie einen Hardware-Sicherheitsschlüssel.

Melden Sie sich mit Multifaktor-Authentifizierung an

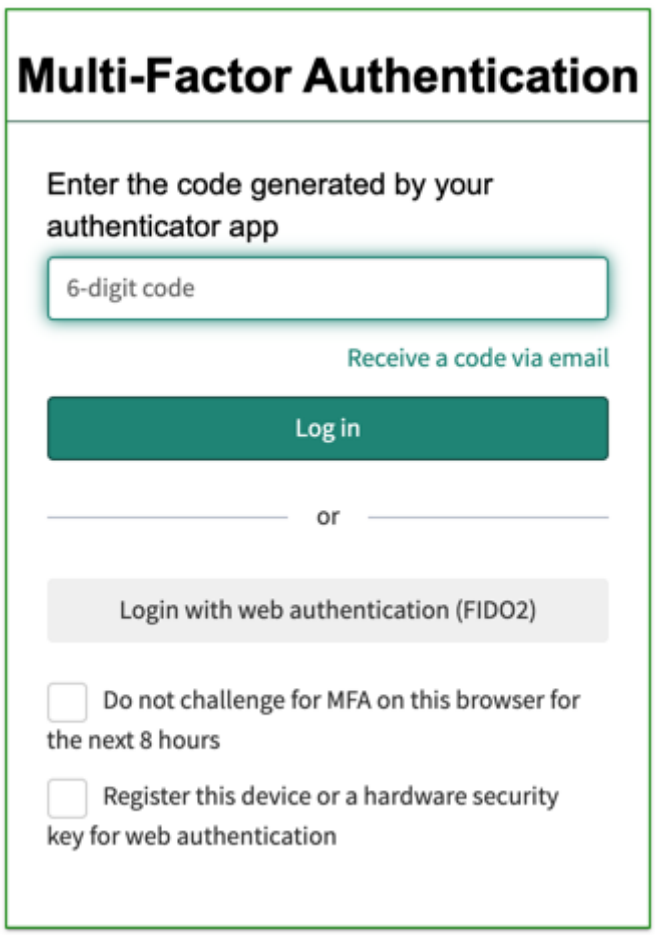
Nachdem die Multifaktor-Authentifizierung für Ihr Benutzerprofil aktiviert wurde, können Sie sich mit dem Passcode anmelden, den Sie von der Google Authenticator-App erhalten.

Vorbereitungen

Für Ihr Profil muss die Multifaktor-Authentifizierung aktiviert sein. Sie können sie in Ihrem Benutzerprofil selbst aktivieren, oder Ihr Administrator kann sie für Sie aktivieren.
Erforderliche Rolle: keine

Prozedur

1. Wechseln Sie zur URL Ihrer Instanz, um den Anmeldebildschirm zu öffnen.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.
3. Klicken Sie auf **Anmelden**.
   Der Bildschirm für die Multifaktor-Authentifizierung wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Öffnen Sie den Authentifikator auf Ihrem Mobilgerät oder in der Browsererweiterung, und notieren Sie sich die Nummer.

   Hinweis:
   Diese Zahl wird alle 30 Sekunden aktualisiert.

5. Geben Sie Ihren sechsstelligen Authentifizierungscode ein.
6. **Wahlweise:** Aktivieren **Sie MFA in diesem Browser für die nächsten 8 Stunden nicht** anfordern, um den Authentifikator bei der Anmeldung für die nächsten acht Stunden zu überspringen.
7. **Wahlweise:** Aktivieren Sie **Dieses Gerät oder einen Hardware-Sicherheitsschlüssel für die Webauthentifizierung** registrieren, um nach der Anmeldung ein biometrisches Gerät oder einen Hardware-Sicherheitsschlüssel zu registrieren.
8. **Wahlweise:** Wenn Sie bereits einen biometrischen Scanner oder Hardwareschlüssel registriert haben, klicken Sie auf **Anmeldung mit Webauthentifizierung (FIDO2)**, und folgen Sie den Anweisungen, um den Anmeldevorgang abzuschließen.
9. **Wahlweise:** Wenn Sie sich an den Passcode erinnern oder keinen Zugriff auf Ihren Authentifikator haben, klicken Sie auf den Link **Code per E-Mail erhalten**.

   Die Instanz sendet einen temporären Passcode an Ihre E-Mail-Adresse. Sie können diesen temporären Passcode nur einmal verwenden, und er ist nur 10 Minuten lang gültig.

   Hinweis:
   Sie müssen in Ihrem Benutzerprofil in der Instanz eine E-Mail-Adresse konfiguriert haben, um diese E-Mail-Nachricht zu erhalten.

10. Klicken Sie **auf Anmelden**.

Authentifikatoranwendungen

Verwenden Sie Authentifikatoranwendungen von Drittanbietern, um temporäre MFA-Passcodes zu generieren.

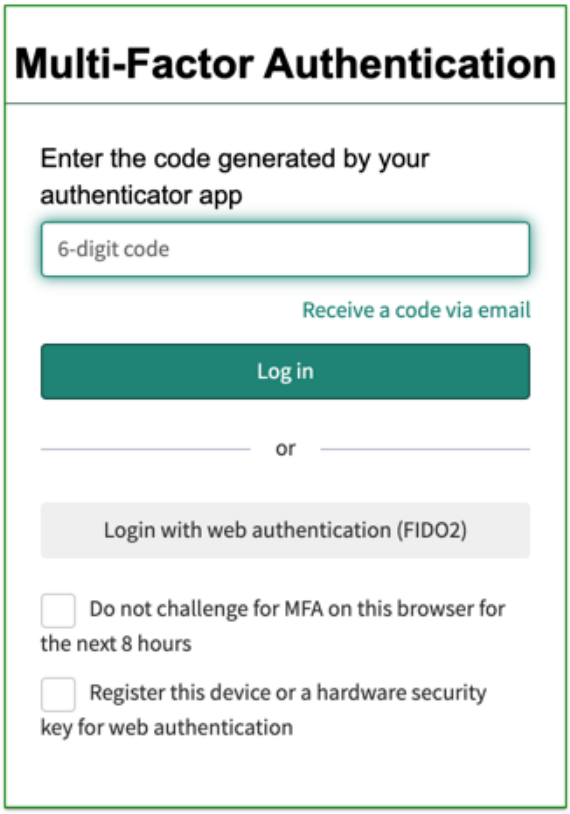
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Authentifikatoranwendung ist Software einer Drittpartei, die temporäre Passcodes generiert. Sie können diese Passcodes zusammen mit Ihrem Passwort verwenden, um sich bei einer Instanz anzumelden, die eine Multifaktor-Authentifizierung (MFA) erfordert.

Wenn Ihr Administrator MFA für Ihre Instanz aktiviert hat, werden Sie nach der Eingabe Ihres Benutzernamens und Ihres Passworts bei der Anmeldung zur Eingabe eines Passcodes aufgefordert.

ServiceNow erfordert Authentifikatoranwendungen, die zeitbasierte Einmalpasswörter (TOTP) unterstützen. ServiceNow testet MFA mit den folgenden Authentifikatoren:

- Google Authentifikator
- Microsoft Authentifikator
- LastPass-Authentifikator
- Auth
- FreeOTP
- Duo
- Okta Verifizieren



Hinweis:
Andere nicht aufgeführte Authentifikatoren sind möglicherweise ebenfalls kompatibel, werden jedoch nicht von ServiceNowgetestet.

Authentifikator-App ändern

Generieren Sie einen neuen Code, um die Authentifikator-App auf Ihrem Gerät zu ändern.

Vorbereitungen

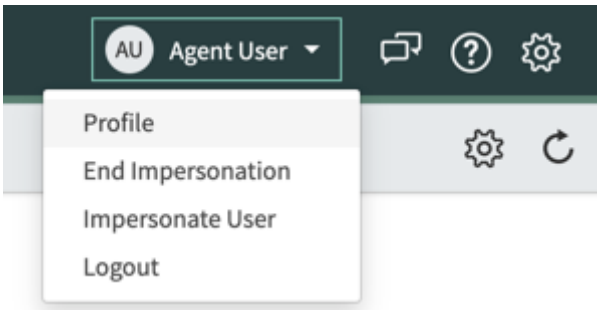
Für Ihr Profil muss die Multifaktor-Authentifizierung aktiviert sein. Sie können sie in Ihrem Benutzerprofil selbst aktivieren, oder Ihr Administrator kann sie für Sie aktivieren.
Erforderliche Rolle: keine

Prozedur

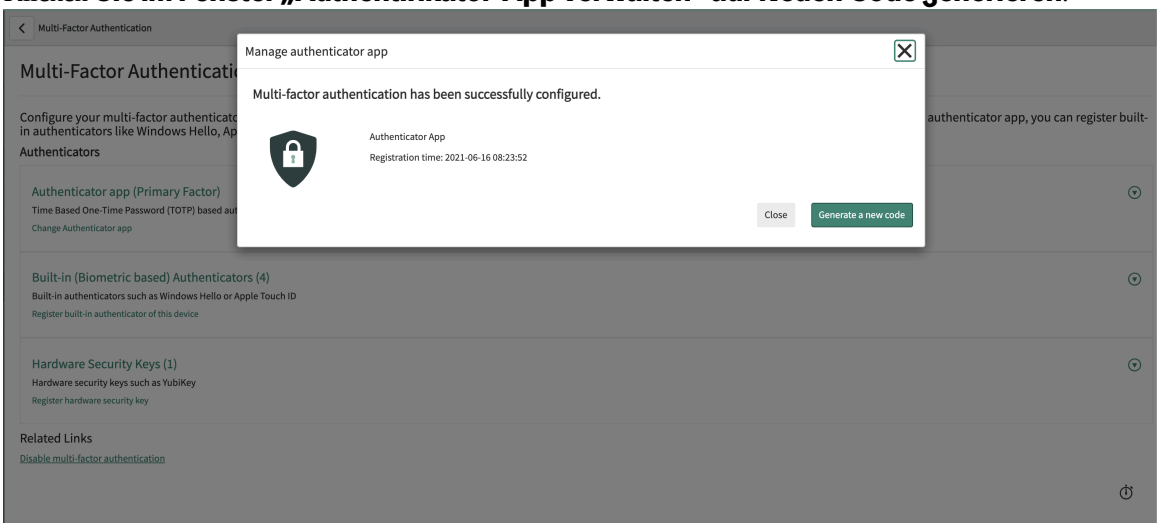
1. Navigieren zu **Alle** > **Selfservice** > **Mein Profil**.

Hinweis:
Sie können Ihr Profil auch aufrufen, indem Sie im Instanz-Header auf Ihren Benutzernamen klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie in Ihrem Benutzerprofil im Abschnitt „ **Zugehörige Links** “ auf **Muti-Faktor-Authentifizierung**.
3. Klicken Sie unter **Authentifikator-App (Primärer Faktor)**auf **Authentifikator-App ändern**.
4. Klicken **Sie im Fenster „Authentifikator-App verwalten“ auf Neuen Code generieren**.



5. Befolgen Sie die Anweisungen auf dem Bildschirm, um eine Authentifikator-App beim Gerät zu registrieren.

Webauthentifizierung

Ihre Benutzer können Hardwareschlüssel oder die biometrischen Leser (FIDO2) ihres Geräts verwenden, um sich bei einer Instanz zu authentifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwareschlüssel

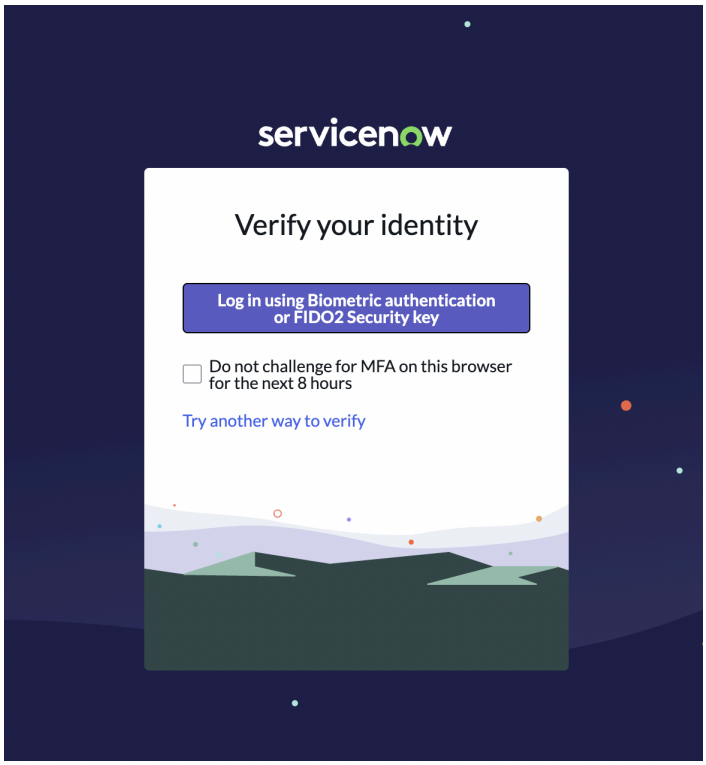
Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden zur Authentifizierung in einen Port Ihres Geräts eingefügt. Weitere Informationen zur Registrierung von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.

Biometrie

Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Benutzer zu identifizieren. Ihre Benutzer können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Weitere Informationen zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie den zweiten Faktor aus, den Sie authentifizieren möchten, und authentifizieren Sie sich bei Ihrer Instanz.



Informationen zum Konfigurieren des Webauthentifizierungs-Plugins finden Sie unter Aktivieren Sie das Webauthentifizierungs-Plugin.

Aktivieren Sie das Webauthentifizierungs-Plugin

Das Plugin „Integration - Web Authentication“ muss für die Webauthentifizierung (FIDO2) aktiviert sein.

Vorbereitungen
Erforderliche Rolle: admin.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „ **Integration – Web Authentication** “ (com.snc.integration.webauthn).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie einen biometrischen Authentifikator

Registrieren Sie einen biometrischen Authentifikator, der als Teil Ihrer Multifaktor-Authentifizierungsanmeldung verwendet werden soll.

Vorbereitungen

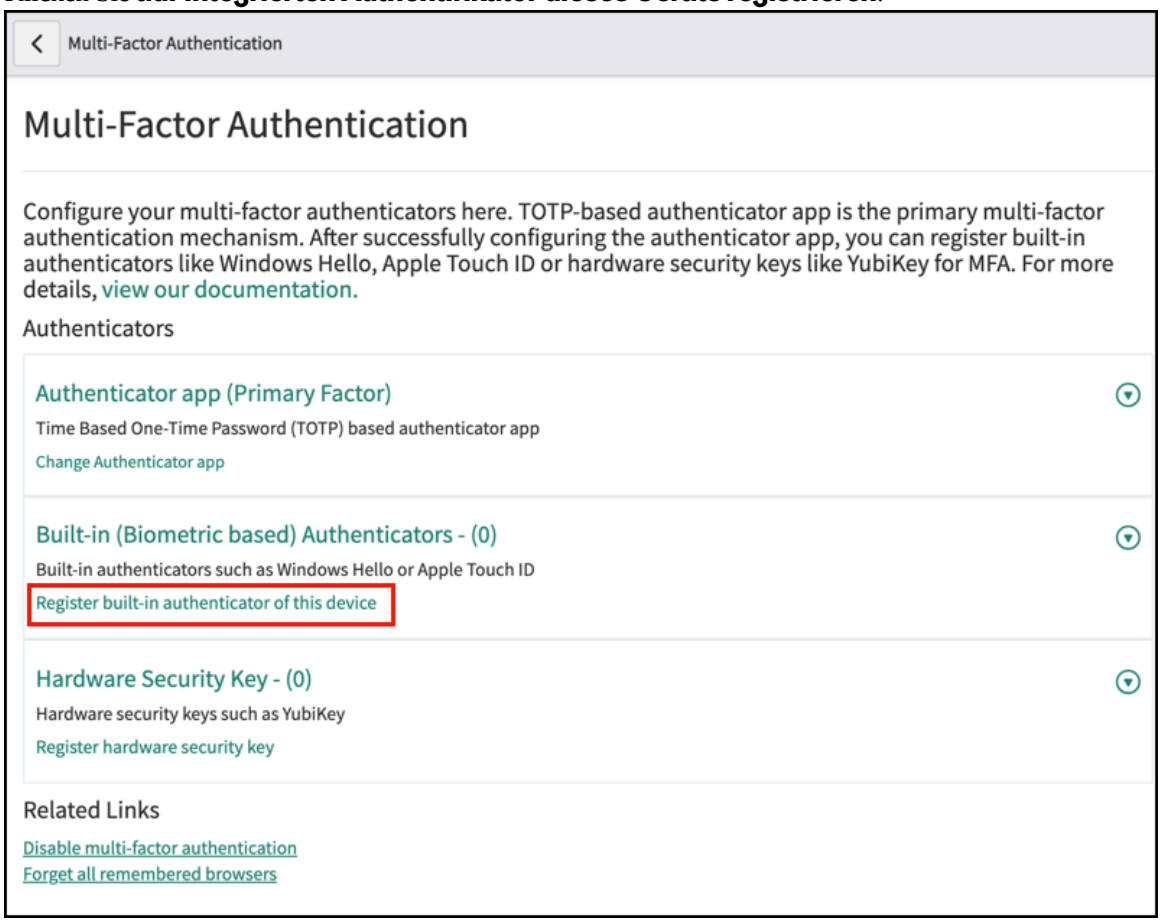
Erforderliche Rolle: keine

Hinweis:

Benutzer müssen zuerst eine Authentifikatoranwendung einrichten, bevor sie einen biometrischen Authentifikator konfigurieren können. Weitere Informationen zum Setup der Authentifikatoranwendung finden Sie unter Richten Sie die Multifaktor-Authentifizierung für Ihr Benutzerprofil ein.

Prozedur

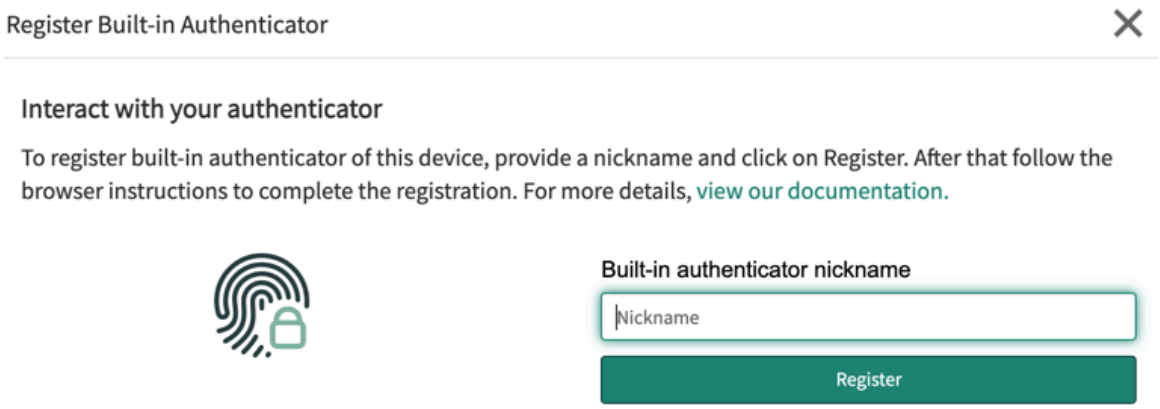
1. Navigieren zu **Alle** > **Selfservice** > **Mein Profil**.
2. Klicken Sie unter **Zugehörige Links**auf **Multifaktor-Authentifizierung**.
   Die Seite für die Multifaktor-Authentifizierung wird geöffnet.
3. Klicken Sie **auf Integrierten Authentifikator dieses Geräts registrieren**.



4. Geben Sie einen Kurznamen für Ihren Authentifikator ein, und klicken Sie auf **Registrieren**.

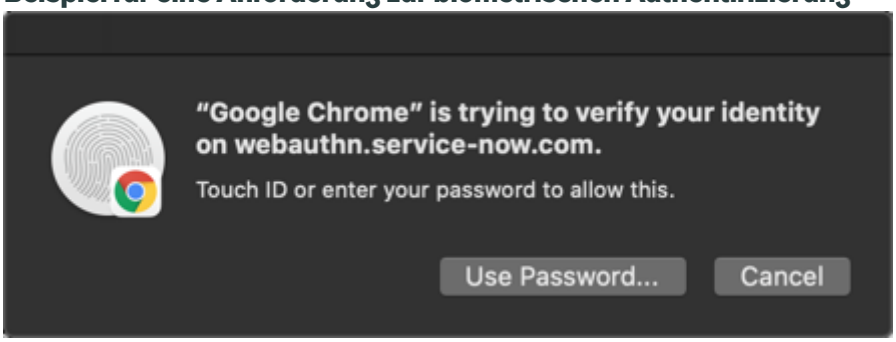
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wenn Sie dazu aufgefordert werden, befolgen Sie die Anweisungen auf dem Bildschirm, um sich bei Ihrem biometrischen Authentifikator zu authentifizieren.
   Diese Nachricht hängt von Ihrem spezifischen Authentifikator ab.

Beispiel für eine Anforderung zur biometrischen Authentifizierung



   Nach erfolgreicher Authentifizierung wird ein Bestätigungsfenster angezeigt.

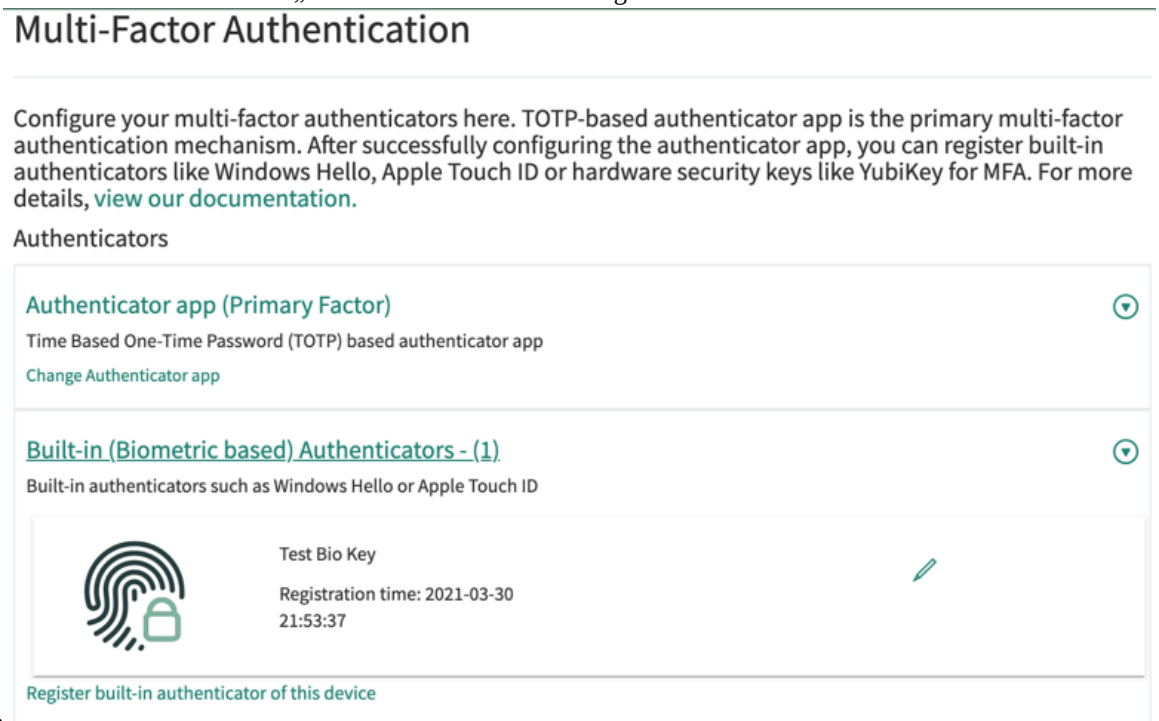
6. Schließen Sie das Bestätigungsfenster.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ihr biometrischer Authentifikator ist registriert. Sie können jetzt den Authentifikator auf der Seite „Multifaktor-Authentifizierung“ sehen.



Registrieren Sie einen Hardware-Sicherheitsschlüssel

Registrieren Sie einen Hardwareschlüssel, der als Teil Ihrer Multifaktor-Authentifizierungsanmeldung verwendet werden soll.

Vorbereitungen

Erforderliche Rolle: keine

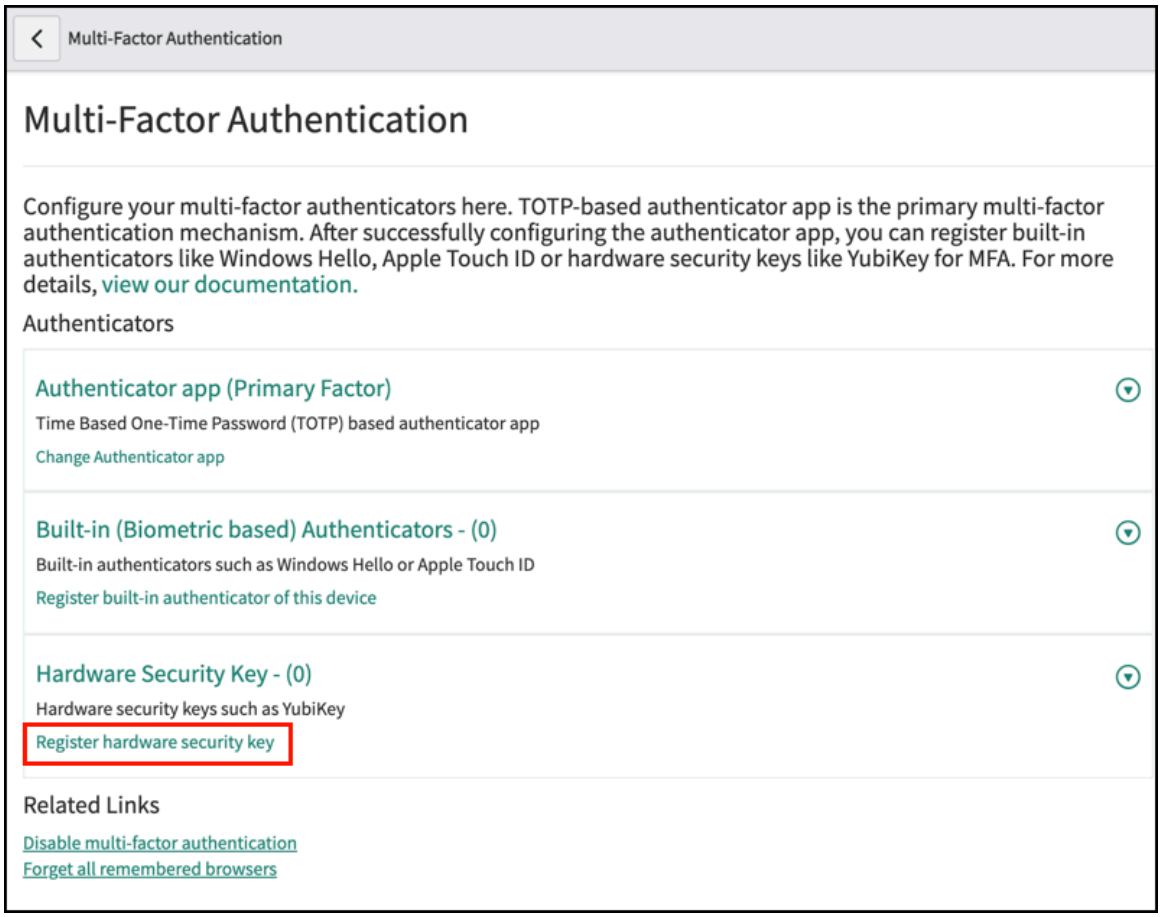
Hinweis:
Benutzer müssen zuerst eine Authentifikatoranwendung einrichten, bevor sie einen Hardwareschlüssel konfigurieren. Weitere Informationen zum Setup der Authentifikatoranwendung finden Sie unter Richten Sie die Multifaktor-Authentifizierung für Ihr Benutzerprofil ein.

Prozedur

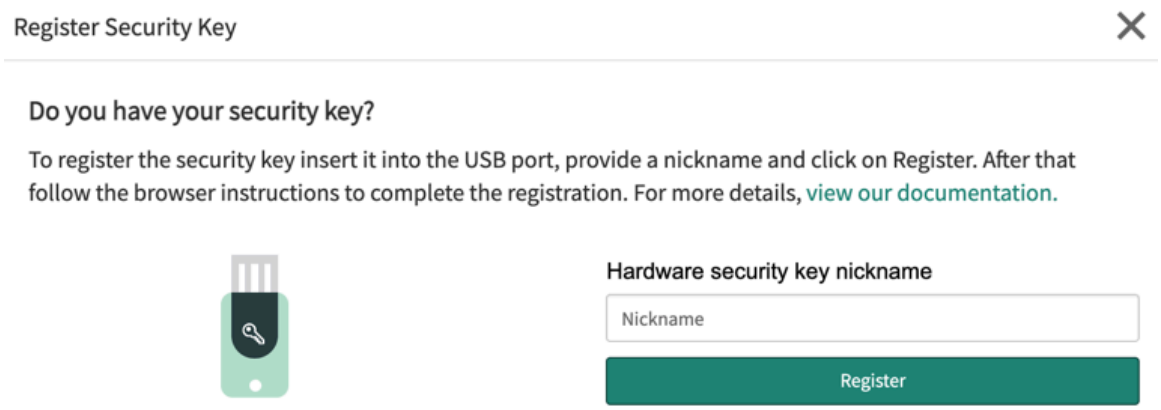
1. Navigieren zu **Alle** > **Selfservice** > **Mein Profil**.
2. Klicken Sie unter **Zugehörige Links**auf **Multifaktor-Authentifizierung**.
   Die Seite Multifaktor-Authentifizierung wird geöffnet.
3. Klicken Sie **auf Hardware-Sicherheitsschlüssel registrieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie einen Kurznamen für Ihren Hardwareschlüssel ein, und klicken Sie auf **Registrieren**.



5. Wenn Sie dazu aufgefordert werden, fügen Sie Ihren Hardware-Sicherheitsschlüssel ein, und aktivieren Sie ihn.
   Nach erfolgreicher Authentifizierung wird ein Bestätigungsfenster angezeigt.
6. Schließen Sie das Bestätigungsfenster.

Ergebnisse

Ihr Hardwareschlüssel ist registriert. Sie sehen jetzt den Schlüssel auf der Seite „Multifaktor-Authentifizierung“.

Multifaktor-Authentifizierung mit Single Sign-on

Konfigurieren Sie die Multifaktor-Authentifizierung (MFA) mit einem SSO-Anbieter (Single Sign-on) für Ihre ServiceNow -Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Da sich viele Benutzer in Ihrer Organisation bei Ihrem Unternehmensnetzwerk anmelden und auf Ihre ServiceNow -Instanz zugreifen, besteht ein höherer Bedarf an einer sicheren Authentifizierung.

MFA in Kombination mit SSO bietet eine erhöhte Sicherheit für Ihre Instanz. Diese Funktion bietet die Flexibilität, MFA für Benutzer bedingt zu aktivieren.

Hinweis:

- ServiceNow MFA wird erzwungen, nachdem der Benutzer nach der erfolgreichen Authentifizierung beim Identitätsanbieter umgeleitet wurde.
- MFA wurde vor dem San Diego-Release nicht mit SSO erzwungen.

Wenn Sie beispielsweise externen Benutzern ein zusätzliches Sicherheitsprotokoll zur Verfügung stellen möchten, können Sie MFA nur für diese Benutzer erzwingen. Auf diese Weise können Sie zusätzliche Authentifizierungsfunktionen hinzufügen und Ihren Benutzerzugriff steuern.

Für die SSO-basierte Anmeldung wie SAML, OpenID Connect und Digest können Sie MFA für die Authentifizierung erzwingen.

MFA mit SSO kann bei Bedarf basierend auf Ihren Anforderungen konfiguriert werden. Mithilfe von Authentifizierungsschemata und Identitätsanbietern können Sie MFA für bestimmte Benutzer mit einem bestimmten Anmeldemechanismus erzwingen.

Sie können MFA für die folgenden Bedingungen erzwingen:

- Authentifizierungsschema
- Identitätsanbieter

MFA mit SSO wird als Teil des Plugins „Adaptive Authentifizierung“ (com.snc.adaptive_authentication) angeboten. Weitere Informationen zum Einrichten der adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

Konfigurieren Sie MFA mit SSO

Erzwingen Sie MFA mit SSO für Ihre Benutzer innerhalb oder außerhalb Ihrer Organisation.

Vorbereitungen
Die MFA mit SSO-Funktion wird als Teil des Plugins „Adaptive Authentifizierung“ (com.snc.adaptive_authentication) angeboten. Sie müssen die Eigenschaft „Adaptive Authentifizierung“ für die Verwendung von MFA mit der SSO-Funktion aktivieren. Weitere Informationen zum Einrichten der adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

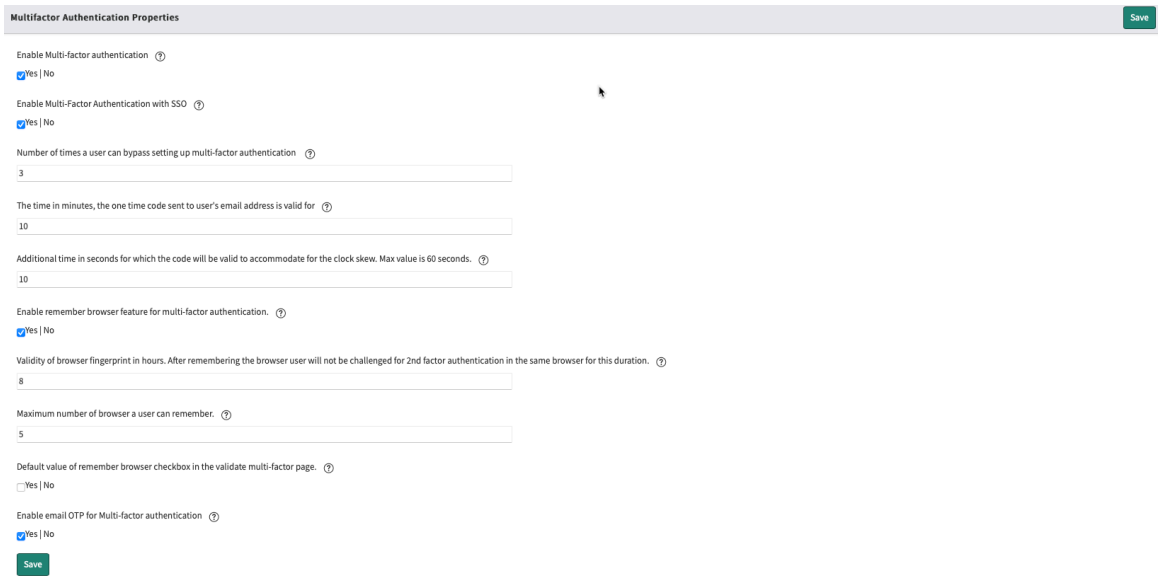
Hinweis:
MFA mit SSO-Anmeldung ist verfügbar, wenn die Eigenschaft `glide.authenticate.mfa.with.multisso.enabled` auf **true**festgelegt ist.

Erforderliche Rolle: admin

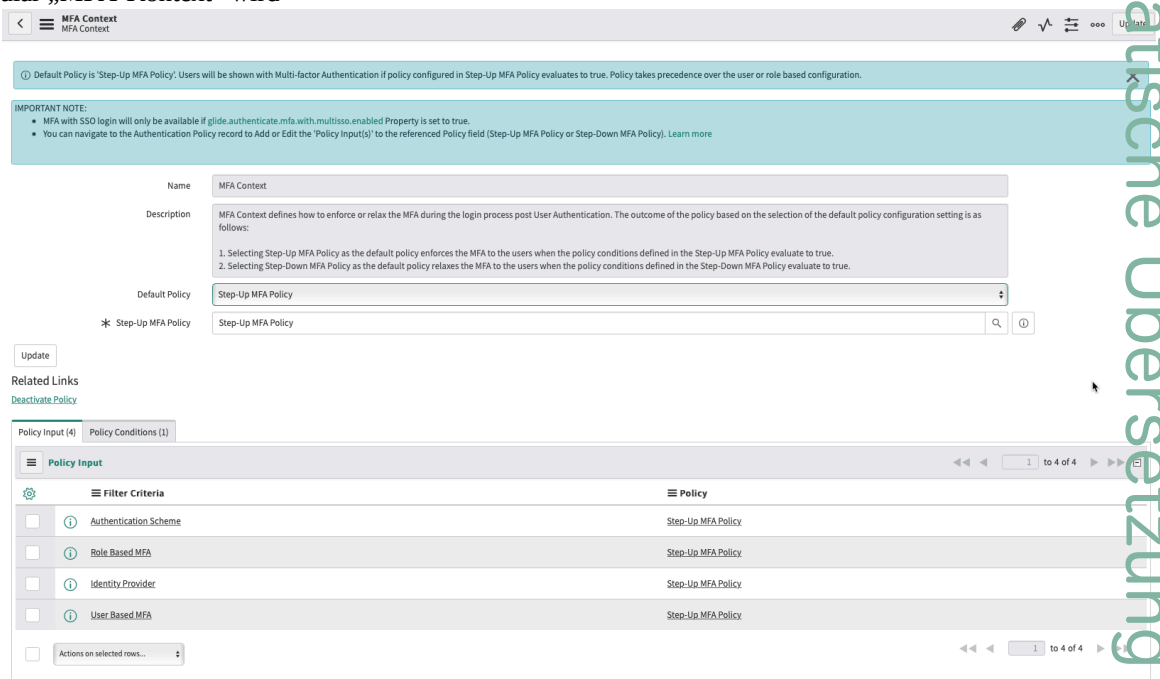
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Eigenschaften**.
2. Aktivieren Sie die Kontrollkästchen **Multifaktor-Authentifizierung** aktivieren und **Multifaktor-Authentifizierung mit SSO** aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Multi-Faktor-Authentifizierung** > **MFA-Kontext**.
   Das Formular „MFA-Kontext“ wird



angezeigt.

> **Hinweis:**
> Standardmäßig lautet die Richtlinie **Step-Up-MFA-Richtlinie**. Benutzer werden mit Multifaktor-Authentifizierung angezeigt, wenn eine in der **Step-Up-MFA-Richtlinie** konfigurierte Bedingung als „ **true**“ ausgewertet wird. Die Richtlinie hat Vorrang vor der anwender- oder rollenbasierten Konfiguration.

5. **Wahlweise:** Um eine Richtlinie zu bearbeiten, kehren Sie zum Datensatz der Authentifizierungsrichtlinie zurück, ändern die Bedingungen und kehren zurück.
   Wenn Sie zum Datensatz „Authentifizierungsrichtlinie“ navigieren, können Sie die Richtlinieneingaben in den referenzierten Richtlinienfeldern, **Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie**, hinzufügen oder bearbeiten.
6. Um eine neue Richtlinienbedingung festzulegen, klicken Sie auf **Richtlinienbedingungen**.

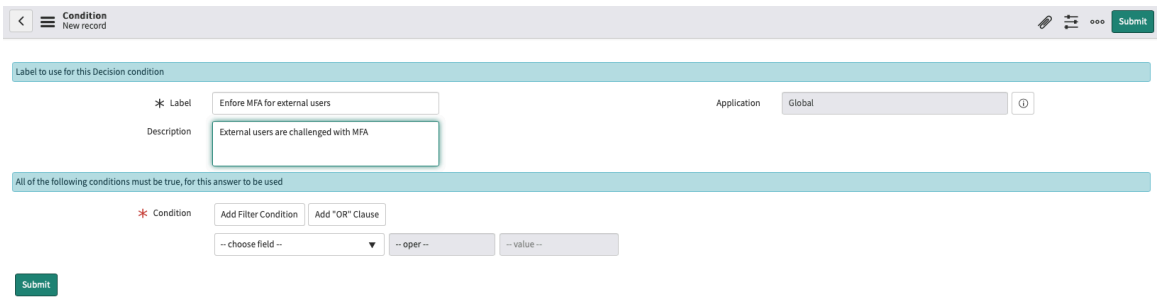
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Neu**.
8. Füllen Sie die Felder des Formulars aus.

Formular „Bedingungen“

Felder	Beschreibung
Bezeichnung	Eindeutiger Name für die Bedingung, die Sie für die Bezeichnung erstellen möchten.
Beschreibung	Beschreibung der Richtlinienbedingung.
Bedingungen	Typ der Bedingung, die Sie für die Richtlinie anwenden möchten. Sie können Filterbedingungen und „ODER“-Klauseln hinzufügen. **Hinweis:** Durch das Hinzufügen verschiedener Filterbedingungen und -klauseln können Sie MFA für bestimmte Benutzer anfordern.



Example

Betrachten Sie das folgende Beispiel, um Ihre Bedingungen einzurichten. Angenommen, Sie möchten das Authentifizierungsschema mit dem Identitätsanbieter als Bedingung für externe Benutzer festlegen. Sie können die Bedingungen wie folgt festlegen:

a. Wählen Sie **Authentifizierungsschema** aus, und legen Sie die Kriterien auf **Single Sign-on** oder **Benutzername und Passwort**fest.

   Basierend auf dieser Auswahl erhält der Benutzer eine SSO-basierte Anmeldung oder ein Anmeldeformular, um den Benutzernamen und das Passwort anzugeben.

b. Wählen Sie **Identitätsanbieter** aus, und geben Sie den Anbieter als IDP-Datensatz an, für den Sie MFA aktivieren möchten. Beispiel: **Okta**.

Basierend auf dieser Auswahl wird der Benutzer, wenn er sich mit SSO anmeldet, nicht mit MFA abgefragt. Wenn sich der Benutzer hingegen mit Oktaanmeldet, wird er mit MFA abgefragt.

9. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Adaptive Authentifizierung

Aktivieren Sie das MFA-Plugin

Multifaktor-Authentifizierung mit Single Sign-on

Single Sign-on (SSO) für mehrere Anbieter

Mit dem externen SSO können Organisationen mehrere SSO-Identitätsanbieter (IdPs) verwenden, um die Authentifizierung zu verwalten und die lokale Datenbankauthentifizierung (Standard) beizubehalten.

Die Integration unterstützt eine beliebige Kombination von lokalen und externen Authentifizierungsmethoden in einer einzelnen Instanz:

- SAML 2.0
- Digest-Authentifizierung
- OpenID Connect

Sie müssen mehrere Schritte ausführen, um Multi-Provider-SSO einzurichten, einschließlich der Konfiguration von Eigenschaften, der Erstellung von Identitätsanbietern (IdPs) und der Konfiguration von Benutzern für die Verwendung von SSO.

Beispielsweise kann ein global verteiltes Unternehmen einen SSO-Provider für seine Mitarbeiter, einen anderen für seine Lieferanten und eine lokale Datenbankauthentifizierung für seine Administratoren benötigen. Alternativ kann ein Unternehmen SAML 2.0 und eine Digest-Token-Authentifizierungslösung in derselben Instanz implementieren.

SSO-Eigenschaften, -Tabellen und -Skripts für mehrere Anbieter

Das Plugin „Integration – Single Sign-on Installer für mehrere Anbieter“ enthält die folgenden Systemeigenschaften, Tabellen und Skripts.

Eigenschaften

Mehrfachanbieter-SSO fügt die folgenden Systemeigenschaften hinzu.

SSO-Eigenschaften für mehrere Anbieter

Name	Beschreibung
`glide.authenticate.multisso.debug`	Aktiviert (true) oder deaktiviert (false) die Debug-Protokollierung für die Multi-Provider-SSO-Integration. • Typ: Wahr | Falsch • Standardwert: falsch
`glide.authenticate.multisso.enabled`	Aktiviert (true) oder deaktiviert (false) Mehrfachanbieter-SSO. • Typ: Wahr | Falsch • Standardwert: falsch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSO-Eigenschaften für mehrere Anbieter (Fortsetzung)

Name	Beschreibung
	Hinweis: Wenn diese Eigenschaft auf „false“ festgelegt wird, wird Mehrfachanbieter-SSO nicht deaktiviert, wenn Account Recovery (ACR) auch für die Instanz aktiviert ist. Um sich mit einem Benutzernamen und einem Passwort anzumelden, muss ACR auch mit der Eigenschaft `glide.sso.acr.enabled` deaktiviert werden. Einzelheiten zu dieser Eigenschaft finden Sie unter Eigenschaften der Accountwiederherstellung.
`glide.authenticate.multissov2_feature.enabled`	Diese Eigenschaft bestimmt, ob die MultiSSOv2-Version in der Instanz aktiviert ist.

Tabellen

Mehrfachanbieter-SSO fügt die folgenden Tabellen hinzu.

Multi-Provider-SSO-Tabellen

Name	Beschreibung
SSO-Eigenschaften [sso_properties]	Speichert Daten für jeden IdP, jedes Schema, allgemeine SSO-Daten usw.
SAML 2 Update 1-Eigenschaften [saml2_update1_properties]	Speichert Daten für SAML 2.0 Update 1-Konfigurationen wie SAML-Zertifikate
Digest-Eigenschaften [digest_properties]	Speichert Daten für Digest-Token-Authentifizierungskonfigurationen
SSO-Verbund [sso_federation]	Speichert Daten für jeden SSO-Verband.
OIDC-Identitätsanbieter [oidc_identity_provider]	Speichert Daten für auf Open ID Connect basierende Identitätsanbieter.

Skripts

Mehrfachanbieter-SSO fügt die folgenden Skripts hinzu.

Multi-Provider-SSO-Skripts

Name	Beschreibung
MultiSSO	Ermöglicht einem Kunden, einen SSO-Typ auf Unternehmensbasis zu definieren.
MultiSSOLogin	Ermöglicht jeder Domäne ein eigenes Anmeldeskript.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Provider-SSO-Skripts (Fortsetzung)

Name	Beschreibung
MultiSSOLogout	Ermöglicht jeder Domäne ein eigenes Abmeldeskript.
MultiSSO_OIDC_custom	Ermöglicht einem Anwender, ein benutzerdefiniertes Single Sign-on-Skript für die OIDC-Verbindung zu definieren.
MultiSSO_OIDC_logout_custom	Ermöglicht einem Anwender, ein benutzerdefiniertes Abmeldeskript für die OIDC-Verbindung zu definieren.
MultiSSO_Abstract_Core	Stellt eine Basisklasse für alle Mehrfachanbieter-SSO-Klassen bereit.
MultiSSO_ClientHelper	Stellt Funktionen eines vom Client aufrufbaren Dienstprogramms für Mehrfachanbieter-SSO bereit.
MultiSSO_VerdautToken	Stellt eine Basissystemlogik für die Authentifizierung mit Digest-Token bereit.
MultiSSO_SAML2_Update1	Stellt Logik zur Verarbeitung der SAML 2.0 Update 1-Authentifizierung für ein Single Sign-on für mehrere Mandanten bereit.

Aktivieren Sie das Multi-Provider-SSO-Plugin

Diese Integration erfordert das Plugin „Integration – Multiple Provider Single Sign-On Installer“ (com.snc.integration.sso.multi.installer).

Vorbereitungen

Erforderliche Rolle: admin.

Das Plugin „com.snc.integration.sso.multi.installer“ kann auch für OIDC, SAML und Digest verwendet werden.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Integration – Single Sign-On Installer für mehrere Anbieter“ (com.snc.integration.sso.multi.installer).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Mehrfachanbieter-SSO-Konfigurationen

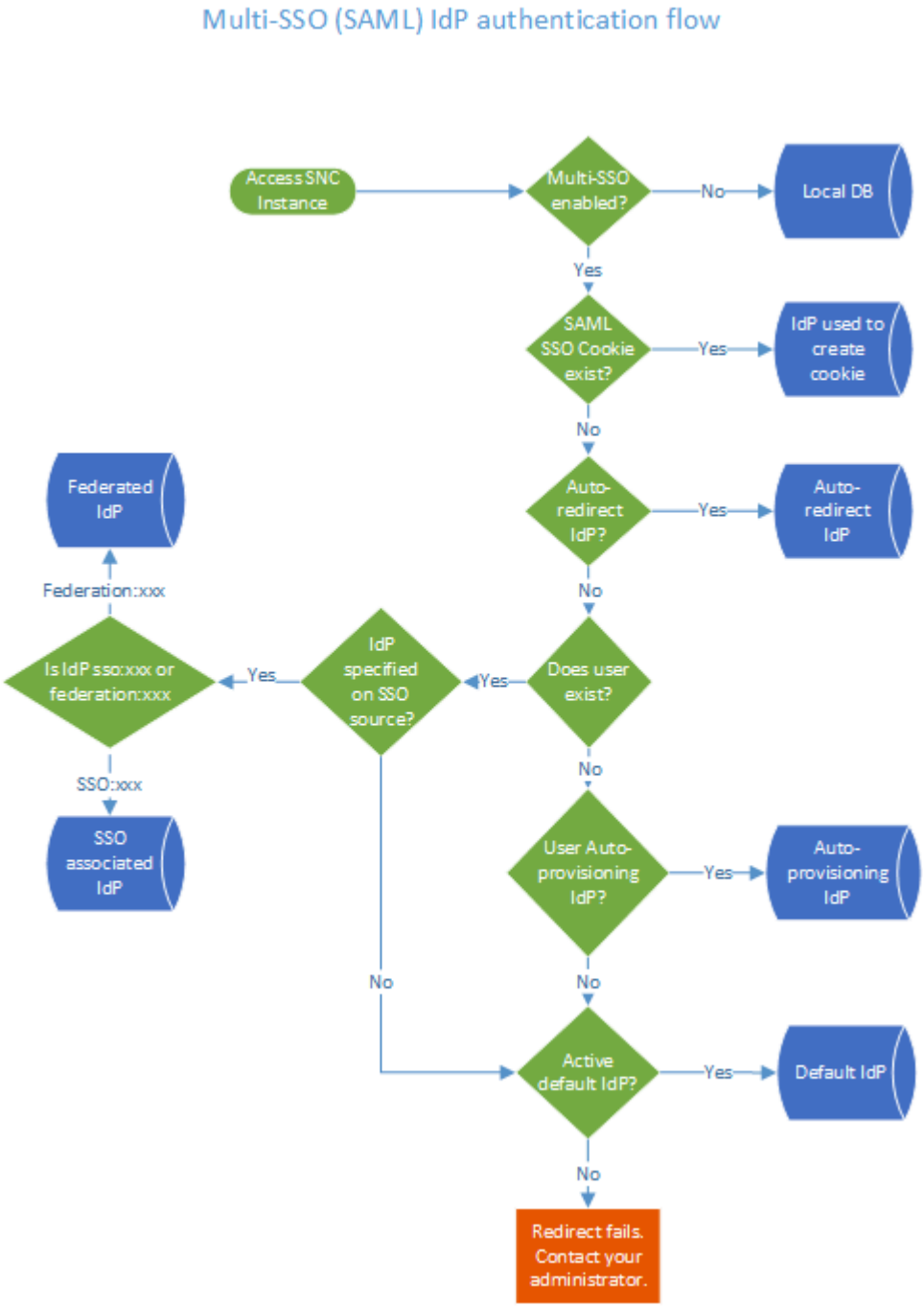
Sie müssen mehrere Schritte ausführen, um Multi-Provider-SSO einzurichten, einschließlich der Konfiguration von Eigenschaften, der Erstellung von Identitätsanbietern (IdPs) und der Konfiguration von Benutzern für die Verwendung von SSO.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IdP-Authentifizierungs-Flow mit Mehrfachanbieter-SSO (SAML).

Beschreibt die verschiedenen Entitäten, die einen Benutzer über das SAML-Multi-SSO authentifizieren können.

Sie können dem Authentifizierungs-Flow folgen, um zu verstehen, wann eine Entität einen Benutzer mit Multi-SSO authentifiziert.



Lokale Datenbank

Wenn Multi-SSO nicht aktiviert ist, wird die Authentifizierung an eine lokale DB weitergeleitet.

SAML-SSO-Cookie-IdP

Wenn ein SAML-SSO-Cookie vorhanden ist, authentifiziert der mit diesem Cookie angegebene IdP den Benutzer.

IdP mit automatischer Umleitung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der IdP für die automatische Umleitung aktiviert ist, authentifiziert dieser IdP den Benutzer.

Föderierter IdP

Wenn der Benutzerbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer in der Benutzertabelle mit dem im **SSO-Quellenfeld** als Verbund festgelegten IdP vorhanden ist: xxx, authentifiziert der verbundene IdP den Benutzer.

Zugeordneter IdP

Wenn der Benutzerbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer in der Benutzertabelle mit dem IdP im Feld **SSO-Quelle** als sso: xxx vorhanden ist, authentifiziert der zugeordnete IdP den Benutzer.

Auto-Bereitstellungs-IdP

Wenn der Benutzerbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer in der Benutzertabelle nicht vorhanden ist, die automatische Bereitstellung jedoch aktiviert ist, authentifiziert der IdP der automatischen Bereitstellung den Benutzer.

Hinweis:
Wenn mehr als ein IdP für die automatische Bereitstellung aktiviert ist, kann der Benutzer den IdP für die automatische Bereitstellung auswählen, den er verwenden kann.

Standard-IdP

Wenn der Benutzerbrowser zum Anmeldebildschirm der externen Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer eine der folgenden Optionen ausführt:

- Ist in der Benutzertabelle nicht vorhanden, automatische Bereitstellung ist nicht aktiviert, und es ist ein aktiver Standard-IdP vorhanden
- In der Benutzertabelle vorhanden, im Datensatz des SSO-Quellbenutzers oder -Unternehmens ist kein IdP angegeben, und es ist ein aktiver Standard-IdP vorhanden

dann authentifiziert der Standard-IdP den Benutzer.

Konfigurieren Sie Multi-Provider-SSO-Eigenschaften

Konfigurieren Sie SSO-Eigenschaften, und fügen Sie der Tabelle „Systemeigenschaften“ eine Eigenschaft hinzu, um eine IdP-Aufnahmeliste zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

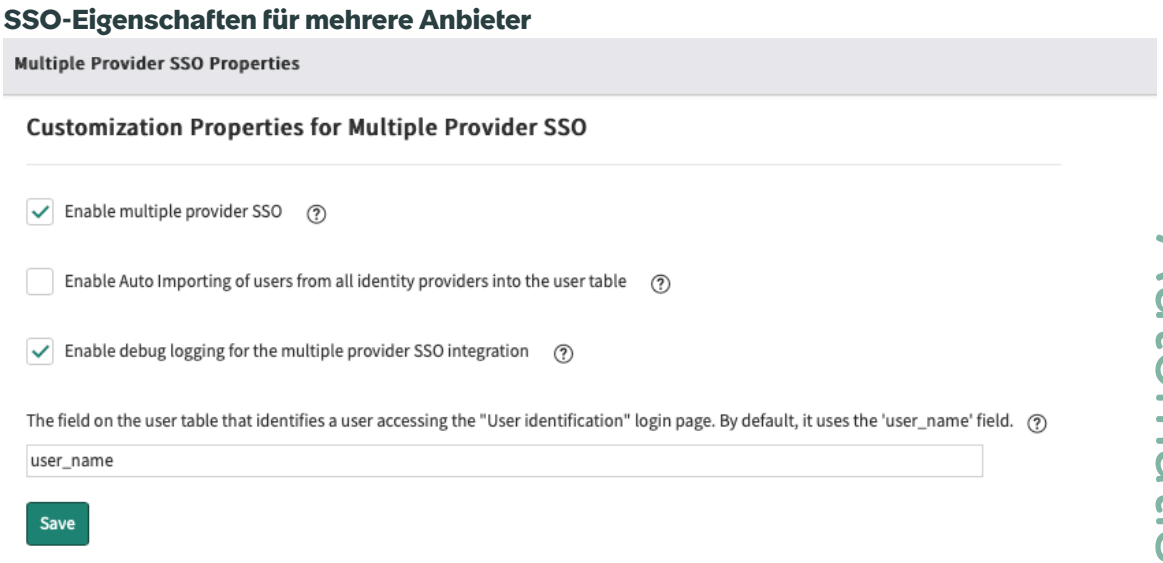
1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Administration** > **Eigenschaften**.
2. Aktivieren Sie das Kontrollkästchen **Mehrfachanbieter-SSO** aktivieren.
   Diese Auswahl fügt den Link Externe Anmeldung verwenden zur Anmeldeseite hinzu.
3. Um die Benutzertabelle mit den Benutzern im IdP zu aktualisieren, wählen Sie die Option **Enable Auto Importing** (Automatischen Import aktivieren) aus.
   Weitere Informationen zum Aktualisieren der Benutzertabelle finden Sie unter SAML-Benutzerbereitstellung verwalten.
4. Um zu aktivieren, dass die Debug-Meldungen am unteren Rand des Content Frame angezeigt werden, aktivieren Sie das Kontrollkästchen **Debug-Protokollierung für SSO-Integration mit mehreren Anbietern** aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Kontrollkästchen aktiviert ist, verlangsamt die Debug-Protokollierungsfunktion die Leistung und verbraucht Speicherplatz zum Generieren von Protokollen.

5. Geben Sie in der Eigenschaft **Das Feld in der Benutzertabelle, das einen Benutzer identifiziert, der auf die Anmeldeseite zur Benutzeridentifizierung zugreift**, das Feld in der Benutzertabelle ein, das den Wert enthält, den der IdP zum Identifizieren des Benutzers verwendet.

   Der Standardwert ist **user_name**.



6. Klicken Sie auf **Speichern**.
7. Weisen Sie Ihre Benutzer an, auf den Link **Externe Anmeldung verwenden** zu klicken, wenn sie sich bei der Instanz anmelden.

Zugehörige Informationen

SAML-Benutzerbereitstellung

Erstellen Sie einen externen Identitätsanbieter

Nachdem Sie die Multi-Provider-SSO-Eigenschaften konfiguriert haben, können Sie den Identitätsanbieter für SAML 2.0 oder Digest-Token aktualisieren oder neu erstellen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Um einen Identitätsanbieter-Datensatz zu bearbeiten, klicken Sie auf den Datensatz.
   - Aktualisieren Sie für Digest-Token-Konfigurationen die Eigenschaften manuell.
   - Aktualisieren Sie für **SAML2** Update 1-Konfigurationen die Metadaten des Identitätsanbieters automatisch mit dem zugehörigen Link Metadaten des Identitätsanbieters importieren, oder aktualisieren Sie die Eigenschaften manuell.
   - Aktualisieren Sie für OpenID Connect-Konfigurationen die Eigenschaften manuell.
3. Um einen neuen Identitätsanbieter zu erstellen, klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Digest-Token-Konfigurationen: Klicken Sie auf **Digest SSO**, und geben Sie die Digest-Eigenschaften für Single Sign-on mit mehreren Anbietern ein.
- Für SAML2-Konfigurationen: Klicken Sie **auf MultiSSOV2_SAML2_custom**, und importieren Sie die Identitätsanbieter-Metadaten von einer URL oder als XML, oder geben Sie die Identitätsanbieter-Informationen manuell ein.

- Für OpenID Connect: Klicken Sie auf **OpenID Connect**, und geben Sie die Client-ID, den geheimen Clientschlüssel und die bekannte Konfigurations-URL ein.

4. Um den IdP als Failover-IdP festzulegen, der verwendet wird, wenn der Standard-IdP nicht verfügbar ist, aktivieren Sie das Kontrollkästchen **Standard**.

   Wenn SAML 2 Update 1 aktiv ist und Sie ein Upgrade auf das Fuji-Release durchführen, wird der IdP von SAML 2 Update 1 als Standard-Failover ausgewählt. Für neue Instanzen oder wenn Sie ein Upgrade von einem Release durchführen, auf dem SAML 2 Update 1 nicht aktiv ist, wird kein standardmäßiger Failover-IdP ausgewählt.

   Hinweis:
   Der Metadatenimportprozess erstellt automatisch einen Zertifikatdatensatz für den Identitätsanbieter. Navigieren Sie zum Modul **x509-Zertifikat**, um das Zertifikat anzuzeigen.

   Hinweis:
   Zertifikate für Single Sign-on müssen immer im PEM-Format vorliegen, damit sie mit SAML-Zertifikaten funktionieren.

5. Wenn E-Signatur aktiv ist, konfigurieren Sie das Identitätsanbieterformular, und fügen Sie das Feld **Assertion Consumer URL for eSignature Authentication hinzu**.
   In den meisten Fällen lautet diese URL: `https://YOURINSTANCE.service-now.com/consumer.do`. Wenn Sie jedoch eine benutzerdefinierte Methode zur Verarbeitung der SAML-Authentifizierung für E-Signatur verwenden, können Sie Ihre eigene Verbraucher-URL einrichten. Wenn Sie nur SAML 2.0 Update 1 und kein Single Sign-on für mehrere Anbieter verwenden, konfigurieren Sie die Assertion-Verbraucher-URL mit den E-Signatur-SAML-Eigenschaften.

Generieren von Metadaten des Instanzserviceanbieters (SP) für SAML

Als Teil Ihrer SSO-Konfiguration können Sie die SP-Metadaten der Instanz generieren, um sie dem IdP bereitzustellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der IdP benötigt die Instanz-SP-Metadaten, um Anforderungen zu authentifizieren und weiterzuleiten.

Prozedur

1. Wählen Sie Ihr installiertes SSO-Plugin aus:

Option	Bezeichnung
Mehrfachanbieter-SSO	Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**. Wählen Sie einen IdP aus, und klicken Sie auf die Schaltfläche **Metadaten generieren**. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschafteneinstellungen.
SAML 2-SSO	Navigieren zu **SAML 2 Single Sign-on** > **Metadaten**. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschafteneinstellungen.

2. Kopieren Sie die SP-Metadaten in das Textfeld.

   Beispiel:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Stellen Sie die SP-Metadaten der Instanz für den IdP bereit.
   Zum Beispiel ermöglicht SSOCircle einem Benutzer, die SP-Metadaten online bereitzustellen.

Konfigurieren Sie Benutzer für Mehrfachanbieter-SSO

Administratoren können Mehrfachanbieter-SSO für einzelne Benutzer oder für alle Benutzer konfigurieren, die zu einem Unternehmen gehören. Sie können Mehrfachanbieter-SSO nicht für Gruppen konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Klicken Sie mit der rechten Maustaste auf den Datensatz eines Identitätsanbieters und wählen Sie **sys_id kopieren**.
3. Kopieren Sie die Daten in die Zwischenablage.
4. Navigieren Sie zu einem Benutzerdatensatz oder einem Unternehmensdatensatz.
5. Konfigurieren Sie das Formular, und fügen Sie das Feld **SSO-Quelle** hinzu.
6. Geben Sie im Feld **SSO-Quelle** eine der folgenden Optionen ein:
   - **SAML-Benutzer**: **Geben Sie sso:** ein, gefolgt von der sys_id des Datensatzes des Identitätsanbieters.
   - **SSO**-Verbandbenutzer: Geben Sie **federation:** ein, gefolgt von der sys_id des Verbunddatensatzes.
7. Klicken Sie auf **Aktualisieren**.

IdP-Verbindungen werden getestet

Beim Testen der Verbindung zu einem IdP werden die Einstellungen validiert, bevor die externe Authentifizierung aktiviert wird.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Das Jakarta-Release unterstützt die Testverbindung in einem Popup-Fenster. Wenn Ihr IdP mit dieser Option nicht ordnungsgemäß funktioniert, können Sie diese Standardeinstellung deaktivieren.
Die MultiSSO-IDP-Metadaten aktualisieren-Aufgabe ruft das Zertifikat für den IdP ab und aktualisiert es, während die Verbindung erstellt, aktualisiert oder getestet wird.

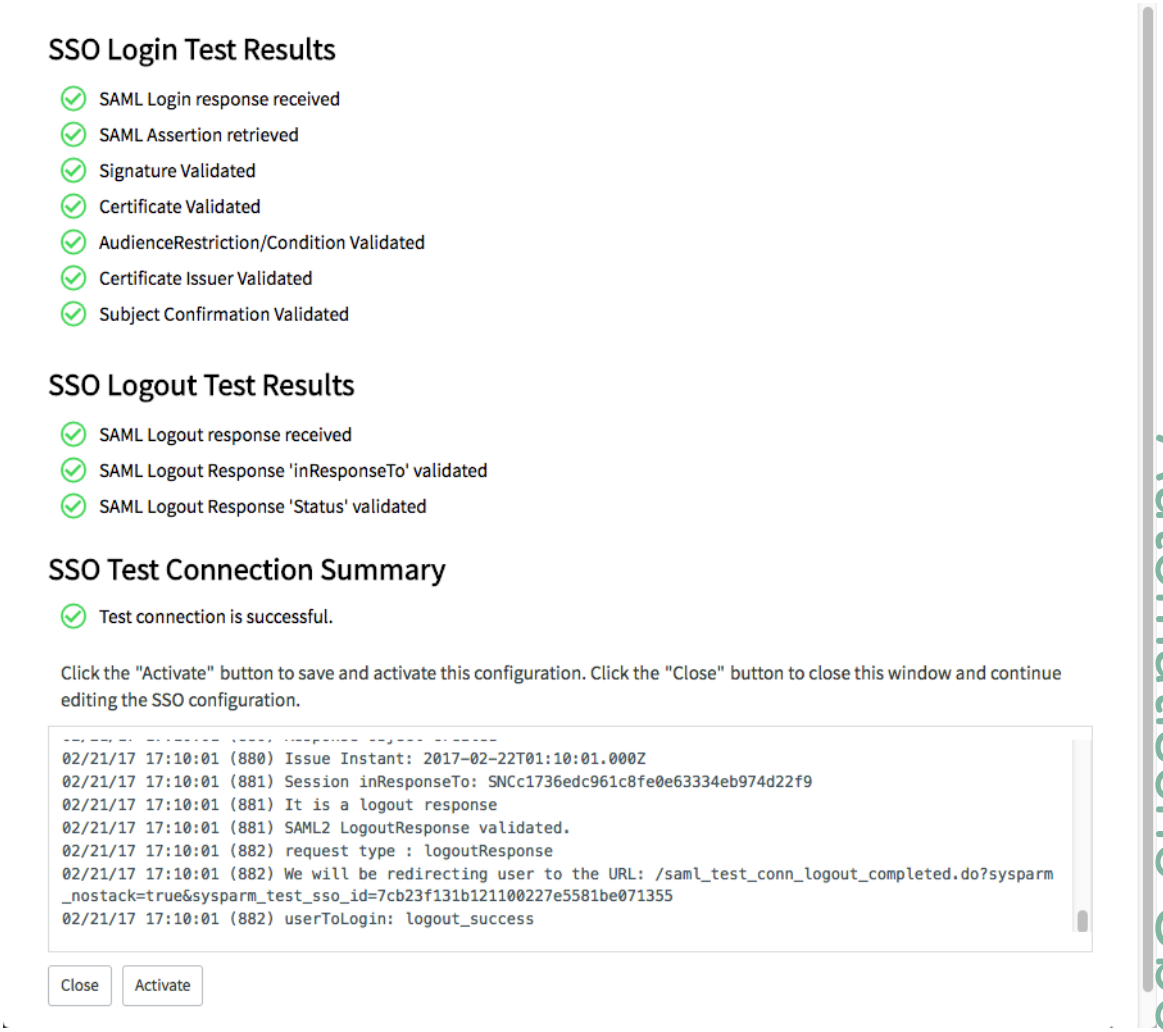
Hinweis:
In einigen IdP-Fällen muss, wenn die Testverbindung fehlschlägt, „glide.authenticate.multisso.test.connection.mandatory“ mit dem Wert „false“ erstellt werden, und Sie können den IdP ohne die Testverbindung aktivieren.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Wählen Sie einen definierten IdP aus, oder klicken Sie auf **Neu**, um einen neuen IdP zu definieren.
3. **Wahlweise:** Konfigurieren Sie einen Identitätsanbieter, wenn Sie einen neuen IdP einrichten.
4. Klicken Sie auf **Verbindung testen**, geben Sie die Anmeldeinformationen für den IdP ein, um die Anmeldung zu überprüfen.
   Sie können den IdP erst aktivieren, wenn eine erfolgreiche Testverbindung hergestellt wurde. Wenn der Test fehlschlägt, können Sie aktualisieren, um Ihre Konfigurationsinformationen zu speichern, aber Sie können diese Konfiguration nicht aktivieren.
5. Überprüfen Sie die Ergebnisse mithilfe der **SSO-Testergebnisse/Zusammenfassung** oder des Abschnitts „ **SSO-Protokolle** testen“, um Protokollnachrichten anzuzeigen.
   Wenn Fehler auftreten, lesen Sie die Multi-SSO (SAML 2.0) – Fehler und Korrekturen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Abbrechen**, wenn der Test abgeschlossen ist.



Allgemeine IdP-Verbindungsfehler

In der folgenden Tabelle werden einige der häufigsten IdP-Verbindungsfehler und ihre Lösungen beschrieben.

Problembehandlung bei IdP-Testverbindungen

Fehlermeldungen	Lösung
Fehler bei der Validierung des Anwenderfelds. Ungültiges Anwenderfeld '<field name> „“ ist kein Feld in der Tabelle „sys_user“.	Vergewissern Sie sich, dass der Inhalt des von Ihnen ausgewählten Felds Benutzertabelle mit dem SAML-NameID-Token übereinstimmt.
Der Aussteller der Assertion ist ungültig.	Vergewissern Sie sich, dass die **Identitätsanbieter-URL** eine gültige URL zu Ihrem IdP enthält. Jede IdP-URL muss eindeutig sein.
AudienceRestriction-Validierung fehlgeschlagen.	Vergewissern Sie sich, dass der **Zielgruppen-URI** eine gültige URL zu Ihrer Instanz enthält.
Abmelden von IdP-Sitzung nicht möglich.	Vergewissern Sie sich, dass die **SingleLogoutRequest** -URL eine gültige URL zum Abmeldeservice Ihres IdP enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung bei IdP-Testverbindungen (Fortsetzung)

Fehlermeldungen	Lösung
Signatur wurde nicht anhand des Schlüssels der Anmeldeinformationen validiert.	Vergewissern Sie sich, dass für den IdP ein gültiges Zertifikat installiert ist.

Multi-SSO (SAML 2.0) – Fehler und Korrekturen

Eine Liste der häufigsten Fehler und zugehörigen Korrekturen für das Setup und die Konfiguration von Multi-SSO (SAML 2.0).

Fehler beim Setup von Multi-SSO (SAML 2.0).

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
NotAfter:<Thu Jun 05 22:57:44 PDT 2014> .	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist.	N/V	Das aktuelle Zertifikat oder die SAML-Assertion ist abgelaufen.	• Synchronisieren Sie die SNC-Uhr mit der SAML-IdP-Serveruhr. • Aktualisieren Sie den SAML 2.0-Zertifikatdatensatz.
• SAML 2.0-Zertifikat wurde nicht gefunden. • In der ServiceNow-Instanz gespeicherte digitale Signatur wurde nicht gefunden.	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist	Die PEM-formatierte Zeichenfolge muss in das Feld PEM-Zertifikat eingegeben werden.	Das SAML-Zertifikat ist nicht vorhanden. Er ist möglicherweise inaktiv.	Stellen Sie sicher, dass das richtige PEM-formatierte Zertifikat in die Instanz hochgeladen wird.
Zertifikate stimmen nicht überein. Erwartet:<certStr> , Istwert:<inboundCert> .	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist.	N/V	Das in SNC verfügbare Zertifikat stimmt nicht mit dem Zertifikat in der Assertion überein. Zu den Ursachen gehören: • Das Zertifikat wird auf dem IdP aktualisiert, aber nicht in der ServiceNow-Instanz. • Das Zertifikat weist das falsche Format auf.	Bestätigen Sie, dass die PEM-formatierte Zeichenfolge im Datensatz des SAML 2.0-Zertifikats mit dem X509-Zertifikat in der SAMLResponse für den Benutzer-IdP übereinstimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
Fehler beim Überprüfen der Gültigkeit des Zertifikats.	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist	N/V	Das aktuelle Zertifikat ist möglicherweise abgelaufen.	Aktualisieren Sie den SAML 2.0-Zertifikatdatensatz.
Fehler beim Validieren des Signaturprofils.	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist.	N/V	Die Assertion ist möglicherweise mit einem anderen Zertifikat signiert.	Überprüfen Sie, ob der IdP dasselbe Zertifikat wie die SNC-Instanz hat.
Attribut „InResponseTo“ in „SubjectConfirmationData“ stimmt nicht überein. Erwartet:<inResponseTo> , Istwert: .	Die Validierung der Antragstellerbestätigung ist fehlgeschlagen.	N/V	Dieser Fehler wird angezeigt, wenn eine der folgenden Situationen auftritt: • Der IdP gibt eine SAMLResponse für eine andere SAMLRequest zurück • Ein Benutzer setzt ein Lesezeichen für die URL mit der SAML-Anforderung anstatt nur für die Instanz-URL • Wenn ein Nullwert erwartet wird, wird die Antwort möglicherweise an einen anderen Knoten gesendet, wenn die Instanz über mehrere Knoten verfügt.	Der IdP-Administrator sollte bestätigen, dass die erwartete SAML-Antwort zurückgegeben wird. Diese Situation kann ein Problem mit dem Lastenausgleichsmodul oder der Infrastruktur sein.
SessionIndex-Wert nicht gefunden:<message> ...	SessionIndex ungültig.	N/V	Der SessionIndex ist in der SNC-Instanz erforderlich. Der IdP gibt ihn in der SAML-Antwort zurück, um eine erfolgreiche	Der IdP-Administrator sollte bestätigen, dass der SessionIndex in

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
			Authentifizierung zu bestätigen.	der SAMLResponse definiert ist.
Es konnte kein gültiges SubjectConfirmation-Element gefunden werden.	Die Validierung der Antragsteller ist fehlgeschlagen.	N/V bestätigung	Bedingungen könnten aufgrund eines Fehlers beim IdP fehlen. Der StatusCode in der Antwort würde Responder anstelle des erwarteten Erfolgs enthalten.	Überprüfen Sie SAMLResponse, um festzustellen, ob Bedingungen in der SAMLResponse enthalten sind. Die gültigen Betreffbestätigungsdaten sind möglicherweise abgelaufen oder nicht für die richtige Zielgruppe.
Nichtübereinstimmung der Assertionszielgruppe. Erwartet:<propAudienceUri> Istwert:<audienceUri> oder AudienceRestriction-Validierung fehlgeschlagen. Keine übereinstimmende Zielgruppe gefunden.	Stellen Sie sicher, dass das Feld „Zielgruppen-URI“ richtig festgelegt ist	Der Zielgruppen-URI, der das SAML2-Token akzeptiert. (Normalerweise ist dies Ihr Instanz-URI. Beispiel: https://demo.service-now.com.)	Der in der SNC-Instanz konfigurierte Zielgruppen-URI muss mit dem Wert im IdP übereinstimmen.	Suchen Sie<saml2:Audience> in der SAMLResponse in den Protokollen und stellen Sie sicher, dass der Wert mit dem in der Instanz übereinstimmt.
Der Aussteller der Assertion ist ungültig. Erwartet:<value on instance> , Istwert:<value returned by IdP>	Der Aussteller der Assertion ist ungültig.	Die Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit Benutzerinformationen ausgibt.	Die IdP-Entitäts-ID (Aussteller) stimmt nicht mit dem in der SNC-Instanz definierten Wert überein.	• Überprüfen Sie, ob IdP oder SP nicht ordnungsgemäß konfiguriert ist. • Vergewissern Sie sich, dass die SAML-Eigenschaft (die Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit Benutzerinformationen ausgibt) richtig festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
Betreff liegt gültig in der Zukunft. Jetzt:<now> , NotBefore:<notBefore> oder Betreff ist abgelaufen. Jetzt:<now> , NotOnOrAfter:<notOnOrAfter>	Die Bestätigung des Antragstellers ist fehlgeschlagen.	Die Anzahl in Sekunden vor der NotBefore-Einschränkung oder nach der NotOnOrAfter-Einschränkung, die als noch gültig betrachtet werden soll.	Die IdP-Uhr ist nicht mit der SP-Uhr synchronisiert.	Aktualisieren Sie die SAML-Eigenschaft glide.authenticate.sso.saml2.timer auf einen größeren Wert. Der Standardwert beträgt 180 Sekunden. Einige Fälle erfordern eine Einstellung von 300 oder höher. Möglicherweise müssen Sie auch die Zeit auf Ihrem IdP-Server überprüfen.
Assertion ist in der Zukunft gültig, jetzt:<now> , notBefore:<notBefore> oder Assertion ist abgelaufen, jetzt:<now> , notOnOrAfter:<notOnOrAfter>	Assertion ist ungültig.	Die Anzahl in Sekunden vor der NotBefore-Einschränkung oder nach der NotOnOrAfter-Einschränkung, die als noch gültig betrachtet werden soll.	IdP-Uhr ist nicht mit SP-Uhr synchronisiert	Aktualisieren Sie die SAML-Eigenschaft auf einen größeren Wert. Standard: 60 Sekunden. Einige Fälle erfordern eine Einstellung von 300 oder höher. Möglicherweise müssen Sie auch die Zeit auf Ihrem IdP-Server überprüfen.

Allgemeine Anmeldungs- und IdP-Fehler

Fehler oder Symptom	Diagnose	Beheben
Anmeldeanforderungen erzeugen eine Endlosschleife zwischen dem System und dem IdP, wenn hohe Sicherheit aktiv ist.	• Normalerweise ist der URL-Endpunkt eine Fehlerseite oder Abmeldeseite. • „logout_redirect.do“ kann diese Schleife erstellen, wenn Sie `glide.security.url.whitelist` definieren, ohne den IdP-Hostnamen zum	Legen Sie die Systemeigenschaft glide.authenticate.failed_redirect fest (oder erstellen Sie sie), um fehlgeschlagene Authentifizierungsanforderungen an diese URL umzuleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Anmeldungs- und IdP-Fehler (Fortsetzung)

Fehler oder Symptom	Diagnose	Beheben
	Eigenschaftswert hinzuzufügen. **Hinweis:** Weitere Informationen zu dieser Eigenschaft finden Sie unter URL-Allow-Liste für Abmeldeumleitungen in Härtungseinstellungen für Instanzsicherheit.	
Das zur Authentifizierung des Benutzers oder der Anforderung verwendete Token ist mit dem Signaturalgorithmus http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 signiert. Dies ist nicht der erwartete Signaturalgorithmus http://www.w3.org/2000/09/xmldsig#rsa-sha1.	Überprüfen Sie die Registerkarte Warnungskontext auf Event-Details.	Navigieren Sie zur Registerkarte „Erweitert“ des Konfigurationsdialogfelds „Relying Party Trust“, und stellen Sie sicher, dass der Algorithmus auf SHA-1 und nicht SHA-256 festgelegt ist.
Die Fehlermeldung urn:oasis:names:tc:SAML:2.0:status:Requester wird in der Systemprotokolltabelle (syslog) angezeigt.	Wenn Ihr IdP (z. B. ADFS) mit der Status oasis:names:tc:SAML:2.0:status:Requester antwortet, bedeutet dies, dass der IdP die Anmeldung aufgrund eines Problems mit der an ihn gesendeten Anforderung abgelehnt hat. Leider enthält die vom IdP erhaltene SAML-Antwort in den meisten Fällen keine weiteren Details für den Fehler.	Überprüfen Sie die an den IdP gesendete SAML-Anforderung, Recherchieren Sie mit Ihrem IdP-Administrator zusammen, um die SAML-Einstellungen Ihrer Instanz zu aktualisieren, um den Fehler zu vermeiden. Möglicherweise müssen Sie sich an Ihren IDP-Provider wenden, um den Grund für den Anmeldefehler zu erfahren.

Beheben Sie Skriptprobleme mit SAML

Beheben Sie Skriptprobleme mit SAML. Es können Skriptprobleme auftreten, wenn SAML zum Zeitpunkt der Aktivierung von Multiple Single Sign-on bereits aktiv ist und Sie die Installations-Exits bereits angepasst haben.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Sichern Sie den geänderten Installations-Exit SAML2SingleSgnon_update1 und die Skripteinbindung SAML2_update1.
2. Setzen Sie sowohl den Installations-Exit als auch die Skripteinbindung auf die Version zurück, die mit dem Baseline-System verfügbar ist.
3. Aktivieren oder aktualisieren Sie das Plugin **„Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter** “.
   Das System aktualisiert SAML und alle erforderlichen Dateien auf SAML 2 Update 1.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Öffnen Sie die Seite mit den Eigenschaften für mehrere SSOs, und aktivieren Sie das Kontrollkästchen **SSO für mehrere Anbieter** aktivieren, um sie zu aktivieren.
5. Fügen Sie die Änderungen am Installations-Exit von SAML2SingleSigno_update1 in die Baseline-Skripteinbindung **MultiSSO_SAML2_Update1 ein, und die** Änderungen an der Skripteinbindung SAML2_update1 in die Baseline-Skripteinbindung SAML2_update1.

Melden Sie sich mit Mehrfachanbieter-SSO an

Die empfohlene und effizienteste Methode für Benutzer, sich mit Mehrfachanbieter-SSO anzumelden, ist die Verwendung einer speziell konfigurierten URL.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Nach der Konfiguration des Mehranbieter-SSO können Sie eine URL an Ihre Benutzer mit dem richtigen IdP in der Parameterzeichenfolge senden. Beispiel:

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Nachdem sich ein Benutzer erfolgreich bei der IdP-Seite angemeldet hat, wird dem Browser ein Cookie mit der sys_id des IdP hinzugefügt. Wenn der Benutzer das nächste Mal versucht, sich anzumelden, leitet das System den Benutzer zur Anmeldung beim IdP-Server um, der sich automatisch bei der Instanz anmeldet.

Wenn ein URL-Parameter nicht festgelegt ist oder der Browsercache geleert wurde, können Benutzer auch Folgendes tun:

Prozedur

1. Klicken Sie auf der Anmeldeseite auf den Link **Externe Anmeldung verwenden**.

   Die externe Anmeldeseite wird angezeigt. Benutzer können auf **Lokale Anmeldung** verwenden klicken, um zur Standardanmeldeseite zurückzukehren.
2. Geben Sie den Wert für das angegebene Feld in der Benutzertabelle ein, die Sie in den SSO-Eigenschaften für mehrere Anbieter konfiguriert haben.

   Der Benutzer wird zum IdP-Server umgeleitet, wo er sich anmeldet.

Ergebnisse
Nachdem sich Benutzer erfolgreich bei einem IdP angemeldet haben, werden sie automatisch zu diesem IdP umgeleitet, wenn sie versuchen, auf die Instanz zuzugreifen. Damit ein Benutzer auf einen anderen IdP zugreift, senden Sie dem Benutzer eine URL mit den neuen IdP-Informationen im Parameter. Der neue IdP überschreibt den alten IdP im Cookie, wenn sich der Benutzer erfolgreich anmeldet. Wenn sich der Benutzer nicht erfolgreich anmeldet, werden die alten IdP-Informationen im Cookie beibehalten.

Ermöglichen Sie Benutzern, den Identitätsanbieter für die Anmeldung auszuwählen

Mit der Unterstützung von SSO-Vereinen können Benutzer auswählen, bei welchem IdP sie sich anmelden möchten.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

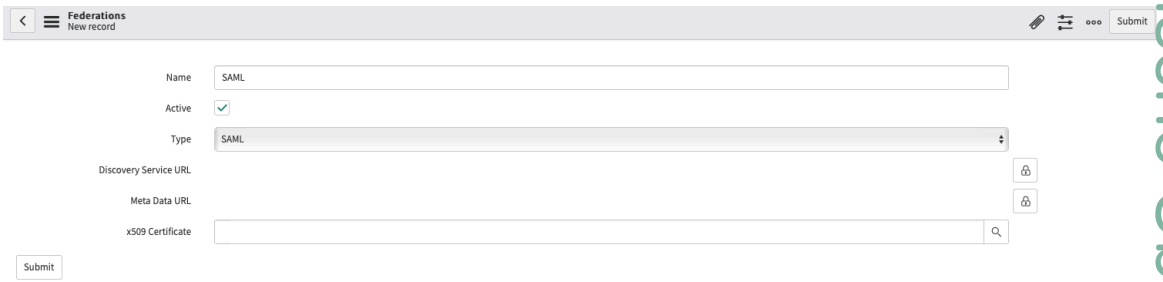
SSO-Verbünde fassen Metadaten von mehreren IdPs und Service Providern zusammen, einschließlich Ihrer Instanz. Verbünde veröffentlichen die Metadaten dann als XML-Datei, die Informationen wie IdP-Namen und IdP-Zertifikate enthält. Administratoren können dann die Instanz anweisen, die XML-Datei zu lesen und die SSO-Eigenschaftentabelle automatisch mit allen erforderlichen IdP-Informationen auszufüllen.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Verbund**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.
5. Nachdem Sie einen Verbund konfiguriert haben, aktivieren Sie die geplante Aufgabe SSO-Metadaten aktualisieren, und konfigurieren Sie dann die Benutzer, die auf die IdPs des Verbunds zugreifen sollen.

Hinweis:
Verwenden Sie die sys_ID des Verbunddatensatzes, den Sie gerade erstellt haben.

Weitere Informationen finden Sie unter IdP-Authentifizierungs-Flow mit Mehrfachanbieter-SSO (SAML).



Die Instanz füllt die SSO-Eigenschaftentabelle mit den IdP-Informationen. Wenn sich Benutzer, die für die Verwendung des Verbunds konfiguriert sind, anmelden, werden sie zu der von Ihnen konfigurierten Discovery-Service-URL umgeleitet. Anschließend wählen sie den IdP aus und geben die erforderlichen Anmeldeinformationen an. Alternativ können Sie Benutzern eine URL mit dem IdP im Parameter senden.

Zulassen, dass Benutzer den Identitätsanbieter für die Anmeldung auswählen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für den Verbund ein.
Aktiv	Aktivieren Sie die Checkbox, damit die Instanz die XML-Datei aus dem Verbund abrufen kann.
Typ	Wählen Sie die Art der Authentifizierung aus, die dieser Verbund unterstützt.
Discovery Service-URL	Geben Sie die URL des Discovery-Service für diesen Verbund ein. Dies ist die Site, auf der Benutzer aufgefordert werden, einen IdP auszuwählen und sich anzumelden.
Metadaten-URL	Geben Sie die URL der XML-Datei ein, die die Verbundmetadaten enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
x509-Zertifikat	Wählen Sie das Verbundzertifikat aus.
Domäne	Wählen Sie die Domäne aus, zu der die Daten gehören sollen.

Hinweis:
Der IdP für die föderierte Identitätsverwaltung von InCommon ist vorkonfiguriert.

Verwenden Sie Serviceportal mit Mehrfachanbieter-SSO, um eine URL umzuleiten

Serviceportal Verwendet eine Kombination aus Systemeigenschaften und Skripteinbindungen, um zu bestimmen, wie das System URL-Weiterleitungen für Benutzer vornimmt, die sich beim Portal anmelden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie die Systemeigenschaft für die automatische Umleitung zu Ihrem primären Identitätsanbieter (IdP) verwenden, leitet Serviceportal automatisch zu diesem IdP um. Wenn Sie mehrere IdPs haben, zeigt Serviceportal auf der Anmeldeseite einen Link zu **Externe Anmeldung verwenden**an.

Prozedur

1. Service Portal-Anmeldeseite konfigurieren
2. Nach der Anmeldung zum Service Portal weiterleiten

Kontowiederherstellung (ACR)

Administratoren können die Accountwiederherstellung (ACR) konfigurieren, um Wiederherstellungsaktivitäten durchzuführen, z. B. um SSO-Fehlkonfigurationen oder abgelaufene Zertifikate zu beheben.

Hinweis:
Durch Aktivieren von ACR werden die lokalen interaktiven Anmeldungen (basierend auf Benutzername oder Passwort) deaktiviert, wenn SSO für Ihre Instanzen aktiviert ist.

ACR bietet die folgenden Funktionen:

- Umgehen Sie als Administrator Ihre SSO-Anmeldung (Single Sign-on), um Probleme mit der SSO-Konfiguration zu beheben.
- Melden Sie sich mit SSO bei an, um Aufgaben mit einem Administratorkonto auszuführen, das als Kontowiederherstellung konfiguriert ist.
- Mit ACR-Flows können Administratoren Selfservicefunktionen verwenden, um die Kontowiederherstellung zu übernehmen, wenn eine Wiederherstellung erforderlich ist, z. B. bei SSO-Fehlkonfigurationen oder abgelaufenen Zertifikaten.
- Reduzieren Sie den nicht autorisierten Zugriff auf die Instanz, und bieten Sie eine solide Grundlage für die Verwendung von ACR außerhalb von SSO-Anwendungsfällen.

Neue Instanz

Damit eine neue Instanz ACR verwenden kann, müssen Sie folgende Schritte durchführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mutli-SSO-Plugin (com.snc.integration.sso.multi.installer) aktivieren
- ACR aktivieren (glide.sso.acr.enabled): Ist bei einer neuen Instanz standardmäßig aktiviert.
- Vor dem Aktivieren der SSO-Eigenschaft (glide.authenticate.multisso.enabled) muss sich der Administrator als ACR-Benutzer registrieren.

Hinweis:
Wenn diese Eigenschaft auf „false“ festgelegt wird, wird Mehrfachanbieter-SSO nicht deaktiviert, wenn Account Recovery (ACR) auch für die Instanz aktiviert ist. Um sich mit einem Benutzernamen und einem Passwort anzumelden, muss ACR auch mit der Eigenschaft `glide.sso.acr.enabled` deaktiviert werden. Einzelheiten zu dieser Eigenschaft finden Sie unter Eigenschaften der Accountwiederherstellung.

- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Benutzer registriert.

Aktualisierte Instanz

Damit eine aktualisierte Instanz ACR verwenden kann, müssen Sie folgende Schritte durchführen:

- Mutli-SSO-Plugin (com.snc.integration.sso.multi.installer) aktivieren
- ACR aktivieren (glide.sso.acr.enabled)

Hinweis:
Im Falle einer aktualisierten Instanz muss der Administrator ACR aktivieren.

- Vor dem Aktivieren der SSO-Eigenschaft (glide.authenticate.multisso.enabled) muss sich der Administrator als ACR-Benutzer registrieren.
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Benutzer registriert.

Konfigurieren Sie Benutzer für die Accountwiederherstellung

Um die Accountwiederherstellung zu verwenden, müssen Sie mindestens einen Administratoraccount als Accountwiederherstellungsbenutzer registrieren. Single Sign-on kann in Ihrer Instanz erst aktiviert werden, wenn mindestens ein Konto konfiguriert ist. Details zu diesem Vorgang finden Sie unter Konfigurieren Sie auf der Seite „Eigenschaften der Accountwiederherstellung“ einen Benutzer für die Accountwiederherstellung.

Hinweis:
Wenn Sie eine Instanz aktualisieren, die bereits Single Sign-on auf Rome oder einen späteren Release verwendet, funktioniert Single Sign-on weiterhin, ohne dass ein Wiederherstellungsbenutzer konfiguriert ist.

Konfiguration der Accountwiederherstellung

Die Funktion zur Kontowiederherstellung ist in den **Plugins „Integration – Multiple Provider Single Sign-On Installer“ (com.snc.integration.sso.multi.installer) enthalten**. Die Funktion ist standardmäßig aktiviert. Sie können diese und andere Einstellungen für die Accountwiederherstellung mithilfe der Systemeigenschaften ändern. Weitere Informationen zu diesen Eigenschaften finden Sie unter Eigenschaften der Accountwiederherstellung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontext der Accountwiederherstellungsrichtlinie

Nachdem Sie einen Benutzer für die Kontowiederherstellung registriert und Single Sign-on (SSO) aktiviert haben, schränkt Ihre Instanz alle lokalen Anmeldungen ein. Diese Einschränkung ist im Kontext der **SSO-ACR-Kontextauthentifizierungsrichtlinie** definiert. Weitere Informationen zum Kontext finden Sie unter Account-Wiederherstellungskontext.

Weitere Informationen dazu, wie Authentifizierungsrichtlinien und Richtlinienkontexte und wie sie in Ihrer Instanz funktionieren, finden Sie unter Adaptive Authentifizierung.

Konfigurieren Sie einen Benutzer für die Accountwiederherstellung

Konfigurieren Sie einen Account-Wiederherstellungsbenutzer, um Account-Wiederherstellungsaktivitäten in Ihrer Instanz auszuführen.

Ein Benutzer für die Accountwiederherstellung ist ein Benutzeraccount, mit dem Administratoren Accountwiederherstellungsaufgaben ausführen können, z. B. die Behebung einer SSO-Fehlkonfiguration oder die Behebung abgelaufener Zertifikate.

Hinweis:
Wenn Sie die Kontowiederherstellung in Ihrer Instanz verwenden, müssen Sie einen Benutzer für die Kontowiederherstellung konfigurieren. Dieser Schritt ist erforderlich, bevor Single Sign-on mit mehreren Anbietern für eine Instanz aktiviert wird.

Konfigurieren Sie auf der Seite „Eigenschaften der Accountwiederherstellung“ einen Benutzer für die Accountwiederherstellung

Konfigurieren Sie eine Accountwiederherstellung über die Eigenschaftenseite der Accountwiederherstellung.

Vorbereitungen
Erforderliche Rolle: admin

Damit eine neue Instanz ACR konfigurieren kann, müssen Sie folgende Schritte durchführen:

- Mutli-SSO-Plugin (`com.snc.integration.sso.multi.installer`) aktivieren
- ACR aktivieren (`glide.sso.acr.enabled`): Ist bei einer neuen Instanz standardmäßig aktiviert.
- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`) muss sich der Administrator als ACR-Benutzer registrieren.
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Benutzer registriert.

Damit eine aktualisierte Instanz ACR verwenden kann, müssen Sie folgende Schritte durchführen:

- Mutli-SSO-Plugin (`com.snc.integration.sso.multi.installer`) aktivieren
- ACR aktivieren (`glide.sso.acr.enabled`)

  Hinweis:
  Im Falle einer aktualisierten Instanz muss der Administrator ACR aktivieren.

- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`) muss sich der Administrator als ACR-Benutzer registrieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn diese Eigenschaft auf „false“ festgelegt wird, wird Mehrfachanbieter-SSO nicht deaktiviert, wenn Account Recovery (ACR) auch für die Instanz aktiviert ist. Um sich mit einem Benutzernamen und einem Passwort anzumelden, muss ACR auch mit der Eigenschaft `glide.sso.acr.enabled` deaktiviert werden. Einzelheiten zu dieser Eigenschaft finden Sie unter Eigenschaften der Accountwiederherstellung.

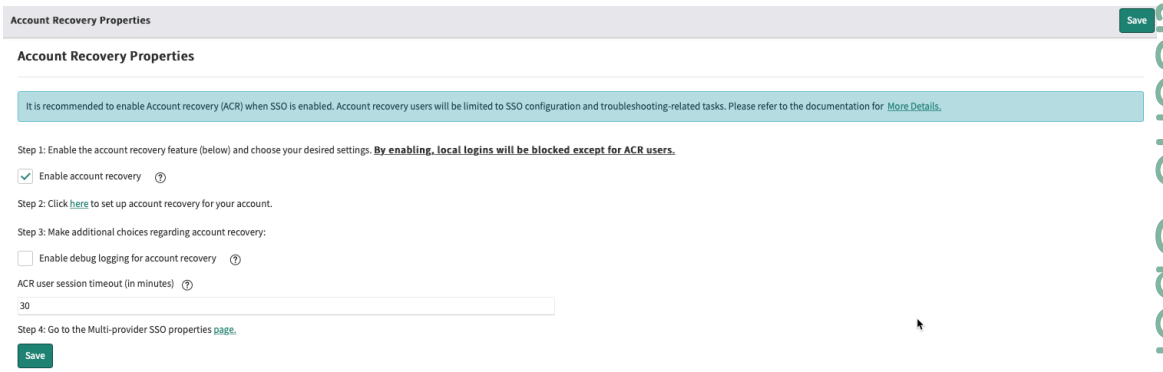
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Benutzer registriert.

Prozedur

1. Navigieren zu **Alle** > **Accountwiederherstellung** > **Eigenschaften**.
2. Klicken Sie **auf Accountwiederherstellung aktivieren**.

   Hinweis:
   Sie müssen die Accountwiederherstellung aktivieren, wenn SSO aktiviert ist. Benutzer der Accountwiederherstellung sind auf SSO-Konfigurations- und Problembehandlungsaufgaben beschränkt.

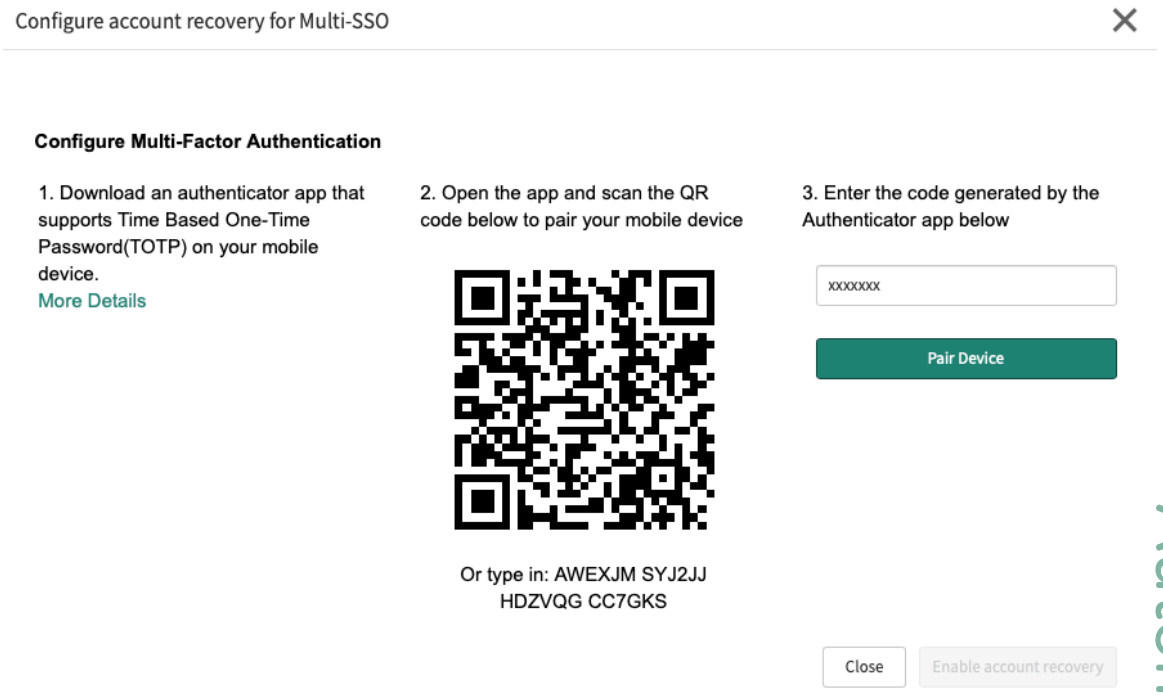
3. Klicken Sie in Schritt 2 auf den Text **hier**.



4. Folgen Sie den Anweisungen auf dem Bildschirm im **Dialogfeld „Kontenwiederherstellung für Multi-SSO konfigurieren“**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem Sie die Schritte auf dem Bildschirm ausgeführt haben, wird die **Option Accountwiederherstellung** aktivieren aktiviert.

5. Klicken Sie **auf Accountwiederherstellung aktivieren**.

Ergebnisse

Sie haben Ihren Benutzeraccount als Accountwiederherstellungsbenutzer konfiguriert. Sie können dieses Konto überprüfen und alle anderen konfigurierten Benutzer für die Kontowiederherstellung anzeigen, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Benutzer**.

Konfigurieren Sie einen Benutzer für die Accountwiederherstellung aus einem Administratorbenutzerprofil

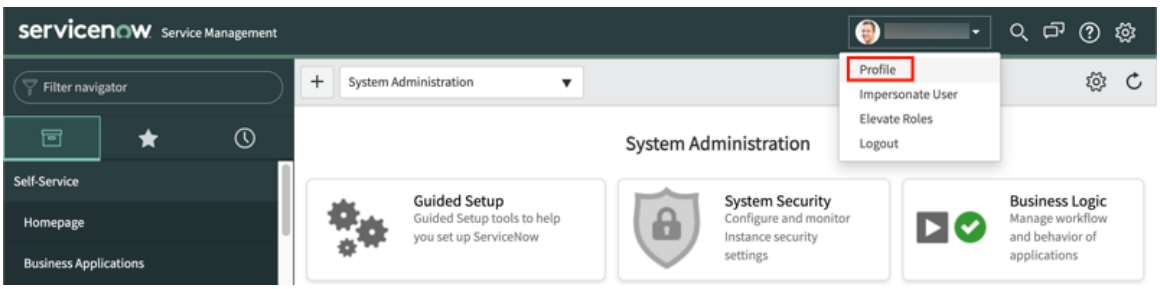
Konfigurieren Sie einen Administrator im Administratorbenutzerprofil als Benutzer für die Accountwiederherstellung.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

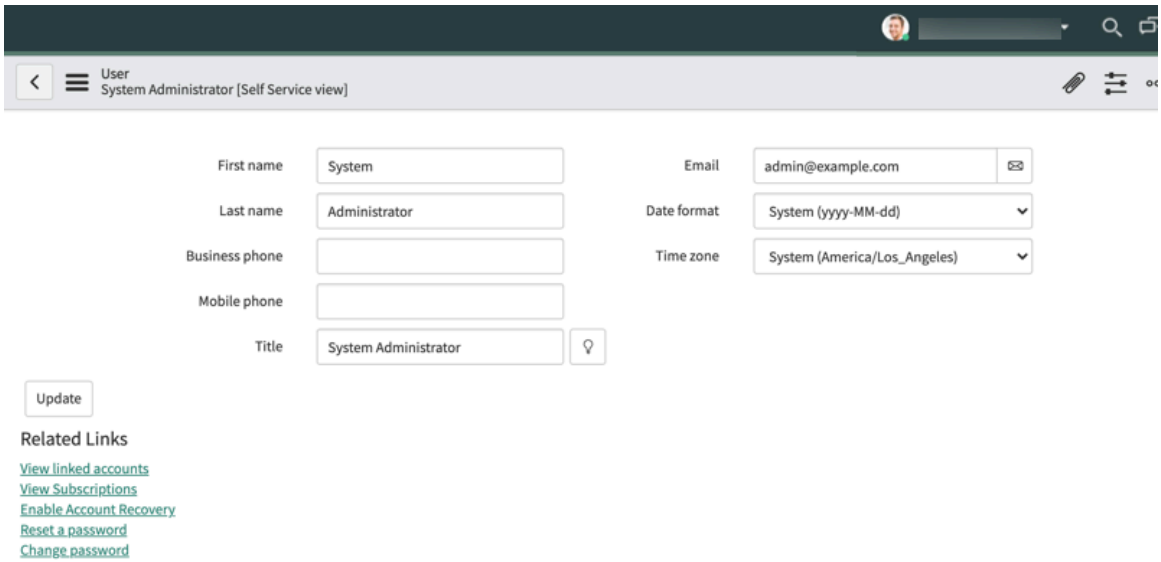
1. Melden Sie sich mit einem Administratorkonto bei Ihrer Instanz an.
2. Klicken Sie im Instanz-Header auf den Benutzernamen und wählen Sie **Profil**aus.



3. Klicken Sie im **Benutzerformular** im Abschnitt „ **Zugehörige Links** “ auf **Accountwiederherstellung aktivieren**.

Automatische Übersetzung

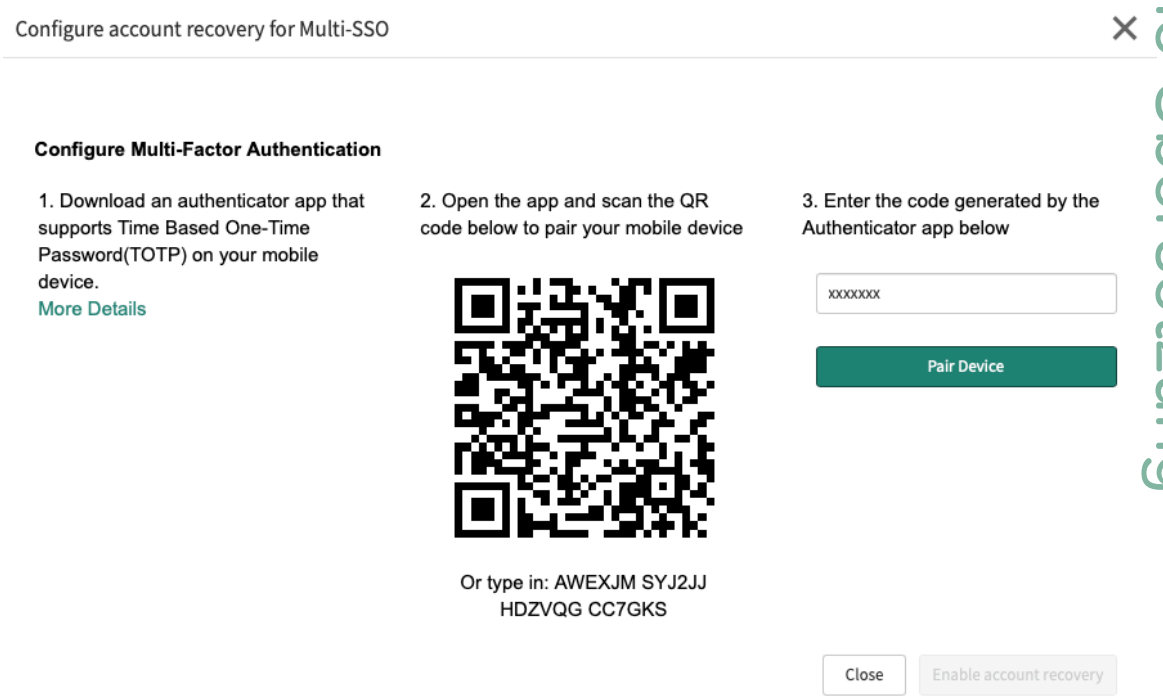
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

Wenn für den ausgewählten Benutzer die Accountwiederherstellung bereits aktiviert ist, wird **Accountwiederherstellung** aktivieren nicht in den zugehörigen Links angezeigt. Stattdessen wird die Option **Accountwiederherstellung deaktivieren angezeigt**.

4. Folgen Sie den Anweisungen auf dem Bildschirm im **Dialogfeld „Kontenwiederherstellung für Multi-SSO konfigurieren“**.



Nachdem Sie die Schritte auf dem Bildschirm ausgeführt haben, wird die **Option Accountwiederherstellung** aktivieren aktiviert.

5. Klicken Sie **auf Accountwiederherstellung aktivieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Sie haben Ihren Benutzeraccount als Accountwiederherstellungsbenutzer konfiguriert. Sie können dieses Konto überprüfen und alle anderen konfigurierten Benutzer für die Kontowiederherstellung anzeigen, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Benutzer**.

Eigenschaften der Accountwiederherstellung

Verwenden Sie Systemeigenschaften, um die Accountwiederherstellung (Account Recovery, ACR) in Ihrer Instanz zu konfigurieren.

Greifen Sie auf die Eigenschaften der Accountwiederherstellung in Ihrer Instanz zu, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Eigenschaften**.

Systemeigenschaften der Accountwiederherstellung

Eigenschaft	Beschreibung
Funktion zur Kontowiederherstellung aktivieren [glide.sso.acr.enabled]	Gibt an, ob die Funktion zur Accountwiederherstellung in Ihrer Instanz aktiviert ist. Diese Eigenschaft ist standardmäßig aktiviert.
Debug-Protokollierung für Account-Wiederherstellung aktivieren [glide.sso.acr.debug.log.enabled]	Gibt an, ob Ihre Instanz Informationen zur Accountwiederherstellung in die Debug-Protokollierung enthält. Diese Eigenschaft ist standardmäßig deaktiviert.
Zeitüberschreitung für ACR-Benutzersitzung (in Minuten) [glide.sso.acr.ui.session.timeout]	Minuten der Inaktivität, bevor Ihre Instanz eine Benutzersitzung zur Accountwiederherstellung beendet. Diese Eigenschaft hat einen Standardwert von 30.

E-Signatur für Mehrfachanbieter-SSO

Mit der E-Signatur mit Mehrfachanbieter-SSO können Sie die E-Signatur-Eigenschaften anstelle der SAML- oder OIDC-Eigenschaften für die Authentifizierung verwenden.

Für die SSO-Überprüfung (Single Sign-on) während der Authentifizierung und für die Anforderung, dass Benutzer vor dem Senden ihrer elektronischen Signatur Anmeldeinformationen angeben müssen, können Sie die Authentifizierung so konfigurieren, dass vor dem Senden einer Signatur die Anmeldeinformationen abgefragt werden.

Sie können das Plugin „Approvals with e-signature“ (`com.glide.e_signature_approvals`) installieren, um die E-Signatur-Konfiguration für SSO-Anmeldungen zu erhalten.

Hinweis:
Sie müssen Code Signing Signatures (`com.glide.code_signing.signatures`) installieren, um das E-Signatur-Plugin zu installieren.

Die Genehmigung mit dem E-Signatur-Plugin aktivieren

Die Genehmigung mit dem E-Signatur-Plugin (com.glide.e_signature_approvals) ermöglicht es Benutzern, Anforderungen zu genehmigen, indem sie ihre Anmeldeinformationen erneut eingeben.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis:
Sie müssen Code Signing Signatures (`com.glide.code_signing.signatures`) installieren, um das E-Signatur-Plugin zu installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Multi-Provider SSO verwenden, um eine SSO-Genehmigung für eine SAML 2.0-Authentifizierung einzurichten

Eine SSO-Genehmigung mit E-Signatur erfordert die Konfiguration der SAML-IdP und der ServiceNow-Instanz.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das SAML-IdP muss das forceAuthn-Attribut in SAML-Bestätigungsanforderungen unterstützen und berücksichtigen. E-Signatur funktioniert ohne diese IdP-Einstellung nicht. Richten Sie eine Genehmigung mit E-Signatur ein, indem Sie Anmeldeinformationen aus einer SAML 2.0-Authentifizierung verwenden.

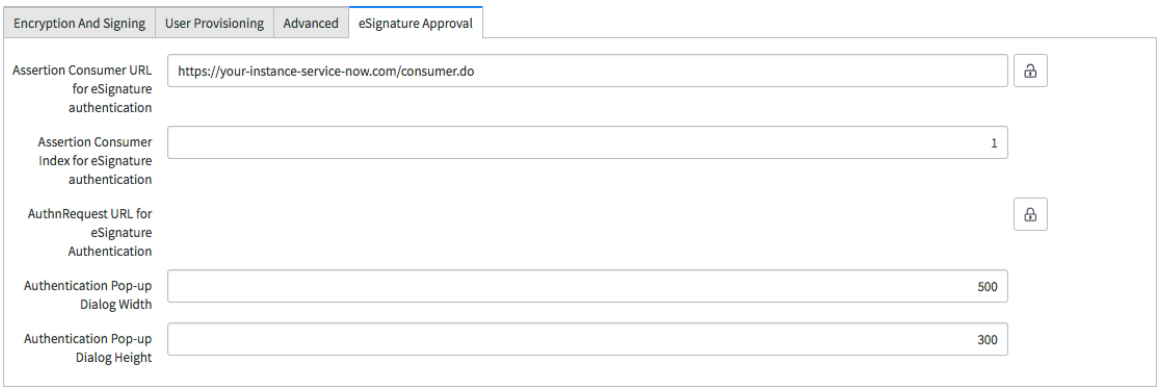
Prozedur

1. Aktivieren oder aktualisieren Sie SAML 2.0 mit dem Plugin „Multi-Provider-SSO aktivieren“.
2. Aktivieren Sie das Plugin für die Genehmigung mit E-Signatur.
3. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider** und stellen Sie sicher, dass auf der Registerkarte „Erweitert“ für die 2.0 SAML-IdP-Konfiguration das Attribut **„AuthnRequest erzwingen“ aktiviert ist**.
   Ihr SAML 2.0-IdP muss das Attribut **„AuthnRequest erzwingen“** unterstützen, andernfalls wird E-Signatur nicht unterstützt.
4. Geben Sie auf der Registerkarte „eSignature-Genehmigung“ die folgenden SAML-Eigenschaften für die E-Signatur ein.

Option	Bezeichnung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Diese Eigenschaft ist standardmäßig auf die entsprechende URL voreingestellt. Um diese Eigenschaft zu konfigurieren, wählen Sie das Schlosssymbol aus, um dieses Feld bearbeitbar zu machen. Klicken Sie nach der Bearbeitung auf das Symbol, um das Feld zu sperren.
Assertionen-Verbraucher-Index für eSignatur-Authentifizierung	Wenn für Ihren Dienstanbieter mehr als eine URL für die AssertionConsumerURL festgelegt ist, können Sie den Index für die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	E-Signatur beginnend mit Index 1 oder höher festlegen.
AuthnRequest-URL für die E-Signatur-Authentifizierung	Sie können die URL eingeben, die auf die SAML 2.0 IdP AuthnRequest-URL für die E-Signatur-Authentifizierung verweist. Wenn die URL mit der Assertion Consumer-URL identisch ist, können Sie diese Einstellung leer lassen.
Breite des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Breite dieses Dialogfelds. Der Standardwert ist 500.
Höhe des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Höhe dieses Dialogfelds. Der Standardwert ist 300.



5. Wählen Sie die Schaltfläche **Metadaten generieren** unter den Registerkarten aus, um die Metadaten des Service Providers neu zu generieren.
6. Kopieren Sie die Metadaten des Service Providers, und aktualisieren Sie sie auf dem SAML-IdP.

Verwenden Sie Mehrfachanbieter-SSO, um eine SSO-Genehmigung für eine OIDC-Authentifizierung einzurichten

Eine SSO-Genehmigung mit E-Signatur erfordert die Konfiguration der SAML-IdP und der ServiceNow-Instanz.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

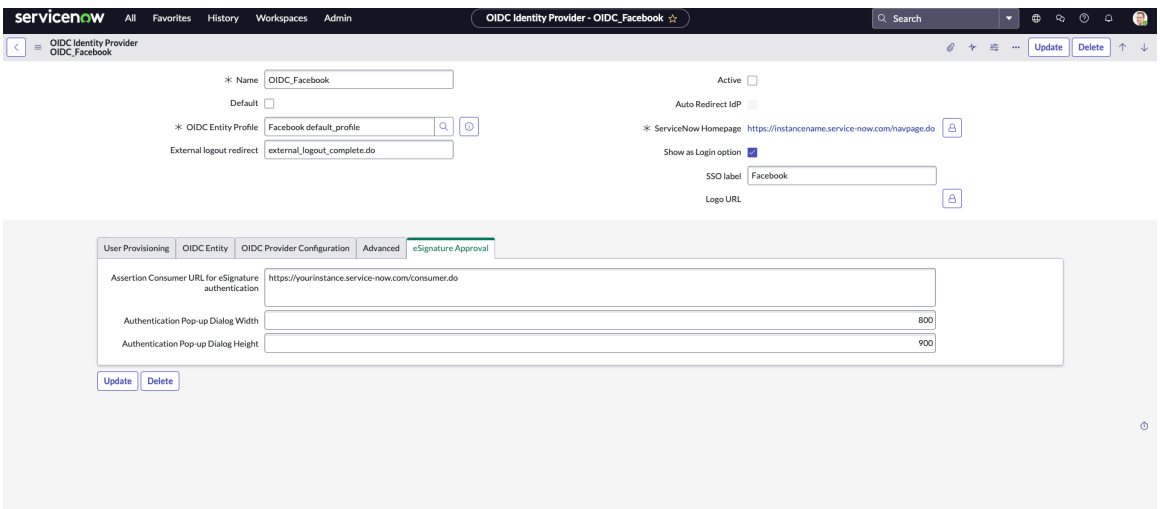
Das SAML-IdP muss das forceAuthn-Attribut in SAML-Bestätigungsanforderungen unterstützen und berücksichtigen. E-Signatur funktioniert ohne diese IdP-Einstellung nicht. Richten Sie eine Genehmigung mit E-Signatur ein, indem Sie Anmeldeinformationen aus einer SAML 2.0-Authentifizierung verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie das Plugin für die Genehmigung mit E-Signatur.
2. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider** und überprüfen Sie Ihre OIDC-Provider-Konfigurationen
3. Geben Sie auf der Registerkarte „eSignature-Genehmigung“ die folgenden SAML-Eigenschaften für die E-Signatur ein.

Option	Bezeichnung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Diese Eigenschaft ist standardmäßig auf die entsprechende URL voreingestellt. Um diese Eigenschaft zu konfigurieren, wählen Sie das Schlosssymbol aus, um dieses Feld bearbeitbar zu machen. Klicken Sie nach der Bearbeitung auf das Symbol, um das Feld zu sperren.
Breite des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Breite dieses Dialogfelds. Der Standardwert ist 800.
Höhe des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Höhe dieses Dialogfelds. Der Standardwert ist 900.



4. Wählen Sie Absenden, wenn Sie die E-Signatur während des ersten **OIDC** -Setups konfigurieren, oder **Aktualisieren**, wenn Sie die Details in der E-Signatur aktualisieren möchten.

OpenID Connect (OIDC) als Single Sign-on (SSO) Identitätsanbieter (IdP)

OpenID Connect (OIDC) ist eine Identitätsebene, die auf dem OAuth-Protokoll basiert und Ihnen und Ihren Endbenutzern eine moderne und intuitive SSO-Experience (Single Sign-on) bietet. OIDC verbessert auch die Anmelde-Experience für mobile Anwendungen, indem Benutzer sich mit ihrem Social Identity Provider bei Anwendungen von ServiceNow anmelden können. Administratoren können beispielsweise Single Sign-on mit einem Identitätsanbieter einer Drittpartei konfigurieren, der OpenID Connect unterstützt. Benutzer haben dann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Möglichkeit, sich mit den Anmeldeinformationen ihres Identitätsanbieters bei Ihrer benutzerdefinierten Anwendung ServiceNow anzumelden.

Sie können soziale Identitätsanbieter wie Google für Ihre Business-to-Customer-Benutzer (B2C) und Unternehmensidentitätsanbieter wie Okta , Microsoft Azure AD für Ihre Business-to-Business-Benutzer verwenden.

OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen

Erstellen oder aktualisieren Sie eine OIDC-Konfiguration (OpenID Connect) mithilfe des Mehrfachanbieter-SSO-Plugins.

OpenID Connect (OIDC)-Konfiguration für Single Sign-on (SSO)

Vorbereitungen

- Registrieren Sie eine OIDC-Anwendung bei Ihrem Identitätsanbieter (IdP), und notieren Sie die Client-ID, den geheimen Clientschlüssel und die URL der bekannten Konfiguration.
- Aktivieren Sie das Multi-Provider-SSO-Plugin
- Konfigurieren Sie Multi-Provider-SSO-Eigenschaften
- Aktivieren Sie das Plugin „Approval with e-Signature “, um eSignature für den OIDC-IdP zu aktivieren.
- Erforderliche Rolle: admin

Wenn Sie eine Client-ID, einen geheimen Clientschlüssel und eine bekannte Konfigurations-URL des Identitätsanbieters haben, können Sie die OIDC-Konfiguration für SSO direkt importieren.

Hinweis:
Die Anmeldeoption mit OIDC-IdP wird nicht unterstützt, wenn das Plugin „Domain Separation“ installiert ist.

Wenn Sie nicht über die erforderlichen Informationen zum Identitätsanbieter verfügen, können Sie OIDC für SSO manuell konfigurieren. Nach Abschluss der Konfiguration können sich Benutzer mit Social Identity-Anbietern von Drittanbietern wie Google OktaServiceNow bei Anwendungen von [] anmelden.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Wählen Sie eine der folgenden Optionen aus.
   - Um eine vorhandene Konfiguration zu aktualisieren, klicken Sie auf einen OIDC-Identitätsanbieter-Datensatz.
   - Um eine neue Konfiguration zu erstellen, klicken Sie auf **Neu**, und wählen Sie **OpenID Connect**aus.
3. Geben Sie für eine neue Konfiguration die OIDC-Konfigurationsinformationen mit einer der folgenden Methoden ein.

Option	Bezeichnung
Importieren Sie die bekannte OpenID Connect-Konfiguration	Wenn Sie die bekannte Konfigurations-URL zusammen mit den zugehörigen Client-Anmeldeinformationen haben, können Sie eine OIDC-Konfiguration direkt importieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Hinweis: Wenn Sie die bekannte OIDC-Konfiguration importieren, werden alle zugehörigen Felder automatisch ausgefüllt.
Konfigurieren Sie das OIDC-Identitätsanbieter-formular manuell	Wenn keine OAuth-OIDC-Entität vorhanden ist, schließen Sie das Popup-Fenster „OpenID Connect-Quellkonfiguration importieren“, und füllen Sie die Felder im Formular „OIDC-Identitätsanbieter“ manuell aus.

Importieren Sie OpenID Connect-Felder mit bekannter Konfiguration

Eigenschaft	Beschreibung
Name	Eindeutiger Name für die Konfiguration des OIDC-Identitätsanbieters.
Client-ID	Client-ID der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Bekannte Konfigurations-URL	URL, die Metadaten zum OIDC-Identitätsanbieter der Drittpartei enthält.

Alle Pflichtfelder im Formular „OIDC-Identitätsanbieter“ müssen ausgefüllt werden.

Bevor Sie das Formular „OIDC-Identitätsanbieter“ manuell ausfüllen, stellen Sie sicher, dass Sie bereits ein OAuth-Entitätsprofil für den OIDC-IdP haben.

Wenn Sie kein OAuth-Entitätsprofil haben, können Sie es mit den Standardvorlagen für externe OIDC-Provider wie Okta, Azure und anderen erstellen.

Der Gewährungstyp des OAuth-Entitätsprofils muss einen Autorisierungscode aufweisen. Weitere Informationen finden Sie unter OAuth-OIDC-Provider auf der Now Platform konfigurieren.

Hinweis:
Sie können die Vorlagen von Identitätsanbietern von Drittanbietern verwenden. Auth0, Azure AD, Google und Okta sind in den Demodaten des Plugins „Single Sign-on-Installationsprogramm für mehrere Anbieter“ verfügbar.

OIDC-Identitätsanbieterfelder

Eigenschaft	Beschreibung
Name	Name des OIDC-Identitätsanbieter-Datensatzes.
Aktiv	Option zum Aktivieren der OIDC-IdP-Konfiguration **Hinweis:** Diese Option kann nur nach einer erfolgreichen Testverbindung aktiviert werden.
Standard	Option zum Festlegen der OIDC-IdP-Konfiguration als Standard, wenn mehr als eine OIDC-Konfiguration vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Automatische IdP-Weiterleitung	Option zum Aktivieren der automatischen Umleitung der Benutzer zur Anmeldeseite des Identitätsanbieters. Dieses Feld wird angezeigt, wenn die Option **Als IdP für automatische Umleitung** festlegen im Abschnitt „Zugehörige Links“ festgelegt ist. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Weiterleitung aktivieren, wird das Cookie `glide_sso_id` automatisch mit dem neuen IdP für die automatische Weiterleitung aktualisiert. Die Systemeigenschaft `glide.authenticate.sso.update.idp.cookie` steuert diese Funktion.
OIDC-Entitätsprofil	OAuth-Entitätsprofil für die OIDC-Konfiguration.
ServiceNow Homepage	Die URL der Anmeldeseite, die für die Authentifizierung verwendet wird. Dieses Feld wird automatisch auf Ihre Instanz-URL festgelegt. Das Format der URL lautet: https://IhreInstanz.service-now.com/navpage.do
Weiterleitung für externe Abmeldung	Die URL, an die die Integration Benutzer nach der Abmeldung umleitet. In der Regel das Portal, das für SSO verwendet wird. Dieses Feld wird automatisch auf external_logout_complete.do festgelegt. Beispiel: https://IhreInstanz.service-now.com/external_logout_complete.do
Als Anmeldeoption anzeigen	Option zum Anzeigen des OIDC-IdP als Anmeldeoption auf der Anmeldeseite. Die Anmeldeoption wird als Schaltfläche „ **Anmeldung mit Identitätsanbieter** “ angezeigt.
SSO-Bezeichnung	Bezeichnung des OIDC-IdP, der auf der Anmeldeseite angezeigt wird. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.
Logo-URL	Öffentlich verfügbare URL, die das Logo des OIDC-IdP-Providers enthält. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.

4. **Wahlweise:** Aktivieren Sie die automatische Benutzerbereitstellung auf der Registerkarte „Benutzerbereitstellung“ > Registerkarte „Benutzerbereitstellung“.

   (Optional) Sie können die automatische Benutzerbereitstellung während der Benutzeranmeldung aktivieren. Wenn die automatische Benutzerbereitstellung aktiviert ist, wird automatisch ein Benutzerdatensatz in der ServiceNow-Instanz erstellt, wenn dieser Benutzerdatensatz nicht vorhanden ist.

Benutzerbereitstellungsfelder

Eigenschaft	Beschreibung
Benutzer automatisch bereitstellen	Option zum Aktivieren der automatischen Anwenderbereitstellung. Diese Eigenschaft erstellt einen Benutzer in der Instanzbenutzertabelle (sys_user), wenn der Benutzer den IdP verlässt, aber nicht in der Benutzertabelle vorhanden ist.
Bereitstellen mit	Datenquelle, die zum Transformieren eines ID-Tokens, eines Benutzerinformationsendpunkts oder von ID-Token und Benutzerinformationen in einen ServiceNow-Benutzer verwendet werden soll. Verwenden Sie die Nachschlageliste, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Transformationstabellenzuordnung zu konfigurieren.
Bereitstellungsdatenquelle	ID-Token-Datenquelle, die für die Benutzerbereitstellung verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Datenquelle von Anwenderinformationen	Die für die Anwenderbereitstellung verwendete Datenquelle des Anwenderinformationsendpunkts. Dieses Feld wird angezeigt, wenn Benutzerinformationen oder ID-Token und Benutzerinformationen für das Feld **Bereitstellung mit** ausgewählt sind.
Anwender bei der nächsten Anmeldung aktualisieren	Option zum Aktivieren der Anwenderaktualisierung bei der nächsten Anmeldung.
Anwenderintervallzeit aktualisieren (Sekunden)	Minimales Zeitintervall in Sekunden zum Aktualisieren eines Benutzerdatensatzes zwischen aufeinanderfolgenden Anmeldungen. Dieses Feld wird automatisch auf 3.600 Sekunden festgelegt. Beispiel: Nachdem sich ein Benutzer angemeldet hat, wird der Benutzerdatensatz 3.600 Sekunden bis zur nächsten Anmeldung aktualisiert. Dieses Feld ist nur verfügbar, wenn das Feld **Benutzer bei der nächsten Anmeldung** aktualisieren aktiviert ist.
Auf bereitgestellte Benutzer angewendete Benutzerrollen	Liste der Rollen, die auf die neu bereitgestellten Benutzer angewendet werden.

5. Registerkarte „OIDC-Entität“.
   Sie können die OIDC-Client-Konfiguration und den OIDC-Verbindungs-Flow mithilfe des Entitätsdatensatzes anzeigen und ändern.
6. Registerkarte „OIDC-Providerkonfiguration“.
   Sie können die bekannte Konfigurations-URL der Validierung des OIDC-IdP- oder ID-Token-Anspruchs anzeigen und ändern.
7. **Wahlweise:** Registerkarte „Erweitert“

   (Optional) Skripts, die beim einmaligen Anmelden und Abmelden ausgeführt werden.

   Erweiterte Felder

Eigenschaft	Beschreibung
Single Sign-on-Skript	Skript, das während Single Sign-on ausgeführt wird. Dieses Feld wird automatisch auf MultiSSO_OIDC_custom festgelegt.
Abmeldeskript	Skript, das ausgeführt wird, nachdem sich der Benutzer abgemeldet hat. Dieses Feld wird automatisch auf MultiSSO_OIDC_logout_custom festgelegt.

8. **Wahlweise:** Konfigurieren Sie auf der Registerkarte eSignature-Genehmigung die eSignature für den OIDC-IdP.

   Hinweis:
   Die Registerkarte eSignature-Genehmigung wird nur angezeigt, wenn Sie das Plugin „ **Approval with e-Signature** “ (com.glide.e_signature_approvals) installieren.

   eSignature-Genehmigungsfelder

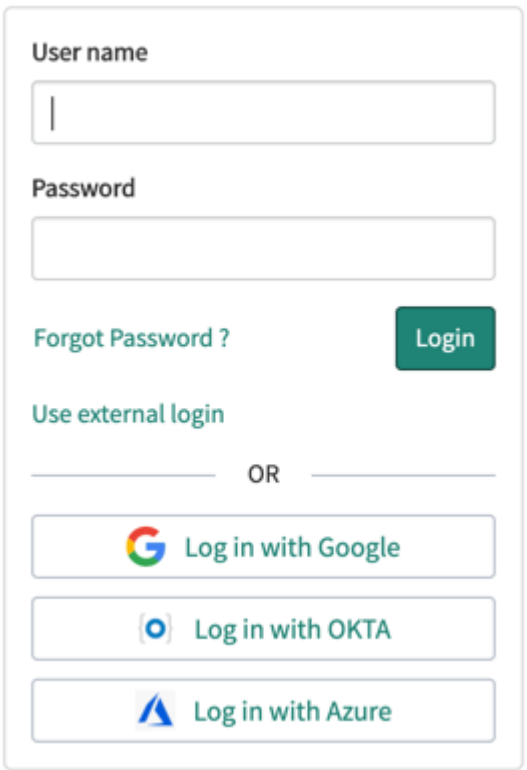
Eigenschaft	Beschreibung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Wenn Sie eine benutzerdefinierte Methode zur Verarbeitung der OIDC-Authentifizierung für eSignature verwenden, können Sie Ihre eigene Verbraucher-URL einrichten. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Sie beispielsweise Mehrfachanbieter-SSO verwenden, müssen Sie diese Eigenschaft nicht verwenden. Dieses Format der URL ist https://IhreInstanz.service-now.com/consumer.do
Breite des Popup-Dialogfelds für Authentifizierung	Breite des Popup-Dialogfelds zur Authentifizierung. Dieses Feld wird automatisch auf 800festgelegt.
Höhe des Popup-Dialogfelds für Authentifizierung	Höhe des Popup-Dialogfelds für die Authentifizierung. Dieses Feld wird automatisch auf 900festgelegt.

9. **Wahlweise:** Navigieren Sie zur Anmeldeseite der Instanz, um zu überprüfen, ob IdP als Anmeldeoption angezeigt wird.
   Die URL muss das folgende Format aufweisen: https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP

   Hinweis:
   Wenn Sie „ **Als Anmeldeoption ausgewählt**“ aktiviert haben, können Sie zur Anmelde-URL der Instanz wechseln.



Facebook-basiertes Single Sign-on (SSO) verwenden

Melden Sie sich bei Ihrer ServiceNow -Instanz mit Ihren Facebook -Anmeldeinformationen im Facebook-basierten SSO an.

Vorbereitungen

Das Facebook-basierte SSO wird zusammen mit Ihrer ServiceNow -Instanz geliefert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Identitätsanbieterkonfigurationen (IdP) für den **OIDC_Facebook-** IdP als **Identitätsanbieter**definieren. Weitere Informationen zu IdP-Konfigurationen finden Sie unter Facebook-basiertes Single Sign-on (SSO) konfigurieren.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Wählen **Sie OIDC_Facebook aus**.
3. Geben Sie auf der Seite OIDC_Facebook die folgenden Felder an:

Hinweis:

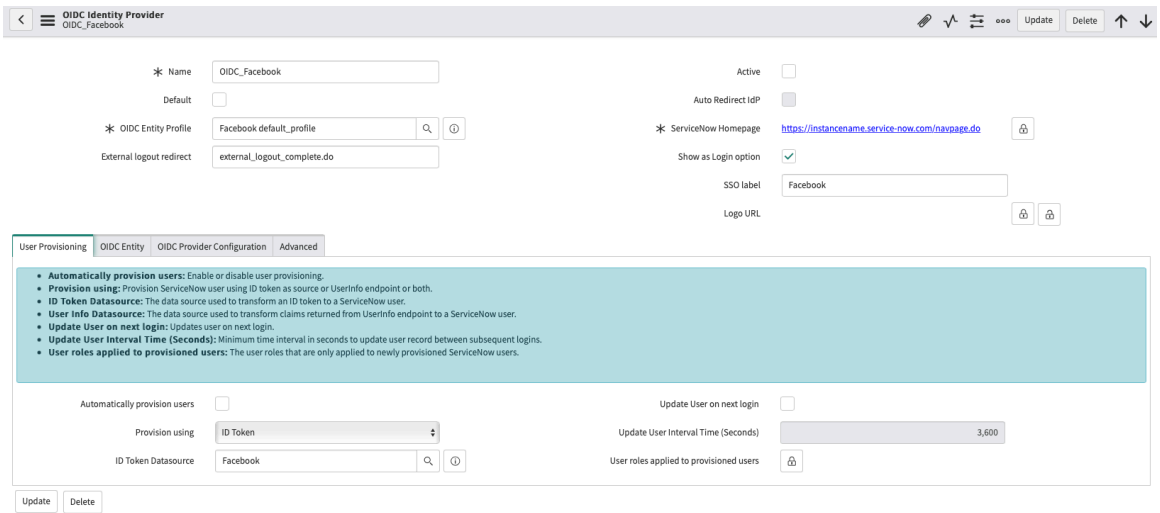
- Die meisten Felder werden bei Verwendung des Standard-IdP automatisch ausgefüllt.
- Details der Homepage ServiceNow müssen angegeben werden.
- Benutzerbezogene Details wie Client-ID und geheimer Clientschlüssel von Facebook müssen innerhalb des IdP angegeben werden.

OIDC_Facebook Identitätsanbieterdetails

Feld	Beschreibung
Name	Name des OIDC-IdP-Datensatzes. Geben Sie OIDC_Facebook ein.
Standard	Option zum Festlegen der OIDC-IdP-Konfiguration als Standard.
OIDC-Entitätsprofil	OAuth-Entitätsprofil für die OIDC-Konfiguration. Geben Sie Facebook default_profile ein.
Weiterleitung für externe Abmeldung	Die URL, an die die Integration Benutzer nach der Abmeldung umleitet. Normalerweise ist diese URL das Portal, das für SSO verwendet wird. Dieses Feld wird automatisch auf **external_logout_complete.do**festgelegt. Beispiel: https://<yourinstance> .service-now.com/external_logout_complete.do .
Aktiv	Option zum Aktivieren der OIDC-IdP-Konfiguration **Hinweis:** Diese Option kann nur nach einer erfolgreichen Testverbindung aktiviert werden.
Automatische IdP-Weiterleitung	Option zum Aktivieren der automatischen Umleitung der Benutzer zur Anmeldeseite des Identitätsanbieters.
ServiceNow Homepage	Die URL der Anmeldeseite, die für die Authentifizierung verwendet wird. Dieses Feld wird automatisch auf Ihre Instanz-URL festgelegt. Das Format der URL ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	https://.<yourinstance> .service-now.com/navpage.do
Als Anmeldeoption anzeigen	Option zum Anzeigen des OIDC-IdP als Anmeldeoption auf der Anmeldeseite. In diesem Fall wird die Anmeldeoption als Schaltfläche **Mit Facebook** anmelden angezeigt.
SSO-Bezeichnung	Bezeichnung des OIDC-IdP, der auf der Anmeldeseite angezeigt wird. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.
Logo-URL	Öffentlich verfügbare URL, die das Logo des OIDC-IdP-Providers enthält. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.



4. **Wahlweise:** Öffnen Sie die Registerkarte **Benutzerbereitstellung**, und füllen Sie die Felder aus.

> **Hinweis:**
> Sie müssen die OIDC-bezogenen Informationen wie Client-ID und Client-Secret Ihrer Benutzer aus Facebookkonfigurieren.

Registerkarte Benutzerbereitstellung

Feld	Beschreibung
Benutzer automatisch bereitstellen	Option zum Aktivieren der automatischen Anwenderbereitstellung. Diese Eigenschaft erstellt einen Benutzer in der Instanzbenutzertabelle [sys_user], wenn der Benutzer auf dem IdP, aber nicht in der Benutzertabelle vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie können die automatische Benutzerbereitstellung während der Benutzeranmeldung aktivieren. Wenn die automatische Benutzerbereitstellung aktiviert ist, wird automatisch ein Benutzerdatensatz in der Instanz ServiceNow erstellt, wenn dieser Benutzerdatensatz nicht vorhanden ist.
Bereitstellen mit	Die Datenquelle, die für die Transformation in einen ServiceNow -Benutzer verwendet werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Ein ID-Token** ○ **Anwenderinfo-Endpunkt** ○ **Sowohl ID-Token als auch Anwenderinformationen** Verwenden Sie die Nachschlageliste, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Transformationstabellenzuordnung zu konfigurieren.
Bereitstellungsdatenquelle	Die ID-Token-Datenquelle, die für die Benutzerbereitstellung verwendet wird.
Datenquelle von Anwenderinformationen	Die für die Benutzerbereitstellung verwendete Datenquelle für den Benutzerinfo-Endpunkt. Dieses Feld wird nur angezeigt, wenn **Benutzerinformationen** oder **ID-Token und Benutzerinformationen gleichzeitig** im Feld **Bereitstellung mit** ausgewählt werden.
Anwender bei der nächsten Anmeldung aktualisieren	Option zum Aktivieren von Benutzer-Updates während der nächsten Anmeldung.
Anwenderintervallzeit aktualisieren (Sekunden)	Minimales Zeitintervall (in Sekunden) zum Aktualisieren eines Benutzerdatensatzes zwischen aufeinanderfolgenden Anmeldungen. Dieses Feld wird automatisch auf 3600 Sekunden festgelegt. Beispiel: Nachdem sich ein Benutzer angemeldet hat, wird der Benutzerdatensatz 3.600 Sekunden bis zur nächsten Anmeldung aktualisiert. Dieses Feld ist nur verfügbar, wenn das Feld **Benutzer bei der nächsten Anmeldung** aktualisieren aktiviert ist.
Auf bereitgestellte Benutzer angewendete Benutzerrollen	Liste der Rollen, die auf die neu bereitgestellten Benutzer angewendet werden.

5. Zeigen Sie auf der Registerkarte **OIDC-Entität** die OIDC-Clientkonfiguration und den OIDC-Verbindungs-Flow mithilfe des Entitätsdatensatzes an und ändern Sie sie.
   Weitere Informationen zur OIDC-basierten Konfiguration finden Sie unter Konfigurieren Sie einen OAuth-OIDC-Provider auf der Now Platform
6. Zeigen Sie auf der Registerkarte **OIDC-Providerkonfiguration** die bekannte Konfigurations-URL des OIDC-IdP an und ändern Sie sie.
7. **Wahlweise:** Öffnen Sie die Registerkarte **Erweitert**, und füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erweitert“

Eigenschaft	Beschreibung
Single Sign-on-Skript	Das Skript, das während Single Sign-on ausgeführt wird.
Abmeldeskript	Das Skript, das ausgeführt wird, nachdem sich der Benutzer abgemeldet hat.

Hinweis:
Skripts werden beim einmaligen Anmelden und Abmelden ausgeführt.

8. Um die Konfiguration zu aktivieren und zu testen, klicken Sie auf **Aktiv**.
9. Um den Datensatz zu aktualisieren, klicken Sie auf **Aktualisieren**.
   Die Facebook-basierte Anmeldeoption wird im Anmeldeformular angezeigt.
10. Wenn Sie sich im Anmeldeformular anmelden, gehen Sie wie folgt vor:
    a. Wählen Sie die Option Facebook.
    b. Um sich bei der Instanz ServiceNow anzumelden, geben Sie Ihre Facebook -Anmeldeinformationen an.

Facebook-basiertes Single Sign-on (SSO) konfigurieren

Konfigurieren Sie ein Facebook-basiertes SSO für Ihre ServiceNow -Instanz.

Vorbereitungen

Sie müssen über eine gültige Client-ID verfügen, die als IdP von Facebookkonfiguriert ist.

Aktivieren Sie die folgenden Eigenschaften:

- Aktivieren Sie Mehrfachanbieter-SSO.
- Aktivieren Sie die Debug-Protokollierung für SSO-Integrationen mit mehreren Anbietern.

Erforderliche Rolle: admin

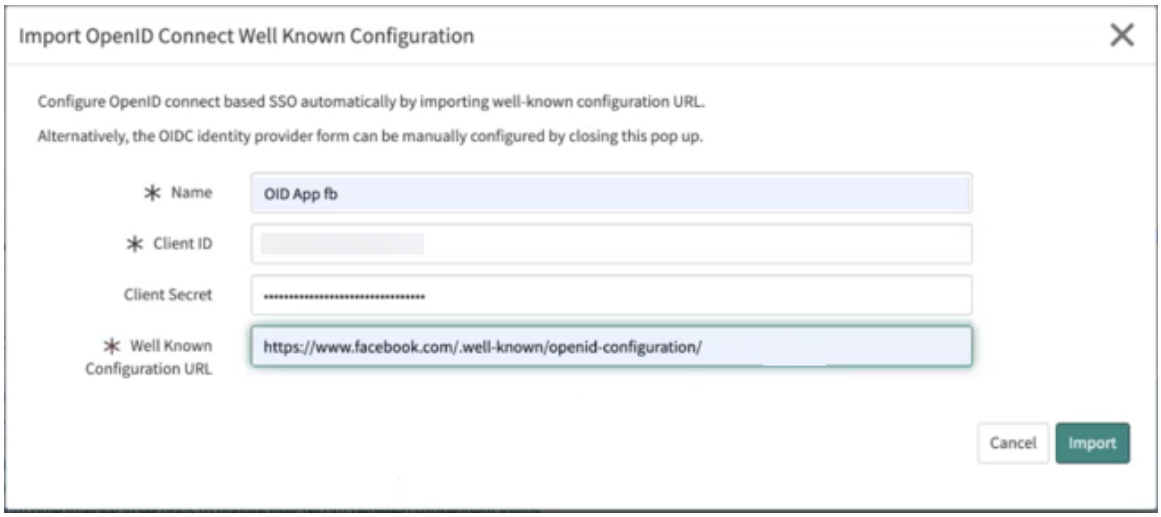
Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Um einen neuen Facebook Identitätsanbieter zu erstellen, klicken Sie auf **Neu**.
3. Klicken Sie **auf OpenID Connect**.
4. Füllen Sie die Felder des Formulars aus.

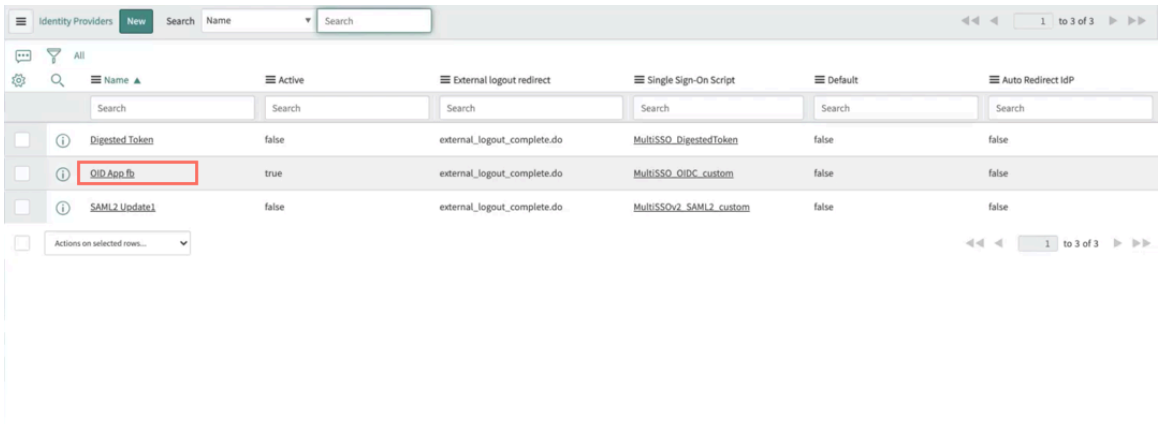
Formular „Bekannte OpenID Connect-Konfiguration importieren“.

Felder	Beschreibung
Name	Eindeutiger Name für die Konfiguration des OIDC-Identitätsanbieters.
Client-ID	Client-ID der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Bekannte Konfigurations-URL	Die URL, die Metadaten zum OIDC-Identitätsanbieter der Drittpartei enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



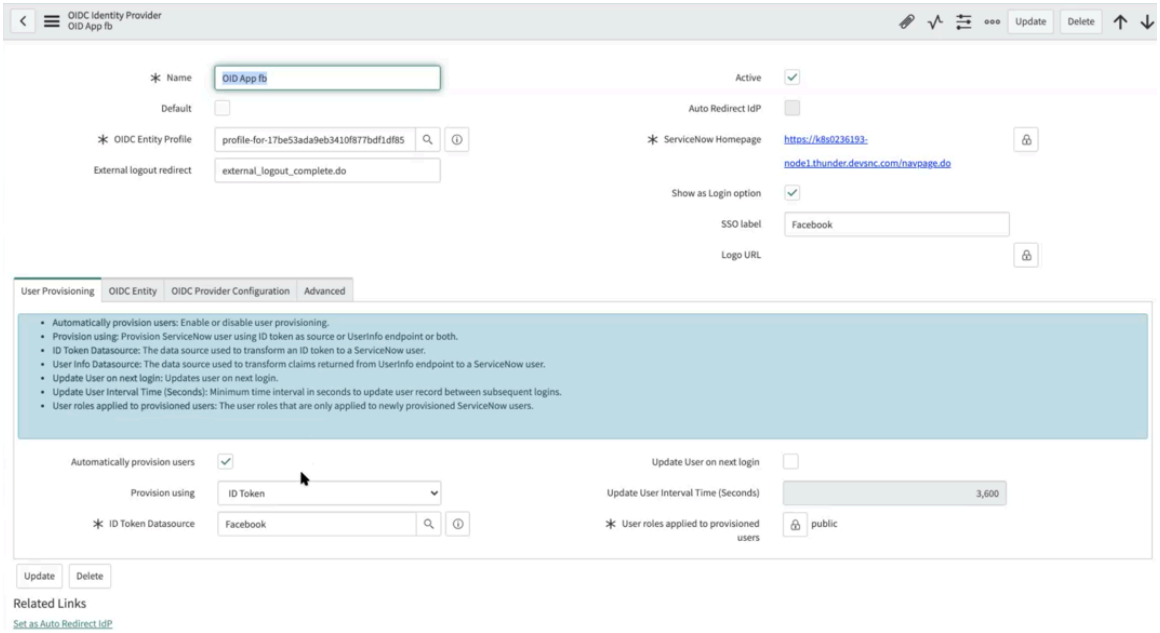
5. Klicken Sie auf **Importieren**.
   Der Facebook-basierte IdP wird erstellt.



6. Wählen Sie den IdP Facebook aus.
7. Gehen Sie im IDP Facebook wie folgt vor:
   a. Validieren Sie alle Felder wie **Name**, **OIDC-Entitätsprofil**, **externe**Abmeldeumleitung und **ServiceNow-Homepage**.
   b. Geben Sie Ihre **SSO-Bezeichnung an**.
8. Geben Sie auf der Registerkarte **Benutzerbereitstellung** die Felder an, die Sie benötigen, um Benutzer für bestimmte Benutzerbereitstellungen und Rollen zu konfigurieren.

   Nur die Pflichtfelder sind erforderlich. Sie können die verbleibenden Felder je nach Bedarf angeben.

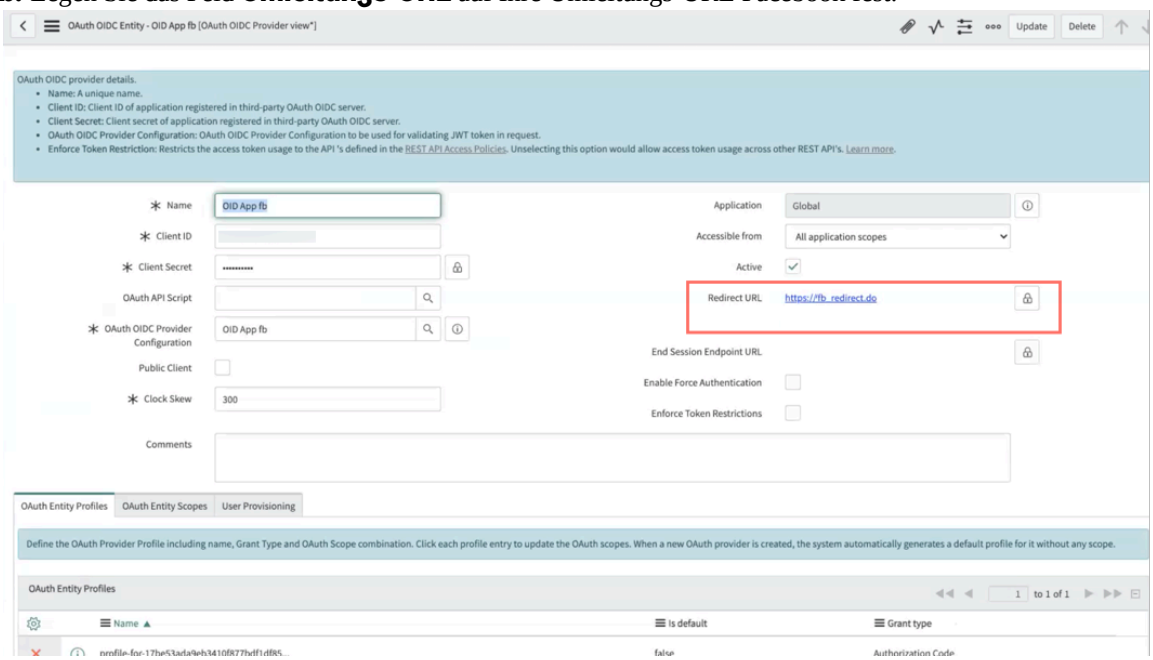
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Gehen Sie auf der Registerkarte **OIDC-Entität** wie folgt vor:

a. Klicken Sie auf die Entität.

b. Legen Sie das Feld **Umleitungs-URL** auf Ihre Umleitungs-URL Facebook fest.

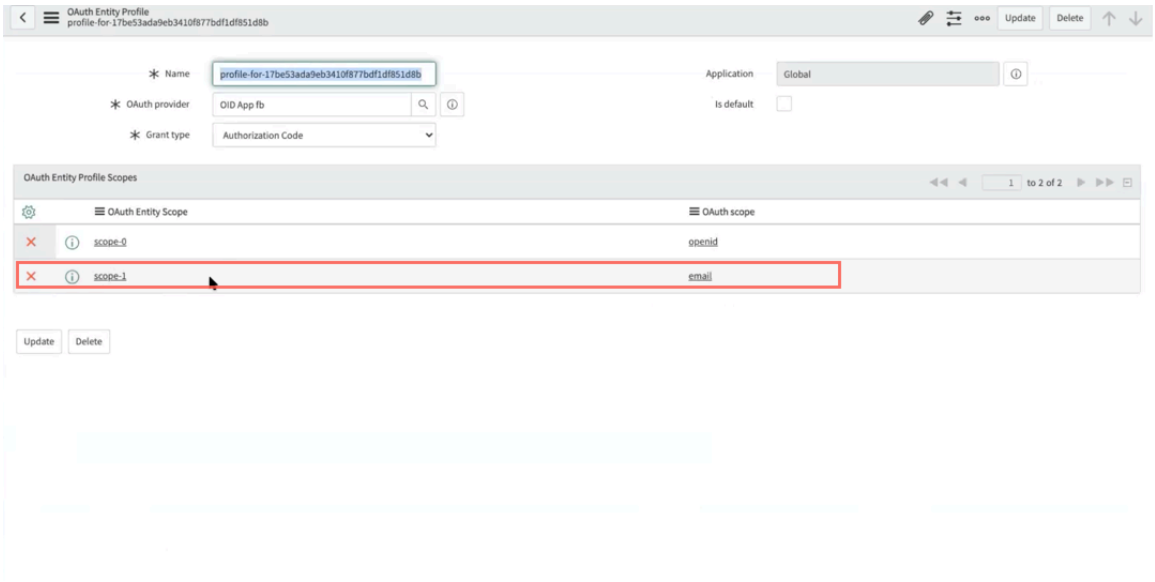


10. Gehen Sie auf der Registerkarte **OAuth-Entitätsprofile** wie folgt vor:

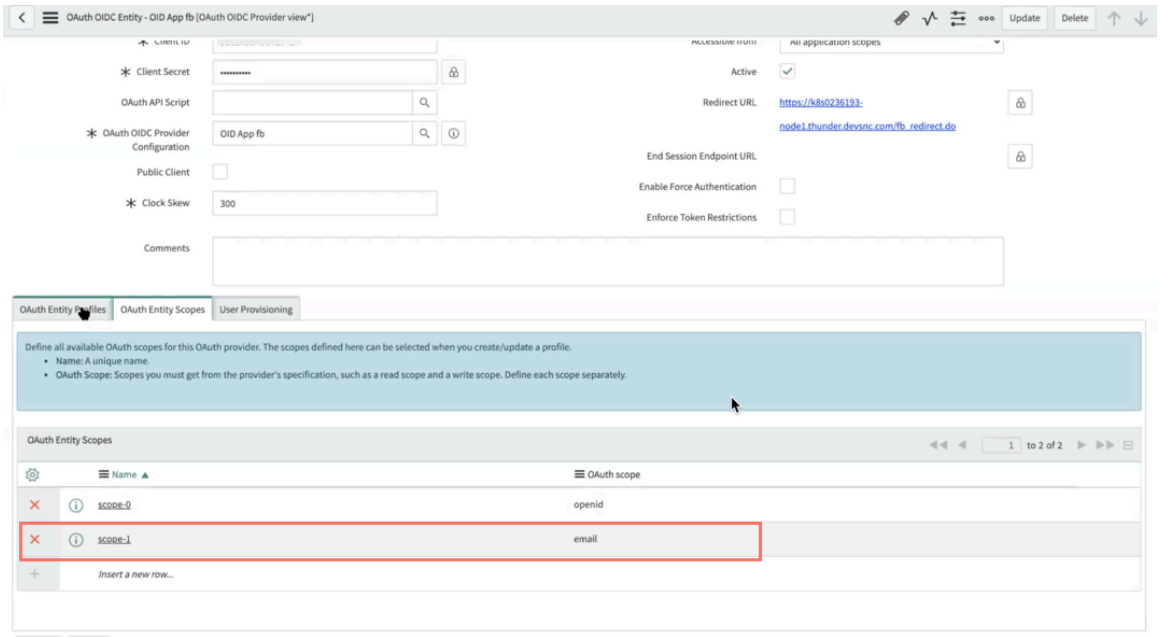
a. Klicken Sie in den Profildetails auf ein Profil.

b. Wählen Sie einen Bereich aus, und überprüfen Sie die Details.
Wählen Sie beispielsweise **scope-1**aus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Klicken Sie auf der Registerkarte **OAuth-Entitätsumfänge** auf den Link **scope-1**, und fügen Sie den Bereich als E- Mailhinzu.



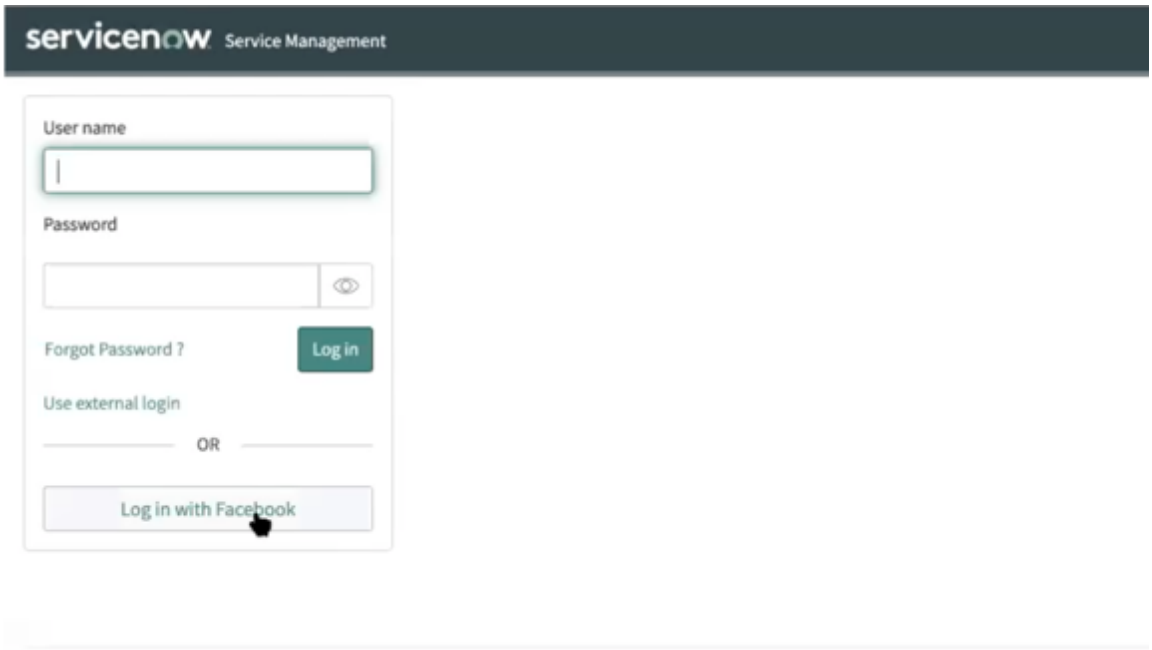
12. Um die Konfiguration zu speichern, klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie auf **Speichern**.
13. Um die Konfiguration als aktiv festzulegen, wählen Sie **Aktiv**aus.

Ergebnisse

Benutzer werden mit der Option Facebook SSO im Anmeldeformular angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen

Erstellen oder aktualisieren Sie eine OIDC-Konfiguration (OpenID Connect) mithilfe des Mehrfachanbieter-SSO-Plugins.

OpenID Connect (OIDC)-Konfiguration für Single Sign-on (SSO)

Vorbereitungen

- Registrieren Sie eine OIDC-Anwendung bei Ihrem Identitätsanbieter (IdP), und notieren Sie die Client-ID, den geheimen Clientschlüssel und die URL der bekannten Konfiguration.
- Aktivieren Sie das Multi-Provider-SSO-Plugin
- Konfigurieren Sie Multi-Provider-SSO-Eigenschaften
- Aktivieren Sie das Plugin „Approval with e-Signature “, um eSignature für den OIDC-IdP zu aktivieren.
- Erforderliche Rolle: admin

Wenn Sie eine Client-ID, einen geheimen Clientschlüssel und eine bekannte Konfigurations-URL des Identitätsanbieters haben, können Sie die OIDC-Konfiguration für SSO direkt importieren.

Hinweis:
Die Anmeldeoption mit OIDC-IdP wird nicht unterstützt, wenn das Plugin „Domain Separation“ installiert ist.

Wenn Sie nicht über die erforderlichen Informationen zum Identitätsanbieter verfügen, können Sie OIDC für SSO manuell konfigurieren. Nach Abschluss der Konfiguration können sich Benutzer mit Social Identity-Anbietern von Drittanbietern wie Google OktaServiceNow bei Anwendungen von [] anmelden.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Wählen Sie eine der folgenden Optionen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um eine vorhandene Konfiguration zu aktualisieren, klicken Sie auf einen OIDC-Identitätsanbieter-Datensatz.
- Um eine neue Konfiguration zu erstellen, klicken Sie auf **Neu**, und wählen Sie **OpenID Connect**aus.

3. Geben Sie für eine neue Konfiguration die OIDC-Konfigurationsinformationen mit einer der folgenden Methoden ein.

Option	Bezeichnung
Importieren Sie die bekannte OpenID Connect-Konfiguration	Wenn Sie die bekannte Konfigurations-URL zusammen mit den zugehörigen Client-Anmeldeinformationen haben, können Sie eine OIDC-Konfiguration direkt importieren. **Hinweis:** Wenn Sie die bekannte OIDC-Konfiguration importieren, werden alle zugehörigen Felder automatisch ausgefüllt.
Konfigurieren Sie das OIDC-Identitätsanbieter-formular manuell	Wenn keine OAuth-OIDC-Entität vorhanden ist, schließen Sie das Popup-Fenster „OpenID Connect-Quellkonfiguration importieren“, und füllen Sie die Felder im Formular „OIDC-Identitätsanbieter“ manuell aus.

Importieren Sie OpenID Connect-Felder mit bekannter Konfiguration

Eigenschaft	Beschreibung
Name	Eindeutiger Name für die Konfiguration des OIDC-Identitätsanbieters.
Client-ID	Client-ID der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Bekannte Konfigurations-URL	URL, die Metadaten zum OIDC-Identitätsanbieter der Drittpartei enthält.

Alle Pflichtfelder im Formular „OIDC-Identitätsanbieter“ müssen ausgefüllt werden.

Bevor Sie das Formular „OIDC-Identitätsanbieter“ manuell ausfüllen, stellen Sie sicher, dass Sie bereits ein OAuth-Entitätsprofil für den OIDC-IdP haben.

Wenn Sie kein OAuth-Entitätsprofil haben, können Sie es mit den Standardvorlagen für externe OIDC-Provider wie Okta, Azure und anderen erstellen.

Der Gewährungstyp des OAuth-Entitätsprofils muss einen Autorisierungscode aufweisen. Weitere Informationen finden Sie unter OAuth-OIDC-Provider auf der Now Platform konfigurieren.

Hinweis:
Sie können die Vorlagen von Identitätsanbietern von Drittanbietern verwenden. Auth0, Azure AD, Google und Okta sind in den Demodaten des Plugins „Single Sign-on-Installationsprogramm für mehrere Anbieter“ verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OIDC-Identitätsanbieterfelder

Eigenschaft	Beschreibung
Name	Name des OIDC-Identitätsanbieter-Datensatzes.
Aktiv	Option zum Aktivieren der OIDC-IdP-Konfiguration **Hinweis:** Diese Option kann nur nach einer erfolgreichen Testverbindung aktiviert werden.
Standard	Option zum Festlegen der OIDC-IdP-Konfiguration als Standard, wenn mehr als eine OIDC-Konfiguration vorhanden ist.
Automatische IdP-Weiterleitung	Option zum Aktivieren der automatischen Umleitung der Benutzer zur Anmeldeseite des Identitätsanbieters. Dieses Feld wird angezeigt, wenn die Option **Als IdP für automatische Umleitung** festlegen im Abschnitt „Zugehörige Links“ festgelegt ist. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Weiterleitung aktivieren, wird das Cookie `glide_sso_id` automatisch mit dem neuen IdP für die automatische Weiterleitung aktualisiert. Die Systemeigenschaft `glide.authenticate.sso.update.idp.cookie` steuert diese Funktion.
OIDC-Entitätsprofil	OAuth-Entitätsprofil für die OIDC-Konfiguration.
ServiceNow Homepage	Die URL der Anmeldeseite, die für die Authentifizierung verwendet wird. Dieses Feld wird automatisch auf Ihre Instanz-URL festgelegt. Das Format der URL lautet: https://IhreInstanz.service-now.com/navpage.do
Weiterleitung für externe Abmeldung	Die URL, an die die Integration Benutzer nach der Abmeldung umleitet. In der Regel das Portal, das für SSO verwendet wird. Dieses Feld wird automatisch auf external_logout_complete.do festgelegt. Beispiel: https://IhreInstanz.service-now.com/external_logout_complete.do
Als Anmeldeoption anzeigen	Option zum Anzeigen des OIDC-IdP als Anmeldeoption auf der Anmeldeseite. Die Anmeldeoption wird als Schaltfläche „ **Anmeldung mit Identitätsanbieter** “ angezeigt.
SSO-Bezeichnung	Bezeichnung des OIDC-IdP, der auf der Anmeldeseite angezeigt wird. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.
Logo-URL	Öffentlich verfügbare URL, die das Logo des OIDC-IdP-Providers enthält. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.

4. **Wahlweise:** Aktivieren Sie die automatische Benutzerbereitstellung auf der Registerkarte „Benutzerbereitstellung“ > Registerkarte „Benutzerbereitstellung“.

   (Optional) Sie können die automatische Benutzerbereitstellung während der Benutzeranmeldung aktivieren. Wenn die automatische Benutzerbereitstellung aktiviert ist, wird automatisch ein Benutzerdatensatz in der ServiceNow-Instanz erstellt, wenn dieser Benutzerdatensatz nicht vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerbereitstellungsfelder

Eigenschaft	Beschreibung
Benutzer automatisch bereitstellen	Option zum Aktivieren der automatischen Anwenderbereitstellung. Diese Eigenschaft erstellt einen Benutzer in der Instanzbenutzertabelle (sys_user), wenn der Benutzer den IdP verlässt, aber nicht in der Benutzertabelle vorhanden ist.
Bereitstellen mit	Datenquelle, die zum Transformieren eines ID-Tokens, eines Benutzerinformationsendpunkts oder von ID-Token und Benutzerinformationen in einen ServiceNow-Benutzer verwendet werden soll. Verwenden Sie die Nachschlageliste, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Transformationstabellenzuordnung zu konfigurieren.
Bereitstellungsdatenquelle	ID-Token-Datenquelle, die für die Benutzerbereitstellung verwendet wird.
Datenquelle von Anwenderinformationen	Die für die Anwenderbereitstellung verwendete Datenquelle des Anwenderinformationsendpunkts. Dieses Feld wird angezeigt, wenn Benutzerinformationen oder ID-Token und Benutzerinformationen für das Feld **Bereitstellung mit** ausgewählt sind.
Anwender bei der nächsten Anmeldung aktualisieren	Option zum Aktivieren der Anwenderaktualisierung bei der nächsten Anmeldung.
Anwenderintervallzeit aktualisieren (Sekunden)	Minimales Zeitintervall in Sekunden zum Aktualisieren eines Benutzerdatensatzes zwischen aufeinanderfolgenden Anmeldungen. Dieses Feld wird automatisch auf 3.600 Sekunden festgelegt. Beispiel: Nachdem sich ein Benutzer angemeldet hat, wird der Benutzerdatensatz 3.600 Sekunden bis zur nächsten Anmeldung aktualisiert. Dieses Feld ist nur verfügbar, wenn das Feld **Benutzer bei der nächsten Anmeldung** aktualisieren aktiviert ist.
Auf bereitgestellte Benutzer angewendete Benutzerrollen	Liste der Rollen, die auf die neu bereitgestellten Benutzer angewendet werden.

5. Registerkarte „OIDC-Entität“.
   Sie können die OIDC-Client-Konfiguration und den OIDC-Verbindungs-Flow mithilfe des Entitätsdatensatzes anzeigen und ändern.
6. Registerkarte „OIDC-Providerkonfiguration“.
   Sie können die bekannte Konfigurations-URL der Validierung des OIDC-IdP- oder ID-Token-Anspruchs anzeigen und ändern.
7. **Wahlweise:** Registerkarte „Erweitert“

   (Optional) Skripts, die beim einmaligen Anmelden und Abmelden ausgeführt werden.

Erweiterte Felder

Eigenschaft	Beschreibung
Single Sign-on-Skript	Skript, das während Single Sign-on ausgeführt wird. Dieses Feld wird automatisch auf MultiSSO_OIDC_custom festgelegt.
Abmeldeskript	Skript, das ausgeführt wird, nachdem sich der Benutzer abgemeldet hat. Dieses Feld wird automatisch auf MultiSSO_OIDC_logout_custom festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. **Wahlweise:** Konfigurieren Sie auf der Registerkarte eSignature-Genehmigung die eSignature für den OIDC-IdP.

   Hinweis:
   Die Registerkarte eSignature-Genehmigung wird nur angezeigt, wenn Sie das Plugin „ **Approval with e-Signature** “ (com.glide.e_signature_approvals) installieren.

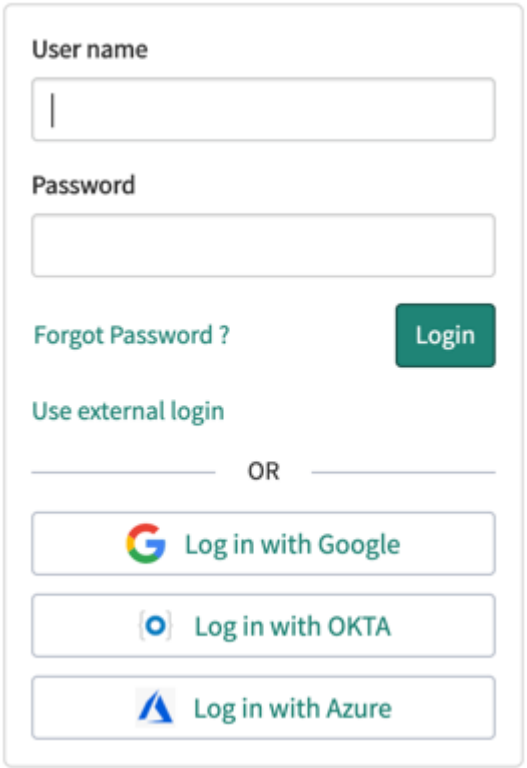
   eSignature-Genehmigungsfelder

Eigenschaft	Beschreibung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Wenn Sie eine benutzerdefinierte Methode zur Verarbeitung der OIDC-Authentifizierung für eSignature verwenden, können Sie Ihre eigene Verbraucher-URL einrichten. Wenn Sie beispielsweise Mehrfachanbieter-SSO verwenden, müssen Sie diese Eigenschaft nicht verwenden. Dieses Format der URL ist https://IhreInstanz.service-now.com/consumer.do
Breite des Popup-Dialogfelds für Authentifizierung	Breite des Popup-Dialogfelds zur Authentifizierung. Dieses Feld wird automatisch auf 800festgelegt.
Höhe des Popup-Dialogfelds für Authentifizierung	Höhe des Popup-Dialogfelds für die Authentifizierung. Dieses Feld wird automatisch auf 900festgelegt.

9. **Wahlweise:** Navigieren Sie zur Anmeldeseite der Instanz, um zu überprüfen, ob IdP als Anmeldeoption angezeigt wird.
   Die URL muss das folgende Format aufweisen: https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie „ **Als Anmeldeoption ausgewählt**“ aktiviert haben, können Sie zur Anmelde-URL der Instanz wechseln.



SAML

Die Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen.

SAML tauscht Sicherheitsinformationen zwischen einem Identitätsanbieter (Ersteller von Assertionen) und einem Service Provider (Verbraucher von Assertionen) aus. SAML ist ein Produkt des OASIS Security Services Technical Commitee. Bei korrekter Implementierung ist SAML eine der sichersten verfügbaren Methoden für Single Sign-on (SSO).

Die SAML 2.0 -Integration ermöglicht SSO durch den Austausch von XML-Token mit einem externen Identitätsanbieter (IdP). Der IdP authentifiziert den Benutzer und übergibt ein NameID-Token an das System. Wenn das System einen Benutzer mit einem übereinstimmenden NameID-Token findet (z. B. die E-Mail-Adresse), meldet die Instanz diesen Benutzer an.

Wenn Sie das SAML 2.0-Plugin für die SSO-Authentifizierung verwenden, müssen Sie die Eigenschaft glide.ui.rotate_sessions auf false setzen. Andernfalls wird die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigt. Benutzer mit der erhöhten Berechtigung security_admin können auf diese Eigenschaft zugreifen.

Hinweis:
Kunden, die eine vorhandene SAML 2.0-Integration verwenden, wird ein Upgrade auf das Multi-Provider-SSO-Plugin empfohlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren und richten Sie SAML 2.0 ein

SAML 2.0 wird über das Plugin „Integration – Multiple Provider Single Sign-On Installer“ aktiviert.

Vorbereitungen

Hinweis:

Erforderliche Rolle: admin

Aktivieren Sie das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“, um die SAML 2.0-Authentifizierung einzurichten. Verweisen Sie auf dieses Plugin, wenn Sie aufgefordert werden, den Plugin-Namen zu suchen und darauf zu klicken.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:

Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Systemeigenschaften des Identitätsanbieters (IdP).

Ein IdP bietet im Allgemeinen ein XML-Dokument mit seinen Authentifizierungs- und Abmeldemetadaten.

Zum Beispiel veröffentlicht SSOCircle seine Metadaten online.

Durchsuchen Sie die IdP-Metadaten, um diese Einträge zu finden:

- Das SingleSignOnService -Element mit einem Attribut „ Binding “, das den Wert HTTP-Redirectenthält. Das Standortattribut listet die URL auf, die die Integration für den AuthnRequest-Service benötigt.
- Das SingleLogoutService -Element mit einem Bindungsattribut, das den Wert HTTP-Redirectenthält. Das Location -Attribut listet die URL auf, die die Integration für den SingleLogoutRequest-Service benötigt.

Hinweis:

Die SAML 2.0-Integration unterstützt nur die Bindung an IdP-Services über HTTP-Umleitung.

Beispiel:

```
<SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
```

```
<SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"ResponseLocation="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
```

Legen Sie die IdP-Aussteller-URL fest

Geben Sie die URL an die IdPs weiter, die das Sicherheitstoken ausstellen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Integration überprüft, ob jede SAML-Antwort dieselbe URL enthält, die in dieser Systemeigenschaft aufgeführt ist, wie die URL, die im *Ausstellerelement* aufgeführt ist. Beispiel:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
     ...
  </saml:Assertion></samlp:Response>
```

Prozedur

1. Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**.
2. In der Eigenschaft *„Identitätsanbieter-URL“, die das SAML2-Sicherheitstoken mit Benutzerinformationen ausgibt.*, geben Sie die URL zu Ihrem IdP ein.

   Jede IdP-URL muss eindeutig sein. Standardmäßig enthält die Integration die URL zu SSOkreisel. Weitere Informationen finden Sie unter http://idp.ssokreisle.com .

Legen Sie die AuthnRequest-Service-URL fest

Legen Sie mithilfe der Metadaten des IdP die Anforderungsservice-URLs für den IdP der Integration fest.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. In der Eigenschaft *Die Basis-URL zum AuthnRequest-Service des Identitätsanbieters. Die AuthnRequest wird an diese URL als SAMLRequest-Parameter*gesendet. Geben Sie die URL für die HTTP-Redirect-Bindung ein, die vom SingleSignOnService -Element abgerufen wurde.
2. Aktivieren Sie das Kontrollkästchen neben *AuthnRequest signieren*, um den Single Sign-on-Service des Identitätsanbieters für den Empfang einer signierten AuthnRequest zu aktivieren.
3. In der Eigenschaft *Wenn das Single Sign-on für SAML 2.0 fehlschlägt, weil die Sitzung nicht authentifiziert ist oder dies die erste Anmeldung ist, wird zu dieser URL umgeleitet. Dies ist die Basis-URL, an die die*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

*anfängliche SAML 2.0 AuthnRequest mit dem SAMLRequest-Parameter*gesendet wird. Geben Sie die URL für die HTTP-Redirect-Bindung ein, die vom SingleSignOnService -Element abgerufen wurde.

Standardmäßig enthält die -Integration die URL zum SSOCircle-Service.

Legen Sie die SingleLogoutRequest-Service-URL fest

Legen Sie die Anforderungsservice-URLs für den IdP der Integration mithilfe der Metadaten des IdP fest.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. In *Die Basis-URL zum SingleLogoutRequest-Service des Identitätsanbieters. Die LogoutRequest wird an diese URL als SAMLRequest-Parameter* gesendet. Geben Sie die URL ein, die aus dem SingleLogoutService- Element abgerufen wurde.
   Die LogoutRequest wird als SAMLRequest-Parameter an diese URL gesendet. Standardmäßig enthält die -Integration die URL zum SSOCircle-Service.
2. Geben Sie in der *URL für die Weiterleitung von Benutzern nach der Abmeldung, in der Regel zurück zum Portal, das SSO aktiviert hat (z. B. http://portal.companya.com/logout)*, die URL ein, an die Benutzer nach der erfolgreichen Abmeldung weitergeleitet werden sollen.

   Wenn Ihr IdP die formularbasierte Authentifizierung verwendet, geben Sie die URL zum Anmeldeformular Ihres IdP ein. Wenn Ihr IdP eine nicht formularbasierte Authentifizierungsmethode wie Kerberos verwendet, sollten Sie die URL auf eine statische Abmeldeseite festlegen. Auf diese Weise werden Benutzer, die sich abmelden, nicht sofort zum IdP umgeleitet und melden sich erneut an. Standardmäßig enthält die Integration die URL zur statischen UI-Seite external_logout_complete.do.

(Optional) Aktivieren Sie signierte Abmeldeanforderungen

Einige IdPs erfordern, dass der Service Provider Abmeldeanforderungen mit einem Zertifikat signiert.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn für Ihren IdP signierte Abmeldeanforderungen erforderlich sind, verwenden Sie die Metadaten des IdP, um die folgenden Systemeigenschaften festzulegen.

Prozedur

1. Auf der Registerkarte „ **Erweitert** “ aus der Eigenschaft *LogoutRequest signieren. Legen Sie diese Eigenschaft auf „true“ fest, wenn der SingleLogoutRequest-Service des Identitätsanbieters eine signierte LogoutRequest*erfordert. Wählen Sie **Ja**, um anzugeben, dass Ihr IdP eine signierte Abmeldeanforderung erfordert, oder wählen Sie **Nein**, um nicht signierte Abmeldeanforderungen zu verwenden.
2. Wenn Sie **Ja** zum Signieren von *LogoutRequest*ausgewählt haben, dann in *Die Protokollbindung für den SingleLogoutRequest-Service des Identitätsanbieters. (Wert kann entweder „urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect“ oder „urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST“ sein.)* -Eigenschaft, Geben Sie einen der unterstützten Werte ein, die im Bindungsattribut aus dem SingleLogoutService- Element aufgeführt sind.

   Standardmäßig verwendet die Integration eine HTTP-Redirect-Bindung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Aktualisieren**.
4. Installieren Sie einen Service Provider-Schlüsselspeicher (SP).

Systemeigenschaften des Service Providers (SP).

Diese Systemeigenschaften definieren, wie die Instanz mit dem IdP als Service Provider interagiert.

Befolgen Sie den sequenziellen Prozess, um IdP als Service Provider zu definieren.

Legen Sie die Instanz-URL für SAML fest

Legen Sie die instanzspezifischen URLs fest, damit der IdP Benutzer authentifizieren kann.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Geben Sie in der Eigenschaft *URL zur ServiceNow-Instanz (normalerweise diese Instanz)*die URL (einschließlich Anmeldeseite) der Instanz ein, für die sich der IdP authentifiziert.
   Beispiel: https://IhreInstanz.service-now.com/navpage.do
2. Geben Sie in der Eigenschaft *Die Entitätsidentifizierung oder der Aussteller*die Basis-URL (ohne Anmeldeseite) der Instanz ein, für die sich der IdP authentifiziert.
   Beispiel: https://IhreInstanz.service-now.com/

Legen Sie die Zielgruppen-URL für SAML fest

Aktivieren Sie Ihre Instanz, um mithilfe der Eigenschaft „Zielgruppe“ zu überprüfen, ob sie der beabsichtigte Empfänger einer SAML-Antwort ist.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Integration überprüft, ob jede SAML-Antwort dieselbe URL enthält, die in dieser Systemeigenschaft aufgeführt ist, wie die URL, die im *Zielgruppenelement* aufgeführt ist. Beispiel:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
...
</samlp:Response>
```

Prozedur

1. Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**.
2. In der Eigenschaft *die Zielgruppen-URI, die das SAML2-Token akzeptiert. (Normalerweise ist dies Ihr Instanz-URI. Beispiel: https://<instance name> .service-now.com.)*, geben Sie die URL Ihrer Instanz ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: https://demoi2.service-now.com. Diese URL muss mit dem Wert des *Zielgruppenelements* in der SAML-Antwort übereinstimmen.

3. Klicken Sie auf **Aktualisieren**.

Richten Sie eine NameID-Richtlinie für SAML ein

Richten Sie eine NameID-Richtlinie für SAML ein. SAML 2.0 erfordert, dass der IdP ein NameID-Token mit dem Service Provider austauscht.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Für die SAML 2.0-Integration muss das NameID-Token einem bestimmten Feld in der Benutzertabelle zugeordnet werden. Die Integration verwendet den Wert des NameID-Tokens, um zu bestimmen, welchen Benutzer der IdP authentifiziert.

Prozedur

1. Durchsuchen Sie die IdP-Metadaten, um das `NameIDFormat-` Element zu finden, das den Wert `emailAddress`enthält.
   Der Wert dieses Elements ist das Standardformat, das die Integration verwendet.
2. Überprüfen Sie andere `NameIDFormat-` Elemente, um festzustellen, ob Formate vorhanden sind, die anderen Feldern in der Benutzertabelle entsprechen.

Bestimmen Sie, welches Benutzertabellenfeld dem NameID-Token entspricht

Identitätsanbieter geben an, welches Format das `NameID-` Token hat.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Zum Einrichten von SAML 2.0 muss ein Feld aus der Benutzertabelle ausgewählt werden, das dem Format des `NameID-` Tokens entspricht. Normalerweise bieten IdPs die Möglichkeit, eine E-Mail-Adresse als `NameID-` Token zu verwenden. Da die Benutzertabelle ein E-Mail-Feld enthält, ist dieses Feld eine logische Wahl für die Verwendung als `NameID-` Token. Um ein anderes Feld aus der Benutzertabelle als `NameID-` Token zu verwenden, stellen Sie zuerst sicher, dass der IdP ein `NameID` -Format anbietet, das dem Wert eines Benutzertabellenfelds entspricht. Dazu muss das Feld möglicherweise der Benutzertabelle hinzugefügt werden.

Prozedur

1. Vergleichen Sie die verfügbaren Formate im `NameIDFormat` -Element des IdP mit Feldern in der Benutzertabelle.
2. Wählen Sie ein `NameID` -Format aus, bei dem in der Benutzertabelle ein übereinstimmender Wert vorhanden ist.
3. Geben Sie im Feld *Benutzertabelle, das mit dem NameID-Element des Antragstellers im Feld SAMLResponse abgeglichen* werden soll, den Namen des Felds Benutzertabelle ein, um nach übereinstimmenden Werten im `NameID-` Token zu suchen.

   Standardmäßig verwendet die Integration das E-Mail-Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die IdP-NameID-Richtlinie fest

Geben Sie an, welches Format der IdP für das NameID- Token verwendet.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Dieses Format wird als Teil der Metadaten des IdP aufgeführt.

Prozedur

1. In der Eigenschaft *Die NameID-Richtlinie, die für die Rückgabe der NameID des Antragstellers in der SAMLResponse verwendet werden soll. Ihr SAML-Identitätsanbieter muss dies unterstützen, indem er die Richtlinie in seinen Metadaten deklariert. Der Wert NameID wird mit dem angegebenen Feld in der Benutzertabelle abgeglichen, um den Benutzer zu suchen.*, geben Sie den Wert des NameIDFormat- Elements ein, das die Integration verwendet.

   Standardmäßig verwendet die Integration für E-Mail-Adressen das NameID-Format des SSO-Kreis.

2. Klicken Sie auf **Speichern**.

Werte im Feld Benutzertabelle für SAML

Stellen Sie sicher, dass das Feld Benutzertabelle der Integration die entsprechenden übereinstimmenden Werte enthält.

Wenn die Integration beispielsweise das E-Mail-Feld als NameID- Token verwendet, stellen Sie sicher, dass die Instanz dieselbe E-Mail-Adresse wie der IdP auflistet. Die Integration kann keinen Benutzer authentifizieren, der keinen übereinstimmenden Wert für das NameID- Token hat.

(Optional) Aktivieren Sie die Bereitstellung einer Authentifizierungskontextklasse für SAML

Sie können die Instanz aktivieren, um eine Authentifizierungskontextklassenanforderung an den IdP zu senden, die das bevorzugte Authentifizierungsanforderungsformat Ihrer Instanz enthält.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie die Erstellung einer AuthContextClass-Nachricht aktivieren, müssen Sie auch ein Referenzformat für die Authentifizierungskontextklasse angeben.

Hinweis:
Einige IdPs erlauben es dem Service Provider nicht, die Authentifizierungskontextklasse festzulegen. Durch Deaktivieren dieser Einstellung kann der IdP die Authentifizierungskontextklasse auswählen.

Prozedur

1. Wählen Sie in der Eigenschaft *AuthnContextClass-Anforderung erstellen in der AuthnRequest-Anweisung die Option***Ja** aus, um eine bestimmte Kontextklasse anzugeben, z. B. Passwortgeschützte Übertragung, oder wählen Sie **Nein**, damit der IdP die am besten geeignete Kontextklasse auswählt.

2. Wenn Sie **Ja** zum *Erstellen einer AuthnContextClass-Anforderung in der AuthnRequest-Anweisung*ausgewählt haben, geben Sie in *der AuthnContextClassRef-Methode, die in unserer SAML 2.0*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AuthnRequest-Eigenschaft an den Identitätsanbieter angefordert wird, die URN der Kontextklasse ein, die Sie für die Authentifizierung verwenden möchten (siehe Tabelle).).

AuthnContextClass URN-Optionen

Authentifizierungstyp	URN der Authentifizierungskontextklasse
Formularbasierte Authentifizierung	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Kerberos-basierte Authentifizierung	urn:federation:authentication:windows

Standardmäßig verwendet die Integration eine PasswordProtected Transport-Authentifizierungsmethode.

3. Klicken Sie auf **Aktualisieren**.

(Optional) Legen Sie Schlüsselspeicher-Eigenschaften für das Signieren von Abmeldeanforderungen für SAML fest

Legen Sie die Schlüsselspeicher-Eigenschaften fest, damit die Integration Abmeldeanforderungen mithilfe Ihres signierten Servers und signierter CA-Zertifikate signieren kann.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Geben Sie in der Eigenschaft *Alias der im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleingabe zum Signieren von SAML 2-Anforderungen*den Aliasnamen ein, den Sie für den SAML 2.0-Schlüsselspeicher erstellt haben.
   Standardmäßig sucht die Integration nach dem Alias *saml2sp*.
2. Geben Sie in der Eigenschaft *Das Passwort der im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleingabe zum Signieren von SAML 2-Anforderungen*das Passwort für Ihren SAML 2.0-Schlüsselspeicher ein.
   Standardmäßig stimmt das Passwort mit dem Standardaliasnamen überein.
3. Klicken Sie auf **Aktualisieren**.
4. Generieren Sie Ihre SP-Metadaten erneut.
   Weitere Informationen finden Sie unter SP-Metadaten.

Erstellen Sie einen Service Provider-Schlüsselspeicher für SAML

Damit Ihre Instanz Abmeldeanforderungen signieren kann, müssen Sie einen Java-Schlüsselspeicher erstellen, der die folgenden Elemente enthält.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

- Signiertes Serverzertifikat für die Instanz
- Signiertes CA-Zertifikat
- Öffentliches und privates Schlüsselpaar

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Ihr eigenes signiertes Zertifikat bei einer privaten Zertifizierungsstelle erstellen oder eines von einer öffentlichen Zertifizierungsstelle erwerben.

Die folgenden Schritte zeigen, wie Sie eine neue Java Keytool-Schlüsselspeicherdatei generieren, eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) erstellen und Zertifikate importieren. Alle Stamm- oder Zwischenzertifikate müssen importiert werden, bevor das primäre Zertifikat für Ihre Domäne importiert wird. Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein.

Hinweis:
Diese Anweisungen sind nicht spezifisch für die Plattform und erfordern technische Kenntnisse über Sicherheitszertifikate. Der technische Support kann bei der Erstellung der Zertifikate nicht helfen.

Prozedur

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Importieren Sie ein CA-Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. Importieren Sie ein signiertes primäres Zertifikat in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

Installieren Sie einen Service Provider-Schlüsselspeicher zum Signieren von SAML-Anforderungen

Führen Sie die folgenden Schritte aus, um den vorhandenen Beispielschlüsselspeicher zu entfernen und Ihren eigenen Service Provider-Schlüsselspeicher zu installieren, der Ihr öffentliches und privates Schlüsselpaar enthält.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie einen Service Provider-Schlüsselspeicher.
2. Navigieren zu **SAML 2 Single Sign-on** > **Zertifikat** oder **Mehrfachanbieter** > **Administrator** > **x509-Zertifikat**.
3. Klicken Sie **auf SAML 2.0 Keystore_Key2048_SHA256**.
4. Klicken Sie auf den Link **Anhänge verwalten**.
5. Aktivieren Sie das Kontrollkästchen Löschen neben *saml2sp_key2048withsha256.jks*.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **Dateien** wählen, und wählen Sie den Schlüsselspeicher aus, der Ihre signierten Zertifikate enthält.
8. Klicken Sie auf **Anhängen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Schließen Sie das Popup „Anhänge“.

Hinweis:
Es wird empfohlen, einen anderen Namen für das neu angehängte Zertifikat anzugeben.

10. Geben Sie im Feld Passwort des *Schlüsselspeichers*das Passwort für den Zugriff auf den SAML 2-Alias ein.
11. Klicken Sie auf **Aktualisieren**.

(Optional) Erweiterte SAML-Eigenschaften

Mit den folgenden erweiterten Einstellungen können Sie die Sicherheit weiter erhöhen und die Integration debuggen.

Erweiterte Einstellungen

Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**.

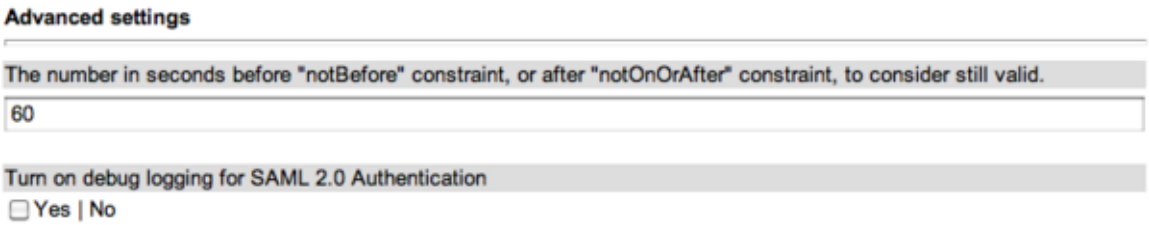


Tabelle „Erweiterte Systemeigenschaften“.

Eigenschaft	Beschreibung
Die Anzahl der Sekunden der Einschränkung „notBefore“ oder nach der Einschränkung „notOnOrAfter“, die als noch gültig betrachtet werden sollen	Geben Sie die Anzahl der Sekunden ein, die den Einschränkungen *NotBefore* und *NotOnOrAfter* hinzugefügt werden sollen, um Zeitunterschiede zwischen der IdP-Uhr und der SP-Uhr zu berücksichtigen. Diese Einschränkungen verhindern Wiederholungsangriffe, indem Anforderungen abgelehnt werden, die nicht innerhalb des angegebenen Zeitrahmens gestellt werden. Wenn sich die IdP-Uhr und die SP-Uhr erheblich unterscheiden, kann die Netzwerklatenz dazu führen, dass die SAML-Anforderung nicht autorisiert ist. Diese Eigenschaft fügt eine Toleranzfrist hinzu, während der SAML-Anforderungen und -Antworten noch als gültig betrachtet werden.
Debug-Protokollierung für SAML 2.0-Authentifizierung aktivieren	Wählen Sie **Ja** aus, um zusätzliche Protokollierungsinformationen für SAML 2.0-Events zu aktivieren.

Installieren Sie das Zertifikat des Identitätsanbieters

Sie können ein PEM-Zertifikat in ein X.509-Zertifikatformular einfügen, damit der Identitätsanbieter die Kommunikation mit dem Service Provider überprüfen kann.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

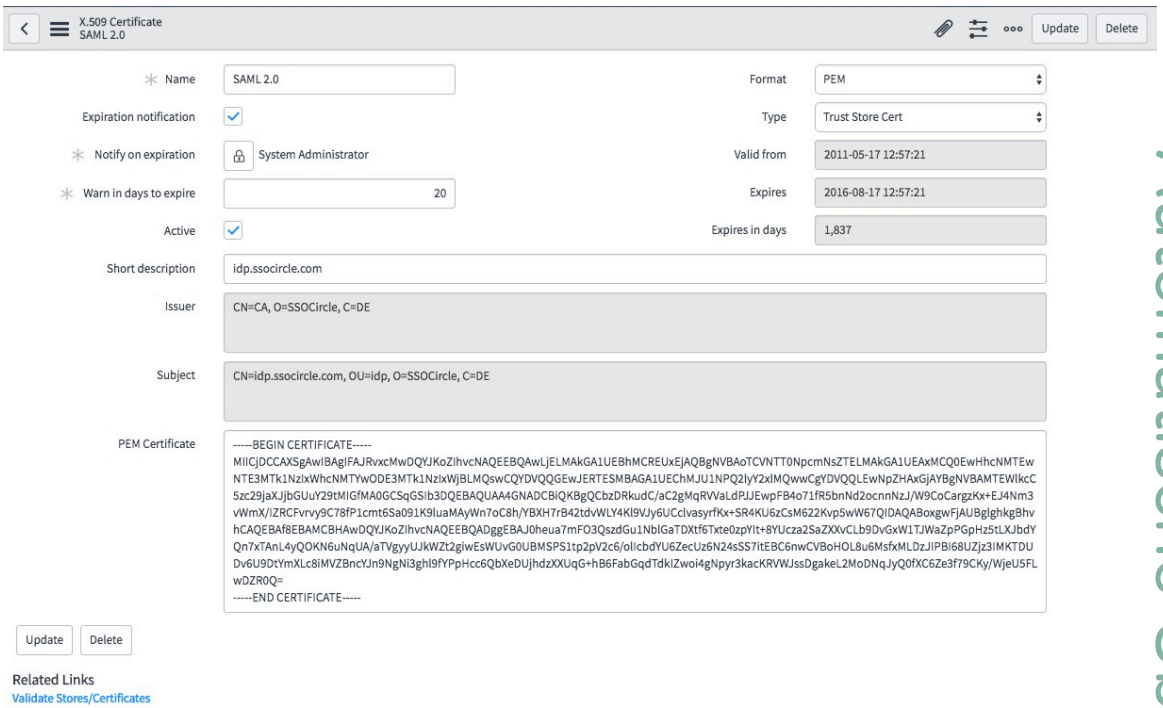
Das Zertifikat des IdP befindet sich in den Metadaten des IdP. Der IdP-Entwickler bestimmt, wo sich die Zertifikatmetadaten befinden, wenn er den lokalen IdP erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Zertifikate für Single Sign-on müssen immer im PEM-Format vorliegen, damit sie mit SAML-Zertifikaten funktionieren.

Prozedur

1. Navigieren zu **Alle** > **SAML Single Sign-on** > **Zertifikat**.
2. Füllen Sie die Formularfelder aus (siehe Tabelle).
3. Klicken Sie auf **Speichern**.



Hinweis:
Die Integration signiert derzeit das Zertifikat in der Kommunikation zwischen der Instanz und dem IdP nicht.

Feld	Beschreibung
Name	Der Zertifikatname. Ändern Sie den Eintrag *Name* nicht. Der Name des X.509-Zertifikats muss *SAML 2.0* lauten, damit die Integration es verwenden kann. Diese Anforderung ist nur erfüllt, wenn Sie Single Sign-on (SSO) für mehrere Anbieternicht verwenden.
Ablaufbenachrichtigung	Wählen Sie diese Option aus, um eine Benachrichtigung an die Benutzer zu senden, die im Feld Bei **Ablauf benachrichtigen** ausgewählt sind. Standardmäßig ist diese Option aktiviert.
Benachrichtigung bei Ablauf	Wählen Sie die Benutzer aus, die die Benachrichtigung über den Ablauf des Zertifikats erneut aktivieren sollen. Wenn keine Benutzer ausgewählt sind, wird standardmäßig der angemeldete Benutzer zusammen mit den letzten beiden angemeldeten Benutzern mit der Administratorrolle hinzugefügt.
Tage vor Ablauf benachrichtigen	Die Anzahl der Tage vor Ablauf, an denen die Instanz die Benachrichtigung sendet. Geben Sie einen Wert von mindestens 20 ein. Für Instanzen, die auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Istanbul und spätere Releases aktualisiert wurden, wird dieser Wert auf 20 festgelegt, sofern kein höherer Wert angegeben ist.
Aktiv	Eine Checkbox, die angibt, dass dieses Zertifikat aktiv ist.
Format	Das Format des Zertifikats. SAML verwendet das **PEM** -Format.
Typ	Der Zertifikatcontainer. Die Instanz erkennt Zertifikate aus Truststores, Java-Schlüsselspeichern und PKCS#12-Schlüsselspeichern.
Gültig ab	Die Instanz fügt diesem Feld automatisch das Zertifikat „Gültig ab“-Datum hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft ab	Die Instanz fügt diesem Feld automatisch das Zertifikat-Ablaufdatum hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft in Tagen ab	Die berechnete Anzahl von Tagen bis zum Ablauf.
Kurzbeschreibung	Eine Beschreibung für das Zertifikat.
Vorfall	Die Instanz fügt den Zertifikataussteller automatisch diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Betreff	Die Instanz fügt den Antragsteller des Zertifikats automatisch diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
PEM-Zertifikat	Geben Sie den Wert des X509-Zertifikats ein.

Nächste Maßnahme
Klicken Sie auf **Speicher/Zertifikate validieren**, um den Truststore und das Zertifikat zu testen.

Ersetzen eines fehlenden Zertifikats für SAML

Wenn das **Zertifikatmodul** eine leere Seite anzeigt, wurde der SAML 2.0-Zertifikatdatensatz gelöscht. Sie können das fehlende Zertifikat ersetzen, indem Sie manuell einen Zertifikatdatensatz erstellen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**.
2. Erstellen Sie einen neuen Datensatz mit dem Namen `SAML 2.0`.

> **Wichtig:**
> Sie MÜSSEN diesen Namen verwenden. Diese Anforderung ist nur erfüllt, wenn Sie Single Sign-on (SSO) für mehrere Anbieternicht verwenden.

3. Klicken **SAML 2 Single Sign-on** > **Zertifikat**.
4. Geben Sie im Feld *PEM-Zertifikat* den Wert des `ds:X509Certificate-` Elements aus den Metadaten Ihres IdP ein.
5. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren Sie einen Service Provider-Schlüsselspeicher zum Signieren von SAML-Anforderungen

Führen Sie die folgenden Schritte aus, um den vorhandenen Beispielschlüsselspeicher zu entfernen und Ihren eigenen Service Provider-Schlüsselspeicher zu installieren, der Ihr öffentliches und privates Schlüsselpaar enthält.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie einen Service Provider-Schlüsselspeicher.
2. Navigieren zu **SAML 2 Single Sign-on** > **Zertifikat** oder **Mehrfachanbieter** > **Administrator** > **x509-Zertifikat**.
3. Klicken Sie **auf SAML 2.0 Keystore_Key2048_SHA256**.
4. Klicken Sie auf den Link **Anhänge verwalten**.
5. Aktivieren Sie das Kontrollkästchen Löschen neben *saml2sp_key2048withsha256.jks*.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **Dateien** wählen, und wählen Sie den Schlüsselspeicher aus, der Ihre signierten Zertifikate enthält.
8. Klicken Sie auf **Anhängen**.
9. Schließen Sie das Popup „Anhänge“.

Hinweis:
Es wird empfohlen, einen anderen Namen für das neu angehängte Zertifikat anzugeben.

10. Geben Sie im Feld Passwort des *Schlüsselspeichers*das Passwort für den Zugriff auf den SAML 2-Alias ein.
11. Klicken Sie auf **Aktualisieren**.

Testen Sie die SAML-Integration

Testen Sie die SAML-Integration, nachdem Sie alle anderen Setup-Aufgaben abgeschlossen haben.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Melden Sie sich bei der Instanz als Benutzer mit der Administratorrolle an.
2. Navigieren zu **SAML 2 Single Sign-on** > **Eigenschaften**.
3. Wählen Sie in der Eigenschaft *Externe Authentifizierung aktivieren*die Option **Ja**aus.

Hinweis:

Wenn Sie die externe Authentifizierung aktivieren, müssen alle Benutzer SAML 2.0 Single Sign-on verwenden. Wenn jemand versucht, ohne Authentifizierung auf die Anwendung zuzugreifen, sendet die Instanz automatisch eine Authentifizierungsanforderung an den (IdP) und leitet den Benutzer zur SAML-IdP-Authentifizierungsseite um.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Speichern**.
5. Melden Sie sich von der Instanz ab.
6. Navigieren Sie zur Instanz-URL.
   Wenn die Integration ordnungsgemäß funktioniert, sollte der IdP die Anmeldeinformationen des Benutzers anfordern.

Zugehörige Informationen

Multi-SSO (SAML 2.0) – Fehler und Korrekturen

Multi-SSO (SAML 2.0) – Fehler und Korrekturen

Eine Liste der häufigsten Fehler und zugehörigen Korrekturen für das Setup und die Konfiguration von Multi-SSO (SAML 2.0).

Fehler beim Setup von Multi-SSO (SAML 2.0).

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
NotAfter:<Thu Jun 05 22:57:44 PDT 2014> .	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist.	N/V	Das aktuelle Zertifikat oder die SAML-Assertion ist abgelaufen.	• Synchronisieren Sie die SNC-Uhr mit der SAML-IdP-Serveruhr. • Aktualisieren Sie den SAML 2.0-Zertifikatdatensatz.
• SAML 2.0-Zertifikat wurde nicht gefunden. • In der ServiceNow-Instanz gespeicherte digitale Signatur wurde nicht gefunden.	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist	Die PEM-formatierte Zeichenfolge muss in das Feld PEM-Zertifikat eingegeben werden.	Das SAML-Zertifikat ist nicht vorhanden. Er ist möglicherweise inaktiv.	Stellen Sie sicher, dass das richtige PEM-formatierte Zertifikat in die Instanz hochgeladen wird.
Zertifikate stimmen nicht überein. Erwartet:<certStr> , Istwert:<inboundCert> .	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist.	N/V	Das in SNC verfügbare Zertifikat stimmt nicht mit dem Zertifikat in der Assertion überein. Zu den Ursachen gehören: • Das Zertifikat wird auf dem IdP aktualisiert, aber nicht in der	Bestätigen Sie, dass die PEM-formatierte Zeichenfolge im Datensatz des SAML 2.0-Zertifikats mit dem X509-Zertifikat in der SAMLResponse für den Benutzer-IdP übereinstimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
			ServiceNow-Instanz. • Das Zertifikat weist das falsche Format auf.	
Fehler beim Überprüfen der Gültigkeit des Zertifikats.	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist	N/V	Das aktuelle Zertifikat ist möglicherweise abgelaufen.	Aktualisieren Sie den SAML 2.0-Zertifikatdatensatz.
Fehler beim Validieren des Signaturprofils.	Stellen Sie sicher, dass das x509-Zertifikat des IdP vorhanden, gültig und aktiv ist.	N/V	Die Assertion ist möglicherweise mit einem anderen Zertifikat signiert.	Überprüfen Sie, ob der IdP dasselbe Zertifikat wie die SNC-Instanz hat.
Attribut „InResponseTo“ in „SubjectConfirmationData“ stimmt nicht überein. Erwartet:<inResponseTo> , Istwert: .	Die Validierung der Antragsteller bestätigung ist fehlgeschlagen.	N/V	Dieser Fehler wird angezeigt, wenn eine der folgenden Situationen auftritt: • Der IdP gibt eine SAMLResponse für eine andere SAMLRequest zurück • Ein Benutzer setzt ein Lesezeichen für die URL mit der SAML-Anforderung anstatt nur für die Instanz-URL • Wenn ein Nullwert erwartet wird, wird die Antwort möglicherweise an einen anderen Knoten gesendet, wenn die Instanz über mehrere Knoten verfügt.	Der IdP-Administrator sollte bestätigen, dass die erwartete SAML-Antwort zurückgegeben wird. Diese Situation kann ein Problem mit dem Lastenausgleichsmodul oder der Infrastruktur sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
SessionIndex-Wert nicht gefunden:<message> ...	SessionIndex ungültig.	N/V	Der SessionIndex ist in der SNC-Instanz erforderlich. Der IdP gibt ihn in der SAML-Antwort zurück, um eine erfolgreiche Authentifizierung zu bestätigen.	Der IdP-Administrator sollte bestätigen, dass der SessionIndex in der SAMLResponse definiert ist.
Es konnte kein gültiges SubjectConfirmation-Element gefunden werden.	Die Validierung der Antragstellerbestätigung ist fehlgeschlagen.	N/V	Bedingungen könnten aufgrund eines Fehlers beim IdP fehlen. Der StatusCode in der Antwort würde Responder anstelle des erwarteten Erfolgs enthalten.	Überprüfen Sie SAMLResponse, um festzustellen, ob Bedingungen in der SAMLResponse enthalten sind. Die gültigen Betreffbestätigungsdaten sind möglicherweise abgelaufen oder nicht für die richtige Zielgruppe.
Nichtübereinstimmung der Assertionszielgruppe. Erwartet:<propAudienceURI> Istwert:<audienceUri> oder AudienceRestriction-Validierung fehlgeschlagen. Keine übereinstimmende Zielgruppe gefunden.	Stellen Sie sicher, dass das Feld „Zielgruppen-URI“ richtig festgelegt ist	Der Zielgruppen-URI, der das SAML2-Token akzeptiert. (Normalerweise ist dies Ihr Instanz-URI. Beispiel: https://demo.service-now.com.)	Der in der SNC-Instanz konfigurierte Zielgruppen-URI muss mit dem Wert im IdP übereinstimmen.	Suchen Sie<saml2:Audience> in der SAMLResponse in den Protokollen und stellen Sie sicher, dass der Wert mit dem in der Instanz übereinstimmt.
Der Aussteller der Assertion ist ungültig. Erwartet:<value on instance> , Istwert:<value returned by IdP>	Der Aussteller der Assertion ist ungültig.	Die Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit Benutzerinformationen ausgibt.	Die IdP-Entitäts-ID (Aussteller) stimmt nicht mit dem in der SNC-Instanz definierten Wert überein.	• Überprüfen Sie, ob IdP oder SP nicht ordnungsgemäß konfiguriert ist. • Vergewissern Sie sich, dass die SAML-Eigenschaft (die Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbind	SAML-Eigenschaft	Diagnose	Beheben
				Benutzerinformationen ausgibt) richtig festgelegt ist.
Betreff liegt gültig in der Zukunft. Jetzt:<now> , NotBefore:<notBefore> oder Betreff ist abgelaufen. Jetzt:<now> , NotOnOrAfter:<notOnOrAfter>	Die Bestätigung des Antragstellers ist fehlgeschlagen	Die Anzahl in Sekunden vor der NotBefore-Einschränkung oder nach der NotOnOrAfter-Einschränkung, die als noch gültig betrachtet werden soll.	Die IdP-Uhr ist nicht mit der SP-Uhr synchronisiert.	Aktualisieren Sie die SAML-Eigenschaft glide.authenticate.sso.saml2.timer auf einen größeren Wert. Der Standardwert beträgt 180 Sekunden. Einige Fälle erfordern eine Einstellung von 300 oder höher. Möglicherweise müssen Sie auch die Zeit auf Ihrem IdP-Server überprüfen.
Assertion ist in der Zukunft gültig, jetzt:<now> , notBefore:<notBefore> oder Assertion ist abgelaufen, jetzt:<now> , notOnOrAfter:<notOnOrAfter>	Assertion ist ungültig.	Die Anzahl in Sekunden vor der NotBefore-Einschränkung oder nach der NotOnOrAfter-Einschränkung, die als noch gültig betrachtet werden soll.	IdP-Uhr ist nicht mit SP-Uhr synchronisiert	Aktualisieren Sie die SAML-Eigenschaft auf einen größeren Wert. Standard: 60 Sekunden. Einige Fälle erfordern eine Einstellung von 300 oder höher. Möglicherweise müssen Sie auch die Zeit auf Ihrem IdP-Server überprüfen.

Allgemeine Anmeldungs- und IdP-Fehler

Fehler oder Symptom	Diagnose	Beheben
Anmeldeanforderungen erzeugen eine Endlosschleife zwischen dem System und dem IdP, wenn hohe Sicherheit aktiv ist.	• Normalerweise ist der URL-Endpunkt eine Fehlerseite oder Abmeldeseite. • „logout_redirect.do“ kann diese Schleife erstellen, wenn Sie *glide.security.url.whitelist* definieren, ohne den IdP-Hostnamen zum	Legen Sie die Systemeigenschaft glide.authenticate.failed_redirect fest (oder erstellen Sie sie), um fehlgeschlagene Authentifizierungsanforderungen an diese URL umzuleiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Anmeldungs- und IdP-Fehler (Fortsetzung)

Fehler oder Symptom	Diagnose	Beheben
	Eigenschaftswert hinzuzufügen. **Hinweis:** Weitere Informationen zu dieser Eigenschaft finden Sie unter URL-Allow-Liste für Abmeldeumleitungen in Härtungseinstellungen für Instanzsicherheit.	
Das zur Authentifizierung des Benutzers oder der Anforderung verwendete Token ist mit dem Signaturalgorithmus http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 signiert. Dies ist nicht der erwartete Signaturalgorithmus http://www.w3.org/2000/09/xmldsig#rsa-sha1.	Überprüfen Sie die Registerkarte Warnungskontext auf Event-Details.	Navigieren Sie zur Registerkarte „Erweitert“ des Konfigurationsdialogfelds „Relying Party Trust“, und stellen Sie sicher, dass der Algorithmus auf SHA-1 und nicht SHA-256 festgelegt ist.
Die Fehlermeldung urn:oasis:names:tc:SAML:2.0:status:Requester wird in der Systemprotokolltabelle (syslog) angezeigt.	Wenn Ihr IdP (z. B. ADFS) mit der Status oasis:names:tc:SAML:2.0:status:Requester antwortet, bedeutet dies, dass der IdP die Anmeldung aufgrund eines Problems mit der an ihn gesendeten Anforderung abgelehnt hat. Leider enthält die vom IdP erhaltene SAML-Antwort in den meisten Fällen keine weiteren Details für den Fehler.	Überprüfen Sie die an den IdP gesendete SAML-Anforderung, Recherchieren Sie mit Ihrem IdP-Administrator zusammen, um die SAML-Einstellungen Ihrer Instanz zu aktualisieren, um den Fehler zu vermeiden. Möglicherweise müssen Sie sich an Ihren IDP-Provider wenden, um den Grund für den Anmeldefehler zu erfahren.

SSO-Anmeldungen (Single Sign-on) umleiten

Wenn SSO aktiviert ist, können Sie Benutzer zu bestimmten Seiten umleiten oder Benutzer anweisen, sich lokal anzumelden.

Wenn ein Benutzer beispielsweise versucht, zu https://customerX.service-now.comzu wechseln, wird anstelle der Standardanmeldeseite möglicherweise ein internes Unternehmensportal angezeigt. Oder wenn sich ein Benutzer von einer Anwendung abmeldet, kann der Browser ihn zu einer bestimmten internen Seite umleiten. Sie können Umleitungseigenschaften innerhalb der Instanz festlegen, um sicherzustellen, dass Benutzer eine SSO-Anmeldeseite anstelle der Standardanmeldeseite sehen.

Hinweis:
Die folgenden Eigenschaften erzwingen SSO nicht. Die Seite „login.do“ ist weiterhin zugänglich, und Benutzer können sich beim System anmelden, wenn sie ein lokales Passwort festgelegt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Umleitungseigenschaften

Wenn sich ein Benutzer abmeldet oder ein Versuch fehlgeschlagen ist, sich mit SSO anzumelden, können Sie festlegen, wohin der Benutzer als nächstes weitergeleitet wird, z. B. auf eine Hauptportalseite oder einen Knowledge Base-Artikel mit SSO-Anmeldeinformationen. Verwenden Sie die folgenden Eigenschaften, um die URLs anzugeben. Wenn eine dieser Eigenschaften in Ihrer Instanz nicht vorhanden ist, können Sie die Eigenschaft erstellen.

glide.authenticate.failed_requirement_redirect

URL, um Benutzer umzuleiten, wenn sie versuchen, auf eine private Seite zuzugreifen (z. B. um einen Incident anzuzeigen) und keine SSO-Anmeldeinformationen bereitstellen. Die Eigenschaft wird normalerweise auf das Anmeldeportal eines Kunden festgelegt (z. B. `http://portal.companya.com/`).

glide.authenticate.failed_redirect

URL zur Umleitung von Anwendern nach einem fehlgeschlagenen SSO-Versuch. Sie können zu einem öffentlichen Wissensartikel umleiten, der den Fehler beschreibt und hilfreiche Links enthält (z. B. `http://portal.companya.com/error`).

glide.authenticate.external.logout_redirect

URL, um Benutzer nach dem Abmelden umzuleiten, normalerweise zurück zu dem Portal, das die Single Sign-on-Anmeldung aktiviert hat (z. B. `http://portal.companya.com/logout`).

glide.authentication.external.disable_local_login

Bei „true“ sind SSO-Anmeldeinformationen für die Hauptanmeldeseite erforderlich. Der Standardwert ist „false“. Diese Eigenschaft muss in Verbindung mit der Eigenschaft *`glide.authenticate.failed_requirement_redirect`* verwendet werden.

Die folgende Tabelle zeigt die Beziehung zwischen den Rückgabewerten des Installationsausgangs, den Eigenschaften und dem erwarteten Verhalten.

Anmeldung nur mit SSO erzwingen

Rückgabewert	Eigenschaft	Verhalten
„failed_missing_requirement“	*`glide.authenticate.failed_requirement_redirect`*	Wenn dieser Wert zurü gibt dies an, dass die er Anmeldeinformationen vorhanden sind. Die An fehl, und die Sitzung w Eigenschaft angegeben Dies ist normalerweise Provider, bei der die An und Anmeldeinformatio
„failed_authentication“	*`glide.authenticate.failed_redirect`*	Wenn dieser Wert zurü gibt dies an, dass die Au angegebenen SSO-Anm fehlgeschlagen ist, der vorhanden ist oder der ist. Die Anmeldung sch Sitzung wird an die in d angegebene URL umge normalerweise die URL Provider, bei der die An und Anmeldeinformatio

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldung nur mit SSO erzwingen (Fortsetzung)

Rückgabewert	Eigenschaft	Verhalten
<Benutzer-ID>	N/V	Anmeldung für den dur angegebenen Benutzer Dieser Wert stimmt mit überein, der in der SSO *glide.authentica* definiert ist („Feldname dem eingehenden Head soll“).

Beschränkung der lokalen Anmeldung

Aus Sicherheitsgründen sollten Sie sich auf Umleitungseigenschaften verlassen, um die lokale Anmeldung zu verhindern. Wenn sich ein Benutzer nie lokal anmelden soll und immer von Ihrem internen Single Sign-on-System authentifiziert wird, sollte jedem Benutzer, der in die Instanz importiert wird, ein zufälliges Passwort zugewiesen werden. Das zufällige Passwort wird am einfachsten beim Benutzerimport festgelegt. Wenn die Benutzerdaten über einen Importsatz in Ihr System importiert werden, können Sie mit dem folgenden Code ein onBefore-Transformationsskript erstellen.

```
var r  = new Packages. java. util. Random ( ) ;

var str1  = Packages. java. lang. Long. toString (Packages. java. lang.
Math. abs (r. nextLong ( ) ) , 36 ) ; var str2  = Packages. java. lang.
Long. toString (Packages. java. lang. Math. abs (r. nextLong ( ) ) , 36
) ;

var newPass  = str1  + str2 ;

target. user_password = newPass ;

//password now set to a random string like this:
//qvm81zdrn7cwwylpvw94eebk
```

Klonen Sie eine Instanz mit einer SAML-Integration

Klonen Sie eine Instanz mit einer SAML-Integration. Bevor Sie eine Instanz klonen, die SAML 2.0 verwendet, behalten Sie die SAML-SSO-bezogenen Einstellungen in der Zielinstanz bei, oder machen Sie den Zugriff auf die Zielinstanz unzugänglich.

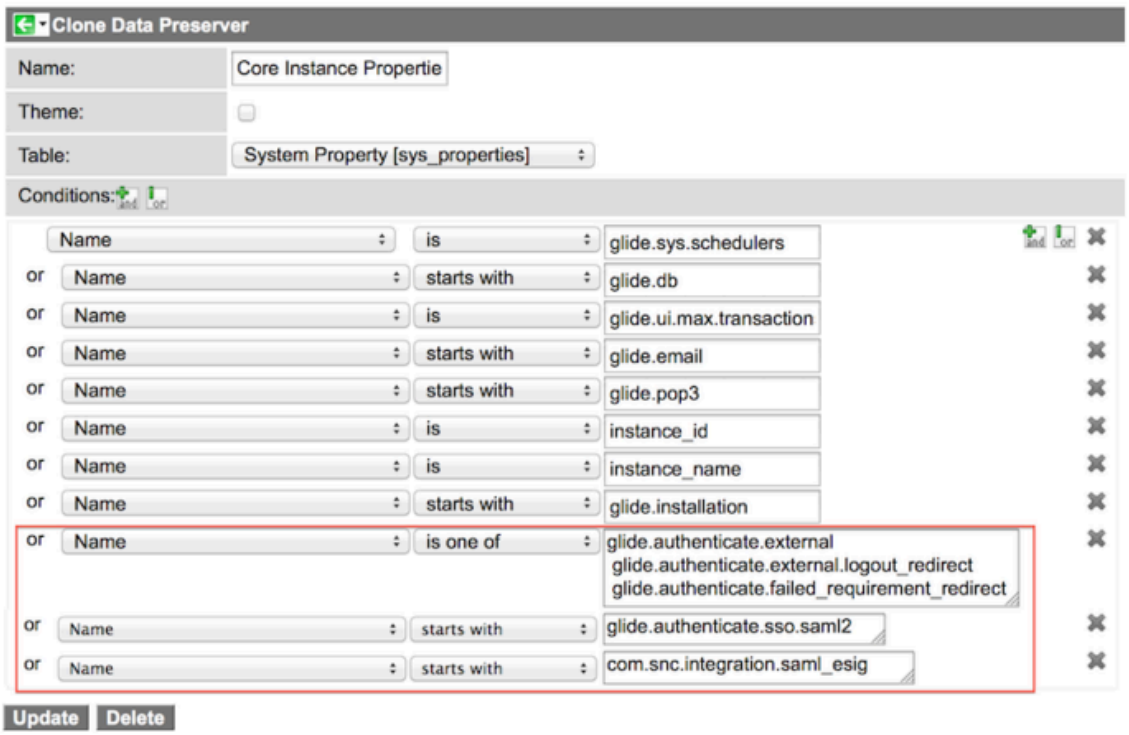
Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie in der Quellinstanz zu **Systemklon** > **Daten erhalten** > **Kerninstanzeigenschaften**.
2. Stellen Sie sicher, dass die folgenden SAML-SSO-bezogenen Eigenschaften mithilfe von Bedingungen erhalten bleiben.
   - glide.authenticate
   - glide.security
   - glide.entry
   - glide.script

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- glide.session
- glide.saml2
- com.glide.communications
- com.snc.integration.saml_esig



Hinweis:
Wenn Sie den Klon erstellen, fügen Sie Anhänge hinzu, damit Zertifikate auf die Zielinstanz übertragen werden. Stellen Sie außerdem sicher, dass die **Checkbox Thema** deaktiviert ist, damit diese Eigenschaften erhalten bleiben, unabhängig davon, ob Sie das Instanzthema beibehalten.

3. Navigieren Sie in der Quellinstanz zu **Systemklon** > **Daten erhalten** , um die SAML-Zertifikate auf sys_certificate und SAML-Benutzer auf sys_user im Zusammenhang mit SAML/SSO/Multi-SSO beizubehalten.

   Wenn Sie sie benötigen, exportieren Sie sie in XML und importieren Sie sie dann manuell auf dem Ziel.

   Warnung:
   Versuchen Sie nicht, das SAML-/SSO-/Multi-SSO-Setup von einem System auf ein anderes zu klonen. Die meisten Übertragungen von SAML/SSO- oder Multi-SSO-Einstellungen funktionieren NICHT, da sie beim Identitätsanbieter konfiguriert werden müssen. Wenn Sie ein funktionierendes Setup überschreiben, kann die Zielinstanz nicht authentifiziert werden, sodass auf Ihre Zielinstanz nicht mehr zugegriffen werden kann. Ändern Sie auch nicht die sys_id Ihres Multi-SSO-Provider-Datensatzes. Dadurch werden Ihre Benutzer gezwungen, ihre Cookies zu leeren. Weitere Informationen zu Vorsichtsmaßnahmen beim Klonen finden Sie unter Prüfliste vor dem Klonen einer Instanz .

4. Schließen Sie die Multi-SSO-Tabellen „sso_properties“, „digest_properties“ und „saml2_update1_properties“ aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Erstellen Sie die SAML-/SSO-/Multi-SSO-Datensätze für jede Instanz manuell und richten Sie die Datensätze auch für Ihren Identitätsanbieter ein.
6. Stellen Sie sicher, dass Sie manuell ein LOCAL-Administratorkonto im sys_user-Datensatz (nicht in LDAP oder SAML) in der Zielinstanz und mit einer sys_id erstellen, die in der Quellinstanz nicht vorhanden ist.
7. Klicken Sie auf **Aktualisieren**.

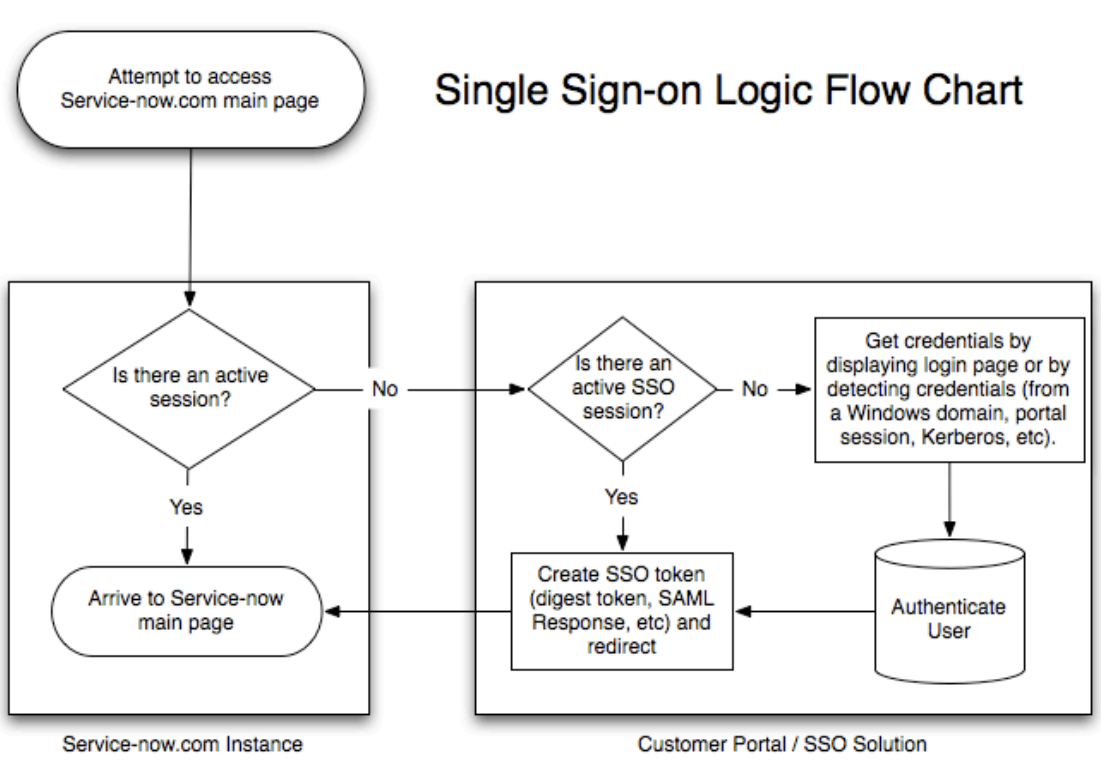
SAML 2.0-Konzepte

Machen Sie sich mit diesen SAML-Konzepten vertraut.

Typischer SAML-Prozess-Flow (Diagramm)

Ein typischer SSO-Logik-Flow umfasst die Suche nach einer aktiven Sitzung, die Überprüfung der Benutzeranmeldeinformationen und die Erstellung des erforderlichen Tokens.

SSO-Standard



Anmeldeprozess-Flow (AuthnRequest).

SAML 2.0 gibt ein Webbrowser-SSO-Profil an, bei dem Informationen zwischen einem Identitätsanbieter (IdP), einem Service Provider (SP) und einem Prinzipal (Benutzer) in einem Webbrowser ausgetauscht werden.

Der Identitätsanbieter kann ein beliebiger SSO-Service sein, der SAML-Authentifizierungsservices anbietet (z. B. SSOCircle). Der Service Provider ist immer eine Instanz. Der Nachrichtenfluss beginnt mit einer Anforderung für eine gesicherte Ressource beim Service Provider.

Fordern Sie die Zielressource beim SP an

Der Prinzipal fordert eine Zielressource beim Service Provider an:

https://instance.service-now.com/

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Instanz überprüft die Anforderung, um festzustellen, ob die URL-Parameter SAMLRequest und RelayState vorhanden sind. Wenn sie vorhanden sind, hat der Benutzer bereits eine Validierung beim IdP durchgeführt und kann die Schritte 2 bis 6 überspringen.

AuthnRequest an Identitätsanbieter ausgeben

Die Instanz erstellt eine AuthnRequest, die mit dem SAMLRequest- Wert an den IdP gesendet werden soll. Die Instanz erstellt und sendet auch einen RelayState- URL-Parameterwert.

Das RelayState- Token ist eine undurchsichtige Referenz zu Statusinformationen, die beim Service Provider verwaltet werden. Der Wert des Parameters SAMLRequest ist der dekomprimierte und base64-codierte Wert des<samlp:AuthnRequest> Element:

```
<samlp:AuthnRequest    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"    ID="identifier_1"
   Version="2.0"    IssueInstant="2004-12-05T09:21:59Z"
 AssertionConsumerServiceIndex="0"><saml:Issuer>https://
sp.example.com/SAML2</saml:Issuer><samlp:NameIDPolicy      AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/></samlp:AuthnRequest>
```

Die Integration codiert dann die URL<samlp:AuthnRequest> Element und sendet es als SAMLRequest- URL-Parameter.

Der SSO-Service verarbeitet die<samlp:AuthnRequest> Element durch URL-Decodierung, base64-Decodierung und Aufblasen der Anforderung in dieser Reihenfolge. Anschließend wird eine Sicherheitsprüfung durchgeführt. Wenn der Benutzer keinen gültigen Sicherheitskontext hat, identifiziert der IdP den Benutzer, indem er zur Eingabe von Anmeldeinformationen auffordert. Wenn der Benutzer bereits angemeldet ist, antwortet der IdP einfach mit den URL-Parametern SAMLResponse<tt> und <tt>RelayState (siehe Schritt 3).

Antworten Sie mit einer SAMLResponse und einem RelayState

Nach dem Sammeln der erforderlichen Anmeldeinformationen validiert der SSO-Service die Anforderung und antwortet mit einem Dokument, das ein XHTML-Formular enthält:

```
<formmethod="post"action="https://instance.service-now.com/navpage.do" ...><input
 type="hidden" name="SAMLResponse" value="response ..." /><input type="hidden"
 name="RelayState" value="token ..." />
   ...
   <input type="submit" value="Submit" /></form>
```

Der Wert des Parameters RelayState stammt aus diesem Schritt. Der Wert des Parameters SAMLResponse entspricht der base64-Codierung der folgenden<samlp:Response> Element:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer><samlp:Status
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><samlp:StatusCode
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode></samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="s23e536bfc51b8487d4d3299dec162d9c2e338823b"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
IssueInstant="2010-04-29T23:21:51Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#">

...
    </Signature><saml:Subject><saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        NameQualifier="http://idp.ssocircle.com"
SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml:NameID><saml:Su
bjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData
          InResponseTo="90AA6073F01567BFB0DF194F596314E2"
          NotOnOrAfter="2010-04-29T23:31:51Z"
Recipient="https://dloomac.service-now.com/navpage.do" /
></saml:SubjectConfirmation></saml:Subject><saml:Conditions
NotBefore="2010-04-29T23:11:51Z"
NotOnOrAfter="2010-04-29T23:31:51Z"><saml:AudienceRestriction><saml:Audience>http
s://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
<saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"
SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnContext><sa
ml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo
rt</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement></saml:Asse
rtion></samlp:Response>
```

Validieren Sie SAMLResponse

Der `SAMLResponse`- Wert wird base64-decodiert und erweitert, um das XML-Dokument in Schritt 3 anzuzeigen. Das Anmeldeskript extrahiert den XML-Wert aus dem Element `//Subject/NameID` und verwendet ihn, um einen vorhandenen Benutzer in der Benutzertabelle zu suchen.

Das Anmeldeskript extrahiert auch die Sitzungs-ID aus dem Element `//AuthnStatement/@SessionIndex` und speichert sie für die `LogoutRequest`.

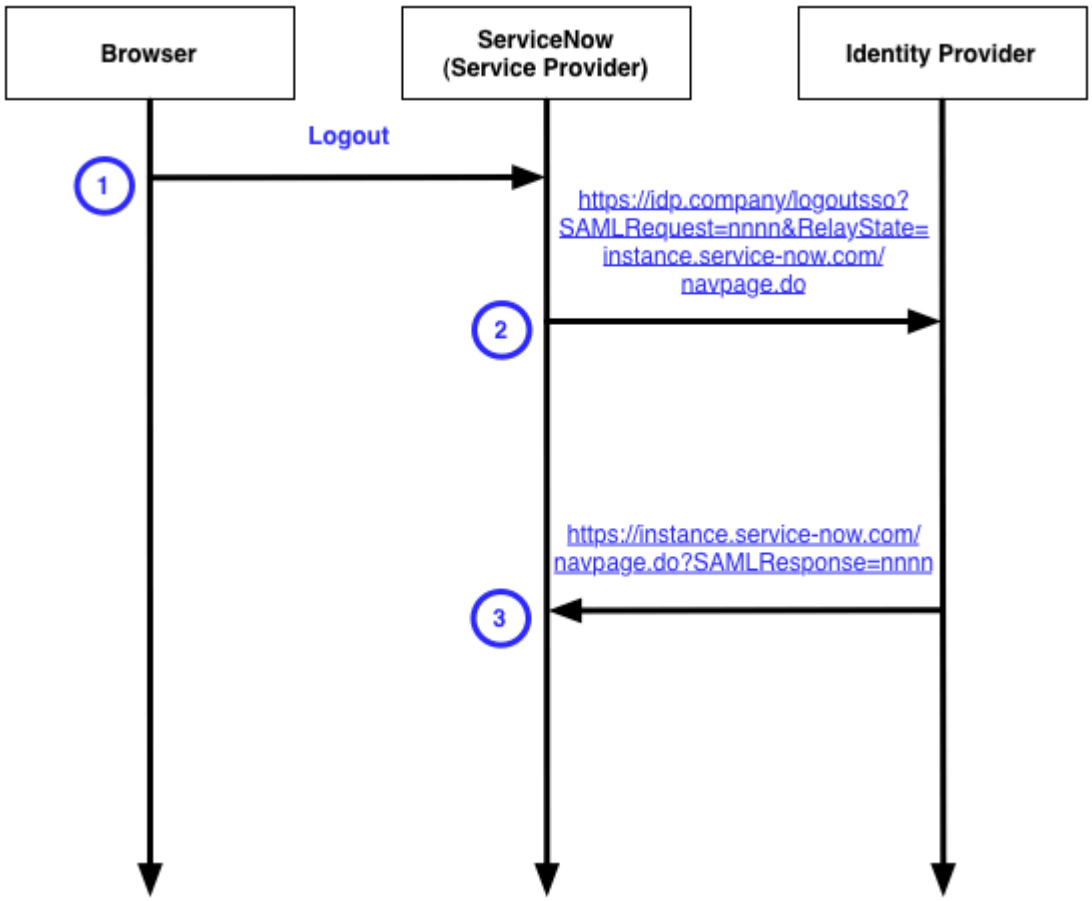
Abmeldeprozess-Flow (LogoutRequest).

Während der Abmeldung gibt die Instanz den SAML 2.0 *LogoutRequest* -Serviceaufruf an den IdP aus.

Dieser Service meldet den Benutzer ab und leitet ihn dann zurück zur angegebenen Abmelde-URL.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAML 2-Abmeldung



Benutzer klickt auf die Schaltfläche „Abmelden“.

Der Benutzer klickt auf die Schaltfläche Abmelden, und die Instanz führt das **Abmeldeskript** aus.

LogoutRequest ausgegeben

Das Abmeldeskript erstellt eine SAML 2.0 `LogoutRequest` und sendet sie an den vorkonfigurierten SingleLogoutRequest SAML 2.0-Service beim IdP. Der IdP entleert die Anforderung und codiert sie dann base64. Ein `LogoutRequest-` Beispiel sieht so aus:

```
<saml2p:LogoutRequestxmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"  IssueInstant="2010-04-28T21:36:11.230Z"
 Version="2.0"><saml2:Issuer
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://dloomac.service-now.com
 </saml2:Issuer><saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:NameID><saml2
p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

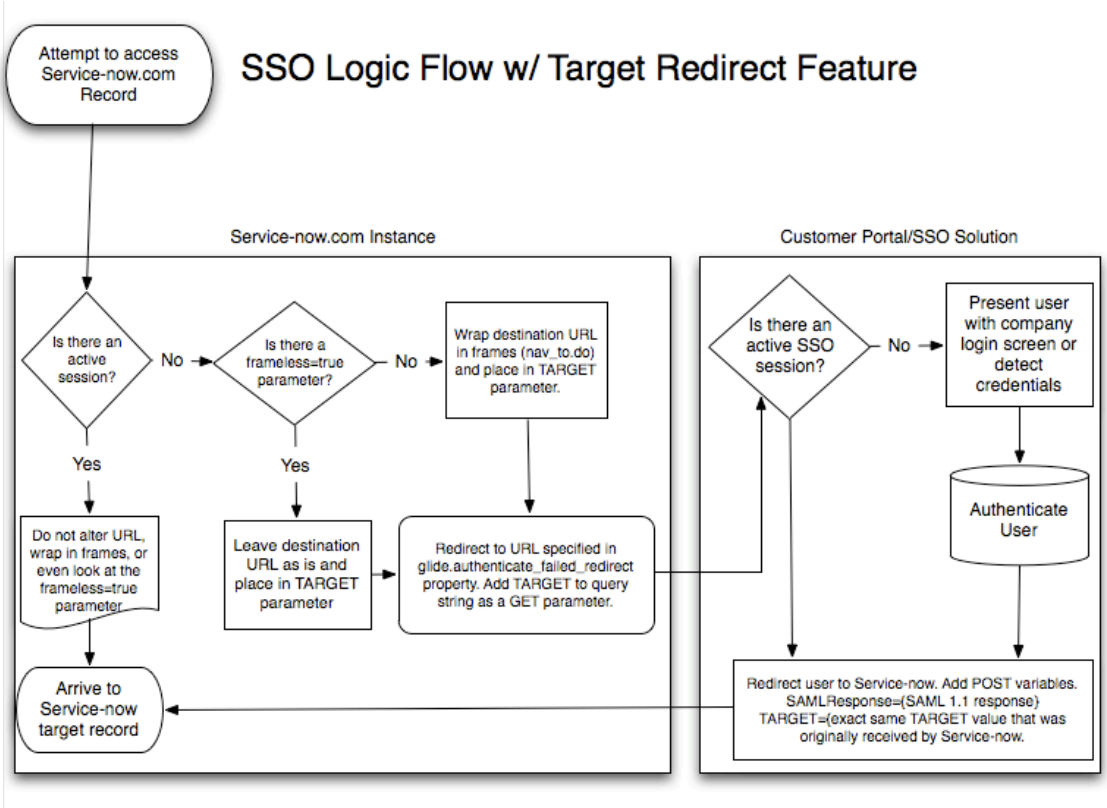
Benutzer meldet sich ab

Der Benutzer meldet sich vom IdP ab. Der IdP leitet zurück zur Instanz, die wiederum zurück zum IdP umleitet, da der Benutzer nicht angemeldet ist.

URL-Informationen für einen SSO-Provider

Während einer Anmeldeabfrage, die aus einem URL-Link zu der Instanz resultiert, die eine SSO-Sitzung erfordert, muss die verweisende URL möglicherweise an den SSO-Provider übergeben werden, damit die URL nach der Authentifizierung an die Instanz zurückgegeben und mit der richtigen Ressource verknüpft werden kann .

SSO-Zielumleitung



Die Rückgabewerte für den Installationsausgang wurden erweitert, um eine URL anstelle oder zusätzlich zu der durch die Eigenschaften definierten URL zu übergeben. Normalerweise geben Sie einen Benutzernamen oder einen vordefinierten Zeichenfolgenwert zurück, um die Autorisierung oder Abfrage der SSO-Sitzung zu steuern. Die folgenden Beispiele zeigen das erweiterte Verhalten der Übergabe einer URL.

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

Im obigen Beispiel wird die URL `https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345` in Form eines URL-Parameters mit dem Namen TARGET an den SSO-Provider übergeben.

Hinweis:
Es wird davon ausgegangen, dass der SSO-Provider diese Informationen im Parameter TARGET verwendet, um zur Instanz zurückzukehren, wenn die Benutzeranmeldeinformationen erfasst und die Authentifizierung übergeben wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Doppelpunkt : trennt die beiden Rückgabewerte, und ein codiertes & (%26amp;) verkettet die in der Eigenschaft `glide.authenticate.failed_missing_requirement` definierte URL und den Parameter TARGET.

SAML 2.0-Konfiguration mit Mehrfachanbieter-SSO

Sie können eine SAML 2.0-SSO-Konfiguration über die Multi-Provider-SSO-Funktion erstellen oder aktualisieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:

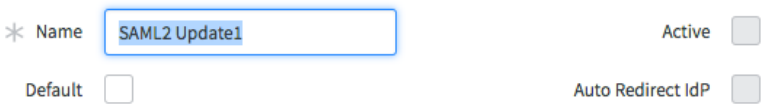
Ab Release Jakarta müssen Sie Ihre Konfiguration mithilfe der Testverbindungsfunktion validieren, bevor Sie Ihre IdP-Konfiguration aktivieren können. Sie können die Aktualisierungsfunktion weiterhin verwenden, um Ihre Konfigurationsdaten zu speichern, aber es ist keine aktive Konfiguration ohne eine erfolgreiche Testverbindung.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Sie haben folgende Möglichkeiten.
   - Um eine Konfiguration zu aktualisieren, klicken Sie auf einen SSO-Konfigurationsdatensatz.
   - Um eine neue Konfiguration zu erstellen, klicken Sie auf **Neu** > **SAML**.
3. Geben Sie für eine neue Konfiguration die IdP-Informationen mit einer der folgenden Methoden ein:

Option	Bezeichnung
Verwenden einer Metadaten-Deskriptor-URL	Klicken Sie auf das Kontrollkästchen URL, und geben Sie die URL des verwendeten IdP ein.
Verwenden der XML-Metadatendeskriptordatei	Klicken Sie auf das Kontrollkästchen XML, und fügen Sie die XML-Daten ein, die vom verwendeten IdP generiert wurden.
Metadaten manuell eingeben	Schließen Sie das Popup-Fenster, und geben Sie die Daten manuell in die Eigenschaftsfelder ein.

Alle Pflichtfelder im Formular „Identitätsanbieter“ müssen ausgefüllt werden.



Single Sign-on-Felder für mehrere Anbieter

Eigenschaft	Erforderlich	Beschreibung
Name	Ja	Geben Sie den Namen für den IdP ein. Dieser IdP ist die Sys-ID der automatischen Umleitung.
Aktiv	Ja	Aktiv muss für den IdP, der für die Authentifizierung verwendet werden soll, auf „true“ festgelegt werden.

Automatische Übersetzung

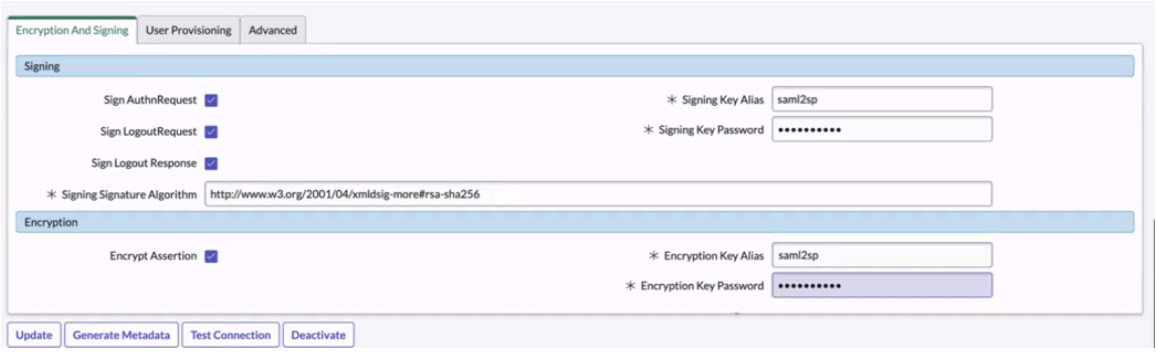
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Erforderlich	Beschreibung
		Hinweis: Die Option zum Festlegen dieser Eigenschaft ist nur nach einer erfolgreichen Testverbindung möglich.
Standard	Nein	Der IdP für die automatische Weiterleitung, früher als primärer IdP bezeichnet, leitet Benutzer automatisch zum Zugriff auf die Basisinstanz-URL um. Diese Eigenschaft legt diese IdP-Konfiguration als Standard fest.
Automatische IdP-Weiterleitung	Nein	Legt diese IdP-Konfiguration als IdP für die automatische Umleitung fest. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Weiterleitung aktivieren, wird das Cookie `glide_sso_id` mit dem neuen IdP für die automatische Weiterleitung aktualisiert. Die automatisch aktivierte Systemeigenschaft `glide.authenticate.sso.update.idp.cookie` steuert diese Funktion.
URL des Identitätsanbieters	Ja	Geben Sie die URL zu Ihrem IdP ein. Jede IdP-URL muss eindeutig sein.
AuthnRequest des Identitätsanbieters	Ja	Geben Sie die URL für die HTTP-Redirect-Bindung ein, die vom SingleSignOnService-Element abgerufen wurde.
SingleLogoutRequest des Identitätsanbieters	Nein	Geben Sie die URL ein, die aus dem SingleLogoutService-Element abgerufen wurde.
ServiceNow Homepage	Ja	Geben Sie die URL (einschließlich Anmeldeseite) der Instanz ein, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/navpage.do
Entitäts-ID/Aussteller	Ja	Geben Sie die Basis-URL ohne Anmeldeseite ein. der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
Zielgruppen-URI	Ja	Geben Sie die Basis-URL ohne Anmeldeseite ein. der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
NameID-Richtlinie	Ja	Geben Sie den Wert des NameIDFormat-Elements ein, das die Integration verwendet.
Weiterleitung für externe Abmeldung	Nein	Geben Sie die URL ein, an die die Integration Benutzer nach der Abmeldung umleitet.
Fehlerhafte Anforderungsumleitung	Nein	Geben Sie die URL für die Umleitung fehlgeschlagener Authentifizierungsanforderungen ein. Standardmäßig ist dies der URL-Endpunkt einer Fehlerseite oder Abmeldeseite, die im IdP konfiguriert ist. Sie können diesen Wert im Feld glide.authenticate.failed_requirement_redirect ausfüllen.

4. **Wahlweise:** Registerkarte „Verschlüsselung und Signatur“.

Hinweis:
Es wird empfohlen, eigene Zertifikate für die Verschlüsselung und Signierung zu verwenden.

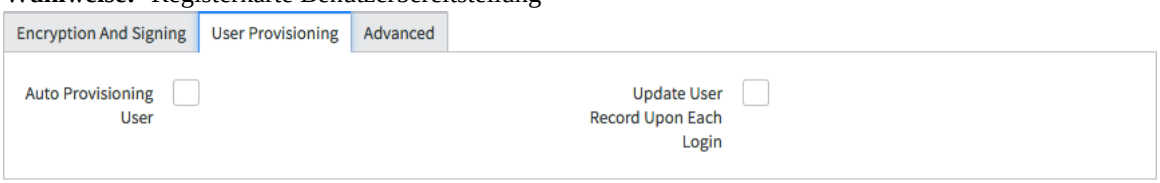
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Felder „Verschlüsselung und Signatur“.

Eigenschaft	Beschreibung
Signaturschlüsselalias	Geben Sie den Signaturalias des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.
Signaturschlüssel-Passwort	Geben Sie das Signaturpasswort des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.
Verschlüsselungsschlüsselalias	Geben Sie den Verschlüsselungsalias des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.
Passwort des Verschlüsselungsschlüssels	Geben Sie das Verschlüsselungspasswort des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.
Assertion verschlüsseln	Aktivieren Sie die Checkbox, um die Assertion in der SAML-Antwort zu verschlüsseln. Die für den IdP generierten Metadaten enthalten das x509-Zertifikat, mit dem der IdP die Assertion in der von ihm generierten SAML-Antwort verschlüsselt.
Signaturalgorithmus für Signieren	Geben Sie die URL ein, die auf den SAML 2.0-Identitätsanbieter AuthnRequest-Verbraucher für die eSignature-Authentifizierung verweist.
AuthnRequest signieren	Aktivieren Sie die Checkbox, um den Single Sign-on-Service des IdP für den Empfang einer signierten AuthnRequest zu aktivieren.
LogoutRequest signieren	Aktivieren Sie die Checkbox, damit der IdP Single Sign-on-Service signierte LogoutRequests empfangen kann.
Abmeldeantwort signieren	Aktivieren Sie die Checkbox, damit der Single Sign-on-Service des IdP eine signierte Abmeldeantwort erhalten kann.

5. **Wahlweise:** Registerkarte Benutzerbereitstellung



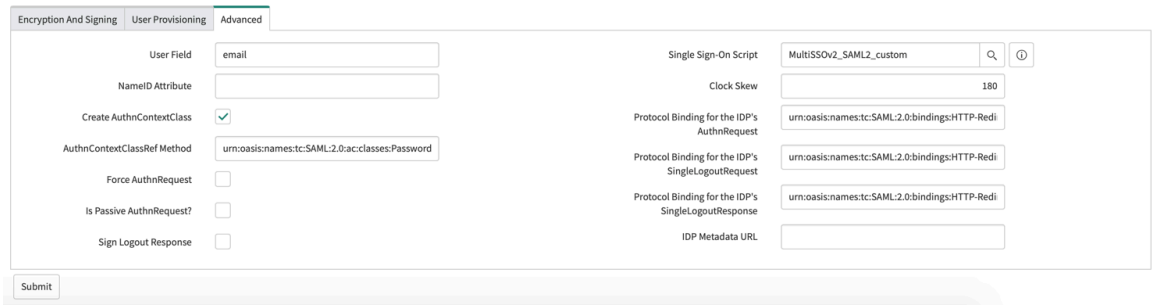
Benutzerbereitstellungsfelder

Eigenschaft	Beschreibung
Automatische Bereitstellung von Benutzer	Aktivieren Sie die automatische Benutzerbereitstellung. Erstellt die Benutzer basierend auf den vom IdP bereitgestellten Informationen, wenn der Benutzer nicht in der Benutzertabelle der Instanz vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Benutzerdatensatz bei jeder Anmeldung aktualisiere	Aktualisiert Benutzerinformationen in der Benutzertabelle der Instanz mit den Informationen im IdP, jedes Mal, wenn sich der Benutzer mit SAML anmeldet.

6. **Wahlweise:** Registerkarte „Erweitert“



Erweiterte Felder

Eigenschaft	Beschreibung
Benutzerfeld	Geben Sie das Feld in der Benutzertabelle ein, das den Wert enthält, den der IdP zum Identifizieren des Benutzers benötigt. Dies ist eine eindeutige ID als Teil der Antwort. Beispiele: Benutzername, Mitarbeiter-ID usw. In der Sys-Benutzertabelle wird diese eindeutige ID mit den Benutzerdetails abgeglichen.
Attribut NameID	Lassen Sie dieses Feld leer, es sei denn, Sie konfigurieren eine neue NameID-Richtlinie. Wenn Sie eine neue Richtlinie konfigurieren, benötigt das System die Benutzertabelle, die zum Identifizieren des Benutzers verwendet werden muss, der sich anmeldet. Das System gleicht das NameID-Token mit dem Namen dieses Benutzertabellenfelds ab.
AuthnContextClass erstellen	Aktivieren Sie die Checkbox, um eine bestimmte Kontextklasse anzugeben, z. B. Passwortgeschützte Übertragung. Wenn das Kontrollkästchen deaktiviert ist, wählt der IdP die am besten geeignete Kontextklasse aus.
AuthnContextClassRef-Methode	Geben Sie die URN des Anmeldemechanismus ein, den der IdP zur Authentifizierung von Benutzern verwenden soll.
AuthnRequest erzwingen	Aktivieren Sie die Checkbox, um das Auftreten von AuthnRequests zu erzwingen.
Ist „Passive AuthnRequest“.	Aktivieren Sie die Checkbox, wenn AuthnRequest passiv ist.
Single Sign-on-Skript	Wählen Sie das Single Sign-on-Skript aus. Der Standardwert ist *MultiSSOV2_SAML2_custom*.
Abmeldeantwort signieren	Geben Sie die Details der Abmeldeantwort in dieses Feld ein.
Taktversatz	Geben Sie die Anzahl der Sekunden zwischen den beiden Attributen ein, aus denen die SAMLResponse-Nonce besteht. Der Standardwert ist 60. Eine gültige SAMLResponse muss zwischen den Datums-/Uhrzeitwerten *notBefore* und *notOnOrAfter* liegen. Eine Beispiel-SAMLResponse-Nachricht finden Sie unter SAML 2-Beispielantwort mit den Elementen SubjectConfirmation und SubjectConfirmationData und SAML 2-Beispielantwort mit AudienceRestrictions- und Audience-Elementen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

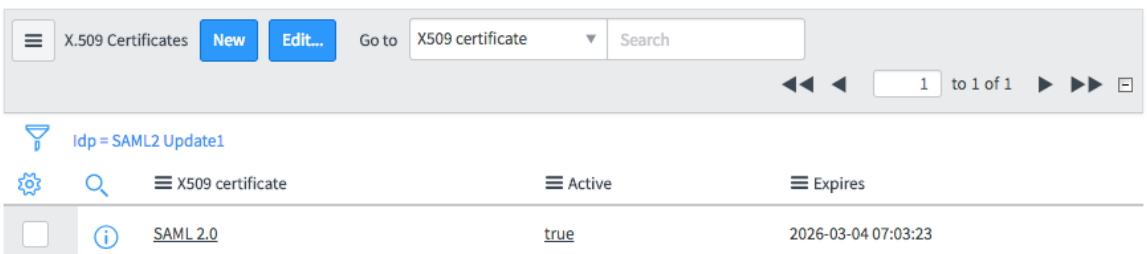
Eigenschaft	Beschreibung
Protokollbindung für SingleLogoutReuqest des IdP	Geben Sie einen der unterstützten Werte ein, die im Attribut „Binding“ aus dem SingleLogoutService-Element aufgeführt sind.
Metadaten-URL, aus der IdP-Eigenschaften importiert werden	Die IdP-Eigenschaften werden von dieser URL importiert. Wenn festgelegt, wird der automatische Import des SAML-Zertifikats vom IdP aktiviert, wenn das vorherige Zertifikat abgelaufen ist. **Hinweis:** Wenn Sie ein Upgrade von SAML2 Update 1 auf Multi-Provider-SSO durchführen oder Ihre SSO-Verbindung manuell einrichten, wird die IdP-Metadaten-URL nicht automatisch ausgefüllt.
Anforderung	Eine eindeutige ID als Teil der Anforderung. Die ID kann Benutzername, Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Umleitungs- als auch die Nachbindung werden für die Anforderung unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.
Antwort	Eine eindeutige ID als Teil der Antwort. Die ID kann Benutzername, Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Umleitung als auch die Nachbindung werden für die Antwort unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.

X.509-Zertifikate für SAML

Speichern und aktivieren Sie die erforderlichen IdP-Zertifikate für Ihre SAML-Konfiguration.

Die X.509-Zertifikate sind die IdP-Zertifikate, die von einer SAML-Konfiguration verwendet werden. Nachdem Sie ein Zertifikat installiert haben, können Sie beliebig viele Zertifikate hinzufügen. Wenn mehrere Zertifikate vorhanden sind, verwendet das System das erste gefundene aktive Zertifikat. Wenn Sie die URL für das **Feld Metadaten-URL festlegen, aus der IdP-Eigenschaften importiert werden**, fragt das System den IdP automatisch nach einem aktuellen, gültigen Zertifikat ab, wenn Ihr Zertifikat nicht mehr gültig ist. Sie hängt dieses Zertifikat an Ihre Instanz an und verwendet es für Ihre aktive SAML-Konfiguration.

Hinweis:
Die Abfrage erfolgt, wenn der IdP außerhalb Ihres Netzwerks zugänglich ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geführte Tour für SAML

Verwenden Sie die Guided Tour für SAML, um SAML für Single Sign-on zu konfigurieren.

Die geführte Tour für SAML hilft Ihnen, sich zu schulen und das SSO für Ihre ServiceNow® -Instanz zu konfigurieren. Administratoren können die Guided Tour auswählen, um sich schnell mit den erforderlichen Aktionen bei der Konfiguration von SSO für die Instanzen vertraut zu machen.

Bevor Sie die Guided Tour verwenden, müssen Sie eine SAML-Anwendung in Ihrem bevorzugten Identitätsanbieter konfigurieren, z. B. Okta, Microsoft Azure, ADFS usw. Informationen zum Konfigurieren einer SAML-Anwendung finden Sie in der folgenden Dokumentation:

- Okta: Für Okta müssen Sie Folgendes durchführen:
  - Fügen Sie eine Okta-SAML-Anwendung hinzu
  - Konfigurieren Sie SAML 2.0 für ServiceNow®
- Microsoft Azure: Single Sign-on (SSO)-Integration mit ServiceNow®
- Ping: SAML-SSO mit konfigurieren ServiceNow®
- ADFS: Integration mit SAML 2.0

Um die geführte Tour für SAML zu verwenden, aktivieren Sie das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“. Weitere Informationen finden Sie unter Aktivieren Sie das Multi-Provider-SSO-Plugin.

Führen Sie die folgenden Schritte aus, um die geführte Tour für SAML zu verwenden:

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identitätsanbieter**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **SAML aus**.
4. Klicken Sie auf das **Hilfesymbol**.
5. Klicken Sie auf **Tour**starten.

Die Guided Tour für SAML verwendet eine Reihe von Schritten, die sich über mehrere Seiten erstrecken, um die Konfiguration abzuschließen. Befolgen Sie die Schritte und Anweisungen, die im Rahmen der Tour bereitgestellt wurden, und schließen Sie die Tour ab. Weitere Informationen zur SAML-Konfiguration finden Sie unter SAML 2.0-Konfiguration mit Mehrfachanbieter-SSO.

Integration von SAML 2.0 mit anderen Funktionen

Sie können Ihre SAML 2.0-Lösung mit anderen Funktionen wie E-Signatur, Deep Linking und ADFS integrieren.

Fügen Sie Deep Linking-Unterstützung für SAML hinzu

Deep-Links ermöglichen es Instanzen, direkte E-Mail-Links zu einem bestimmten Datensatz im System zu unterstützen.

Wenn die SAML 2.0-Integration aktiviert ist, müssen Deep-Link-URLs eine Authentifizierungsprüfung bestehen, bevor der IdP den Benutzer zur ursprünglich angeforderten URL umleitet. Betrachten Sie beispielsweise eine E-Mail, die diese URL enthält: https://<instance name> .service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Instanz sendet eine Authentifizierungsanforderung an den IdP und verwendet den URL-Parameter RelayState, um die ursprünglich angeforderte Ressource beizubehalten (in diesem Fall uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d). Nachdem der IdP den Benutzer authentifiziert hat, liest die Instanz den Wert des URL-Parameters RelayState und leitet den Benutzer zur angeforderten Ressource um (falls in der Instanz vorhanden).

Um Deep Linking-Unterstützung hinzuzufügen, vergewissern Sie sich, dass der Identitätsanbieter den URL-Parameter RelayState unterstützt.

ADFS-Integration mit SAML 2.0

Das ServiceNow Multi-Provider-SSO-Plugin unterstützt eine SAML 2. Single Sign-on-Integration (SSO) mit Microsoft ADFS.

Weitere Informationen zur Installation und Konfiguration von AD FS finden Sie unter Übersicht über Active Directory-Verbundservices. Das Multi-Provider-SSO-Plugin wurde mit einer SAML 2.0 SSO-Integration mit ADFS 2.0, 3.0, Azure AD konfiguriert und getestet. In werden SAML-Antworten in nicht unterstützt

Richten Sie ADFS für SAML ein

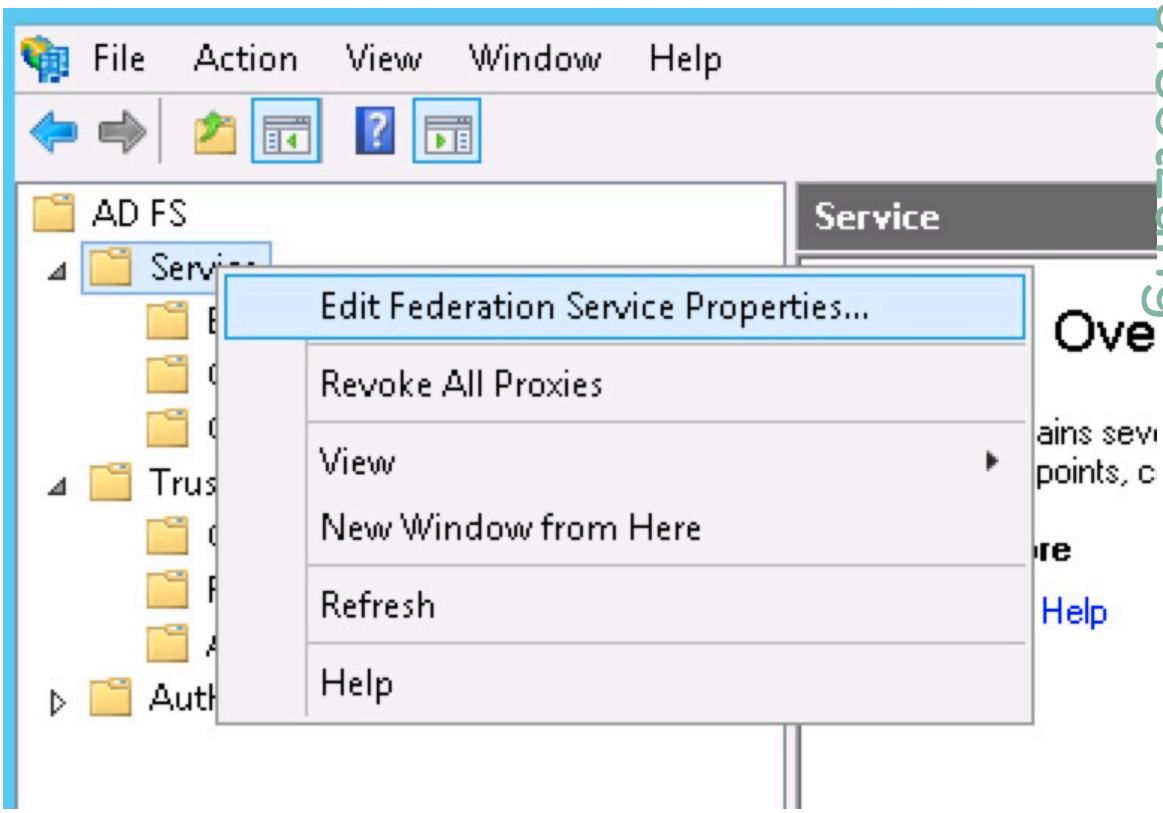
Richten Sie ADFS für SAML ein. Dieses Verfahren verwendet ADFS 2.0 und zeigt samportal.example.com als ADFS-Website an. Ersetzen Sie dies durch Ihre ADFS-Websiteadresse.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

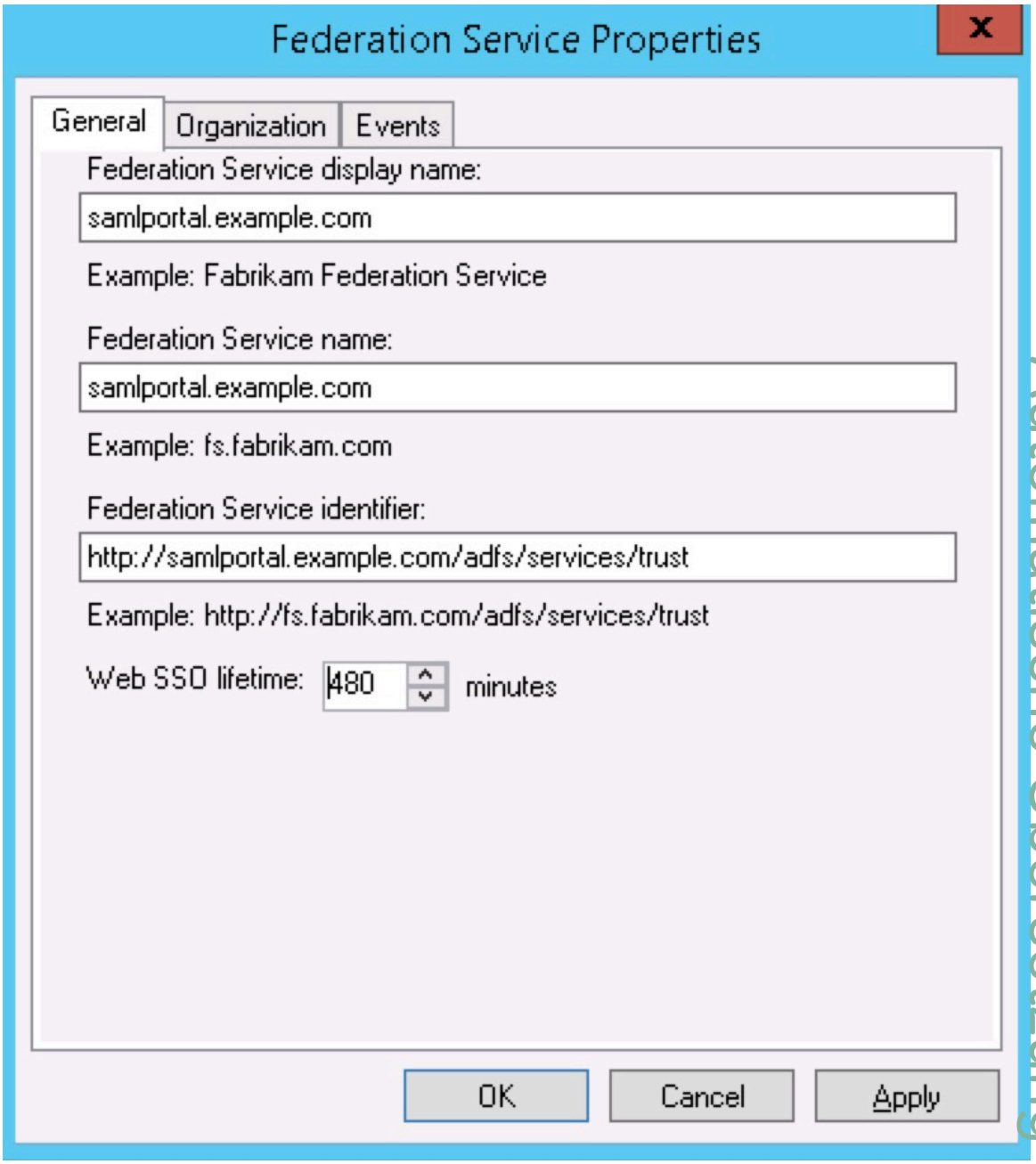
1. Melden Sie sich beim ADFS 3.0-Server an, und öffnen Sie die Managementkonsole.
2. Klicken Sie mit der rechten Maustaste auf **Service**, und wählen Sie **Eigenschaften des Verbundservice bearbeiten**aus.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Bestätigen Sie, dass die allgemeinen Einstellungen mit Ihren DNS-Einträgen und Zertifikatnamen übereinstimmen.



4. Navigieren Sie zu den Zertifikaten, und exportieren Sie das Token-Signaturzertifikat.

   a. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Zertifikat anzeigen**aus.

   b. Wählen Sie die Registerkarte **Details** aus.

   c. Klicken Sie **auf In Datei kopieren**.
   Der Zertifikatexport-Assistent wird geöffnet.

   d. Wählen Sie **Weiter**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Vergewissern Sie sich, dass die Option **No, not export the private key** (Nein, privaten Schlüssel nicht exportieren) ausgewählt ist, und klicken Sie dann auf **Weiter**.

f. Wählen Sie **DER-codierte Binärdatei X.509 (.cer)**aus, und klicken Sie dann auf **Weiter**.

g. Wählen Sie aus, wo Sie die Datei speichern möchten, geben Sie ihr einen Namen, und klicken Sie auf **Weiter**.

h. Wählen Sie **Fertigstellen** aus.
Die Instanz erfordert, dass dieses Zertifikat im PEM-Format vorliegt. Sie können dieses Zertifikat mit Client-Tools oder Online-Tools wie SSL Shopper konvertieren.

5. Verwenden Sie das soeben erstellte DER/Binary-Zertifikat, und exportieren Sie es im Standard-PEM-Format.

Richten Sie die Instanz für ADFS ein

Konfigurieren Sie Ihre Instanz und die SAML 2.0-Einstellungen für die Verwendung mit AD FS.

Vorbereitungen
Führen Sie diese Schritte erst aus, nachdem Sie ADFS für SAML eingerichtet haben. Weitere Informationen zu diesem Vorgang finden Sie unter ADFS für SAML einrichten.

Erforderliche Rolle: admin

Prozedur

1. Wenn noch nicht aktiv, aktivieren Sie das Plugin „Integration – Multiple Provider Single Sign-On Installer“.
2. Konfigurieren Sie SAML, aber wenn Sie das IdP-Zertifikat installieren, hängen Sie das PEM-Zertifikat an, das Sie bei Richten Sie ADFS für SAML einerstellt haben.
3. Klicken Sie auf **Speichern**.
4. Vergewissern Sie sich, dass die **Felder** Problem und **Betreff** Werte enthalten und keine Fehler vorhanden sind.
   Wenn ein Fehler auftritt, öffnen Sie das gespeicherte PEM-formatierte Zertifikat in Editor, kopieren Sie das Zertifikat und fügen Sie es in das Feld PEM-Zertifikat ein.
5. Vergewissern Sie sich, dass der Installations-Exit SAML2SingleSigno_update1 aktiv ist.
6. Setzen Sie die SAML 2.0-Konfiguration fort.

Hinweis:
Wenn ein Zertifikat auf dem ADFS-Server aktualisiert wird, müssen Sie auch ein aktualisiertes Zertifikat in die Instanz hochladen.

Konfigurieren Sie eine vertrauende ADFS-Seite

Nehmen Sie die Instanzmetadaten, und importieren Sie sie in Ihren ADFS-Server. Die manuelle Konfiguration der vertrauenden Partei scheint jedoch einfacher zu implementieren zu sein.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider** > **SAML2-Update1** > **Verschlüsselung und Signatur** und stellen Sie sicher, dass die SAML-Eigenschaft AuthnRequest signieren (`glide.authenticate.sso.saml2.require_signed_authnrequest`) nicht aktiv ist. Lassen Sie diese Eigenschaft nur aktiv, wenn Ihr ADFS-Administrator überprüfen kann, ob Sie signierte Anforderungen benötigen.
2. Kopieren Sie die Metadaten, die Sie über den SAML 2-Metadaten-Link generiert haben, und speichern Sie sie in einer Datei.
3. Melden Sie sich beim ADFS-Server an, und öffnen Sie die Managementkonsole.
4. Wählen Sie **Trusts der vertrauenden Partei aus**.
5. Wählen Sie in der oberen rechten Ecke des Fensters **Relying Party Trust hinzufügen** aus.

   Der Assistent zum Hinzufügen wird angezeigt.
6. Klicken Sie auf **Start**, um zu beginnen.
7. Verwenden Sie die Option **Datei** importieren, um die Metadatendatei zu importieren.
8. Geben Sie ihm einen Anzeigenamen wie ServiceNow, und geben Sie die gewünschten Notizen ein.
9. Wählen Sie **ADFS 3.0-Profil aus**.
10. Wählen Sie kein Tokenverschlüsselungszertifikat aus.
    Es wird das Zertifikat verwendet, das für den bereits exportierten Service definiert ist. Das Definieren eines Zertifikats verhindert die ordnungsgemäße Kommunikation mit der Instanz.
11. Aktivieren Sie keine Einstellungen für die **Konfigurations-URL**.
12. Geben Sie den Instanzstandort, mit dem Sie eine Verbindung hergestellt haben, als Vertrauensbezeichner der vertrauenden Partei ein.
    Verwenden Sie in diesem Fall https://company.service-now.com, und klicken Sie auf **Hinzufügen**.
13. Ermöglichen Sie allen Benutzern den Zugriff auf diese vertrauende Partei.
14. Klicken Sie auf **Weiter**, und deaktivieren Sie das Kontrollkästchen **Ansprüche nach Abschluss öffnen**.
15. Schließen Sie diese Seite.
    Die neue Vertrauensstellung der vertrauenden Partei wird im Fenster angezeigt.
16. Klicken Sie mit der rechten Maustaste auf den Trust der vertrauenden Partei, und wählen Sie **Eigenschaften**aus.
17. Navigieren Sie zur Registerkarte **Erweitert**, und legen Sie den **sicheren Hash-Algorithmus** entweder auf SHA-256 oder SHA-1 fest.
18. Navigieren Sie zur Registerkarte Endpunkte, und fügen Sie einen **SAML-Assertionsverbraucher** mit einer **Post** -Bindung und der URL https://company.service-now.com/navpage.dohinzu.

Konfigurieren Sie die Anspruchsregeln der abhängigen Partei für ADFS

Bearbeiten Sie die Anspruchsregeln, um eine ordnungsgemäße Kommunikation mit der Instanz zu ermöglichen.

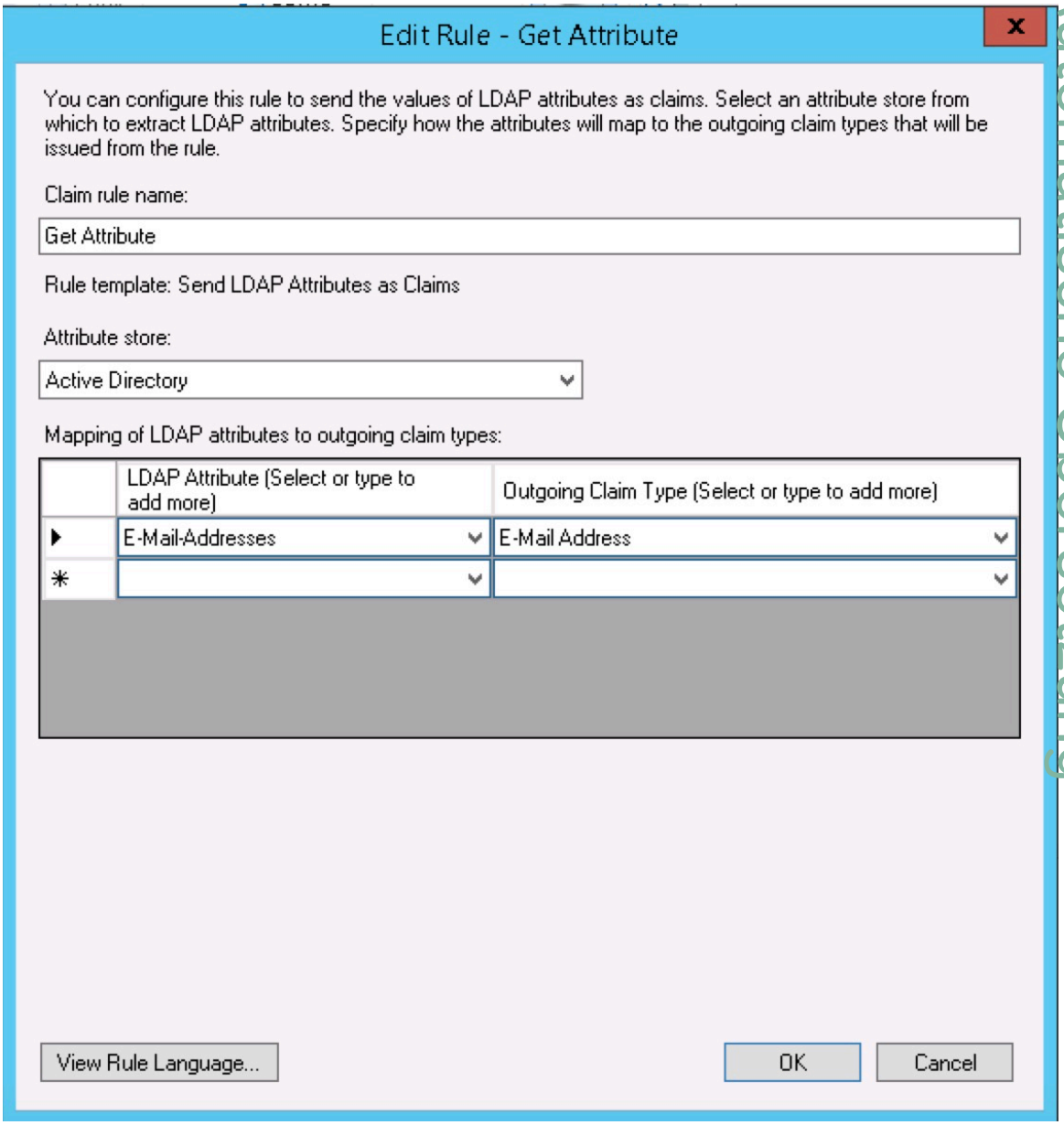
Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich beim ADFS-Server an, und öffnen Sie die Managementkonsole.
2. Klicken Sie mit der rechten Maustaste auf den Trust der vertrauenden Partei, und wählen Sie **Anspruchsregeln bearbeiten**aus.
3. Klicken Sie auf die Registerkarte **Ausgabe-Transformationsregeln**.
4. Wählen **Sie Regeln hinzufügen aus**.
5. Wählen **Sie Send LDAP Attribute as Claims** (LDAP-Attribut als Ansprüche senden) als zu verwendende Anspruchsregelvorlage aus.
6. Geben Sie dem Anspruch einen Namen wie LDAP-Attribute abrufen.
7. Legen Sie den **Attributspeicher** auf Active Directory, das **LDAP-Attribut** auf E-Mail-Adressenund den **ausgehenden Anspruchstyp** auf E-Mail-Adresse fest.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

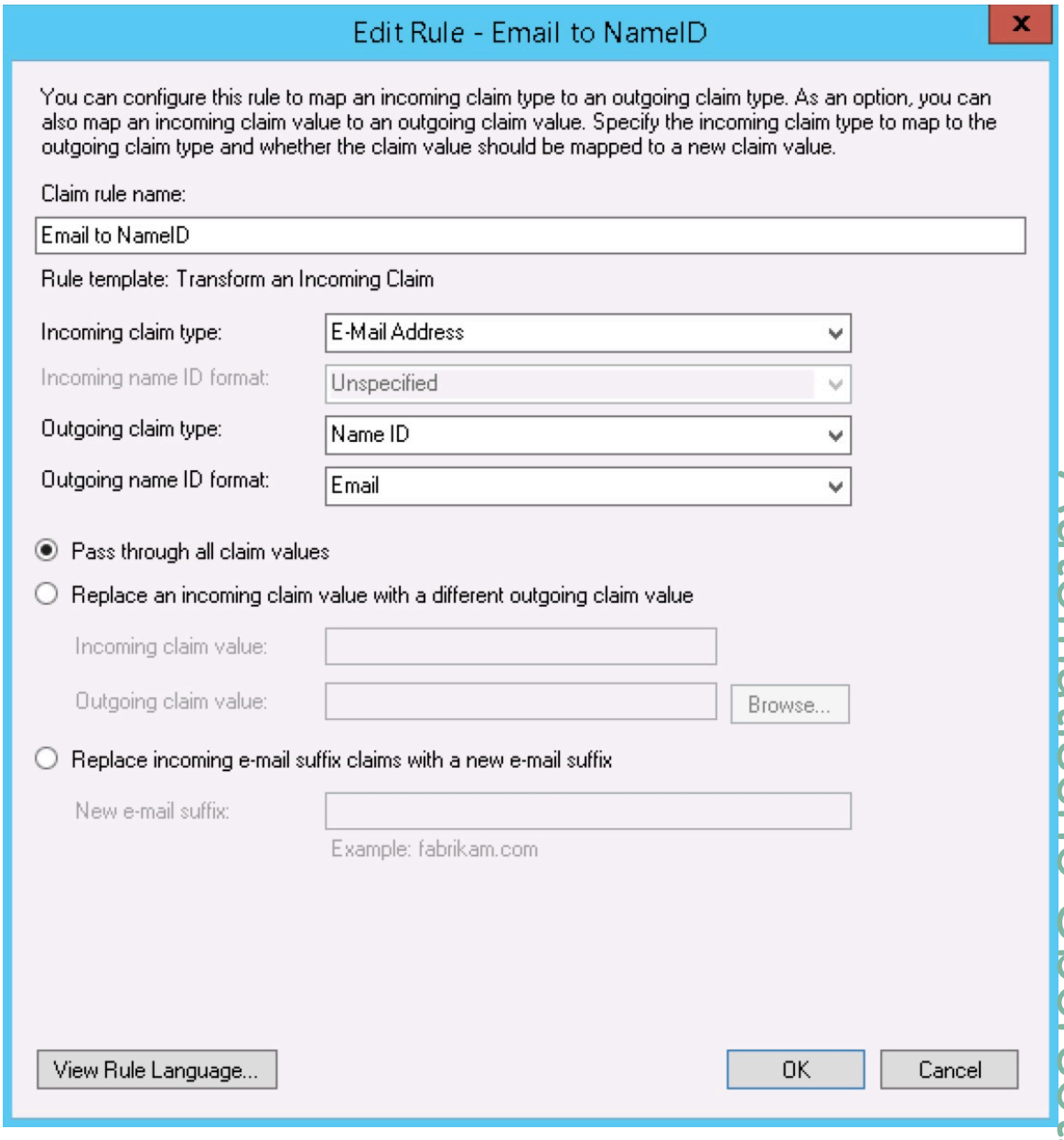
```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
 == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
query = ";mail;{0}", param = c.Value);
```

8. Wählen Sie **Fertigstellen** aus.
9. Wählen **Sie Regeln hinzufügen aus**.
10. Wählen Sie **Transform an Incoming Claim** (Eingehenden Anspruch umwandeln) als zu verwendende Anspruchsregelvorlage aus.
11. Geben Sie dem Anspruch einen Namen, z. B. E-Mail an Name ID.
12. Legen Sie den **eingehenden Anspruchstyp** in der vorherigen Regel auf den **ausgehenden Anspruchstyp fest**.
    Beispiel: E-Mail-Adresse.
13. Legen Sie den **ausgehenden Anspruchstyp** auf Namens-ID und das **ausgehende Namens-ID-Format** auf E- Mail fest.

    Hinweis:
    Diese Werte müssen mit der Namens-ID-Richtlinie übereinstimmen, die Sie während der SAML 2.0-Konfiguration definieren.

14. Wählen Sie **Alle Anspruchswerte übergeben aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Diese Anspruchsregel sollte der folgenden Regelsprache ähneln.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. Klicken Sie auf **Fertigstellen**.

Erstellen Sie einen SAML-Abmeldeendpunkt

Erstellen Sie einen SAML-Abmeldeendpunkt, um die Einzelabmeldung zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen finden Sie in diesem Artikel zur ADFS-Abmeldung .

Prozedur

1. Gehe zu **ADFS-Manager** > **Vertrauensstellungen** > **Trusts der vertrauenden Partei** > **Eigenschaften**.
2. Klicken Sie auf der Registerkarte Endpunkte auf **SAML hinzufügen**.
3. Konfigurieren Sie die Einstellungen:
   - **Endpunkttyp**: SAML-Abmeldung
   - **Bindung**: POST
   - **Vertrauenswürdige URL**: Die URL Ihres ADFS-Servers. Beispiel:

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - **Antwort-URL**: Die Abmelde-URL der Anwendung. Beispiel:

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

Testen Sie die ADFS-Konfiguration

Testen Sie Ihre ADFS-Konfiguration, um sicherzustellen, dass sie ordnungsgemäß als Identitätsanbieter funktioniert.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie einen Internet Explorer-Browser.
2. Navigieren Sie zu Ihrem ADFS-Portal.

   Beispiel: `https://samportal.example.com/adfs/ls/idpinitiatedsgnon.aspx`. Diese Seite enthält eine Dropdown-Liste aller konfigurierten Vertrauensstellungen der vertrauenden Partei.
3. Wählen Sie die vertrauende Partei aus, die Ihrer Instanz zugeordnet ist.
4. Klicken **Sie auf Mit Anmeldung fortfahren**.

   Wenn Sie die externe SAML 2.0-Authentifizierung ordnungsgemäß konfiguriert haben, sollten Sie automatisch bei der Instanz angemeldet werden.
5. Testen Sie eine direkte Anmelde-URL, indem Sie zu `https://samportal.example.com/adfs/ls/idpinitiatedsigno.aspx?logintoRP=https://company.service-now.com`navigieren.

(Workaround) Aktivieren Sie die vom Service Provider initiierte Authentifizierung

Verwenden Sie diese Problemumgehung, wenn die Authentifizierung fehlschlägt, weil Sie nicht über SAML 2.0 Update 1 verfügen. Dieses Problem kann auftreten, wenn Benutzer versuchen, die IdP-Authentifizierung zu überspringen und direkt zur Instanz zu navigieren.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieser Fehler tritt auf, wenn die Instanz ADFS nicht die erforderliche Definition und Semantik für das Attribut SPNameQualifier in der SAMLResponse bereitstellt.

Aktivieren Sie die vom Service Provider initiierte Authentifizierung, indem Sie eine der folgenden Aktionen ausführen:

Prozedur

- Führen Sie ein Upgrade auf SAML 2.0 Update 1 durch, und deaktivieren Sie die Option zum Erstellen einer AuthnContextClass-Anforderung.
  Weitere Informationen finden Sie unter Aktivieren und richten Sie SAML 2.0 ein.
- Ändern Sie die **SAML2-Skripteinbindung**, um die Definitionen des Attributs SPNameQualifier auszukommentieren, wenn SAML 2.0 aktiv ist (nicht SAML 2.0 Update 1).

  Kommentieren Sie diese Zeilen in den Funktionen „createNameID“ und „createNameIDPolicy“ aus:

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

Nächste Maßnahme

Wenn Sie nicht möchten, dass die Anmeldeaufforderung Ihres ADFS-Servers beim Zugriff auf die Instanz angezeigt wird, legen Sie die folgende Eigenschaft von SAML 2.0 Update 1 auf „false“ fest: **Erstellen Sie eine AuthnContextClass-Anforderung in der AuthnRequest-**Anweisung (`glide.authenticate.sso.saml2.createrequestedauthncontext`).

(Workaround) Unterstützung der Kerberos-Authentifizierung

Für die SAML 2.0-Integration ist eine Problemumgehung verfügbar, die den Authentifizierungskontext von formularbasierter Authentifizierung in Windows-basierte Authentifizierung ändert.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Derzeit verwendet die SAML 2-Integration einen PasswordProtectedTransport- oder „Formularbasierte Authentifizierung“-Authentifizierungskontext. Dieser Authentifizierungskontext erfordert, dass der IdP Benutzern ein Formular für die Anmeldeinformationen für die Authentifizierung vorlegt. Mit Kerberos ist eine SAML-Sitzung bereits über eine eingerichtete Windows-Anmeldung aktiv, sodass sich der Benutzer nicht beim IdP authentifizieren muss.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Öffnen Sie den IdP-Datensatz **SAML2 Update1**.
3. Legen Sie die **AuthnContextClassRef-Methode, die in unsere SAML 2.0 AuthnRequest an den Identitätsanbieter aufgenommen wird**, auf eine der folgenden Optionen fest:

Werte der AuthnContextClassRef-Methode	
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	**(Standard)**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

urn:federation:authentication:windows

4. Klicken Sie auf **Aktualisieren**.

Azure AD-Integration mit SAML 2.0

Integrieren Sie ServiceNow mit Azure Active Directory (Azure AD).

Durch die Integration von ServiceNow mit Azure AD können Sie:

- Steuern Sie in Azure AD, wer Zugriff auf ServiceNowhat.
- Ermöglichen Sie Benutzern die automatische Anmeldung bei ServiceNow mit ihren Azure AD-Konten.
- Verwalten Sie Ihre -Konten im Azure-Portal.

Voraussetzungen

Um zu beginnen, müssen Sie Folgendes ausführen:

- Ein Azure AD-Abonnement. Wenn Sie kein Abonnement haben, können Sie einen kostenlosen Account erhalten.
- Ein ServiceNow Single Sign-on (SSO) aktiviert.
- Eine ServiceNow -Instanz oder ein -Mandant von ServiceNow, die San Diego-Versionen oder höher unterstützt.
- Für einen ServiceNow -Mandanten muss das Single Sign-on-Plugin für mehrere Anbieter aktiviert sein.
- Aktivieren Sie für die automatische Konfiguration das Multi-Provider-Plugin für ServiceNow.

Satz von Aktionen für die Konfiguration

Im Folgenden finden Sie die Aktionen, die zum Konfigurieren von Azure AD ausgeführt werden müssen:

- Fügen Sie ServiceNow aus dem Katalog zu Azure AD hinzu.
- Konfigurieren Sie Azure AD SSO
- Erstellen Sie einen Azure AD-Testbenutzer
- Weisen Sie den Azure AD-Testbenutzer zu
- ServiceNow konfigurieren

Fügen Sie ServiceNow aus der Galerie hinzu

Fügen Sie ServiceNow aus dem Katalog Ihrer Liste der verwalteten SaaS-Apps in Azure AD hinzu.

Vorbereitungen
Erforderliche Rolle: Azure-Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich mit einem Microsoft-Konto beim Azure-Portal an.
2. Wählen Sie im linken Bereich den Service **Azure Active Directory** aus.
3. Navigieren zu **Unternehmensanwendungen** > **Alle Anwendungen**.
4. Um eine neue Anwendung hinzuzufügen, wählen Sie **Neue** Anwendung.
5. Geben Sie im Abschnitt Aus der Galerie hinzufügen ServiceNow in das Suchfeld ein.
6. Wählen Sie im Ergebnisbereich ServiceNow aus, und fügen Sie dann die App hinzu.
7. Warten Sie einige Sekunden, während die App Ihrem Mandanten hinzugefügt wird.

Konfigurieren Sie Azure AD SSO

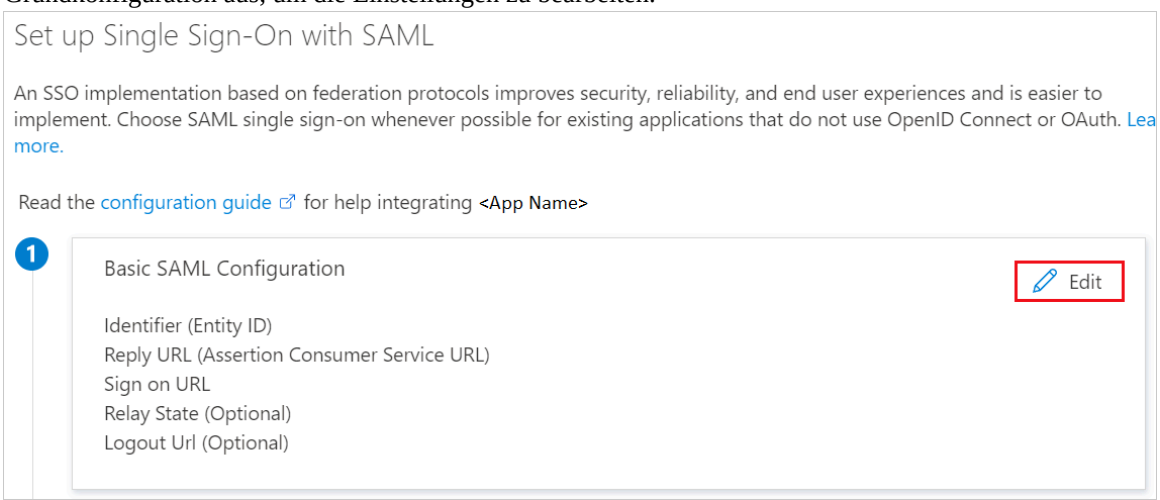
Konfigurieren Sie Azure AD SSO im Azure-Portal.

Vorbereitungen

Erforderliche Rolle: Azure-Administrator

Prozedur

1. Suchen Sie im Azure-Portal auf der Anwendungsintegrationsseite ServiceNow nach dem Abschnitt Verwalten.
2. Wählen Sie Single Sign-on aus.
   Wählen Sie auf der Seite Single Sign-on-Methode auswählen die Option SAML aus.
3. Wählen Sie auf der Seite Single Sign-on mit SAML einrichten das Stiftsymbol für SAML-Grundkonfiguration aus, um die Einstellungen zu bearbeiten.



4. Führen Sie im Abschnitt SAML-Grundkonfiguration folgende Schritte aus:

   a. **Geben Sie unter Anmelde-URL**eines der folgenden URL-Muster ein:

```
https://<instancename>.service-now.com/navpage.do
https://<instance-name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Hinweis:
Sie müssen die sys_id innerhalb dieser URL angeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Geben Sie im Feld Bezeichner (Entitäts-ID) eine URL mit dem Muster https://ein.<instance-name> .service-now.com .

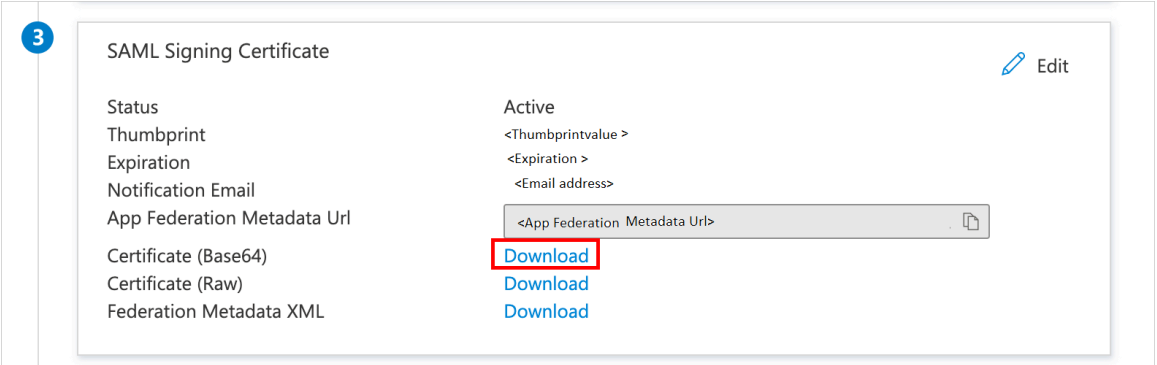
c. Geben Sie für **Antwort-URL**eines der folgenden URL-Muster ein:

```
https://<instancename>.service-now.com/navpage.do
https://<instancename>.service-now.com/customer.do
```

d. Geben Sie im Feld Abmelde-URL eine URL mit dem Muster ein: https://<instancename> .service-now.com/navpage.do

Hinweis:
Sie müssen die tatsächliche Anmelde-URL, Antwort-URL, Abmelde-URL und Bezeichner aktualisieren. Die in diesen URLs angezeigten Werte dienen zu Demozwecken.

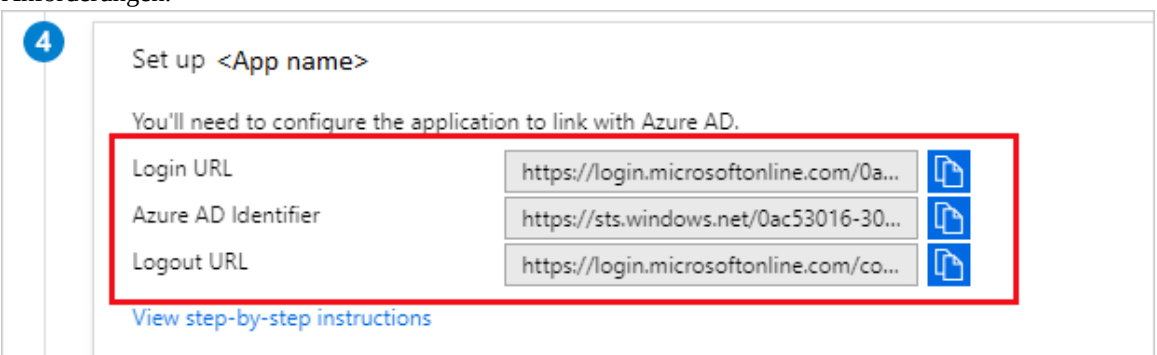
5. Suchen Sie auf der Seite Single Sign-on mit SAML einrichten im Abschnitt SAML-Signaturzertifikat nach **Zertifikat (Base64)**.



a. Klicken Sie auf die Schaltfläche „Kopieren“, um die URL der **App-Verbundmetadaten**zu kopieren und in den Editor einzufügen.
Diese URL ist für die weitere Konfiguration erforderlich.

b. Wählen Sie **Herunterladen** aus, um das Zertifikat (Base64) herunterzuladen.

6. Kopieren Sie im Abschnitt „Setup ServiceNow “ die entsprechenden URLs basierend auf Ihren Anforderungen.



Erstellen Sie einen Azure AD-Testbenutzer

Erstellen Sie einen Testbenutzer in Azure AD.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Azure-Administrator

Prozedur

1. Navigieren Sie im Azure-Portal zu **Alle** > **Azure Active Directory** > **Benutzer** > **Alle Benutzer**.
2. Wählen Sie **Neuer Benutzer aus**.
3. Geben Sie in den Benutzereigenschaften die folgenden Informationen an:
   - Name
   - Benutzername
   - Passwort
4. Klicken Sie auf **Erstellen**.

Weisen Sie den Azure AD-Testbenutzer zu

Weisen Sie den Azure AD-Testbenutzer zu, der für die Verwendung des einmaligen Anmeldens von Azure erstellt wurde, indem Sie Zugriff auf ServiceNowgewähren.

Vorbereitungen
Erforderliche Rolle: Azure-Administrator

Prozedur

1. Navigieren Sie im Azure-Portal zu **Alle** > **Unternehmensanwendungen** > **Alle Anwendungen**.
2. Wählen Sie in der Anwendungsliste ServiceNowaus.
3. Wählen Sie auf der Seite der App im Abschnitt Verwalten die Option **Benutzer und Gruppen aus**.
4. Wählen Sie **Anwender hinzufügen** aus.
5. Wählen Sie im Fenster **„Zuweisung** hinzufügen“ die Option **Benutzer und Gruppen aus**.
6. Wählen Sie im Fenster **Benutzer und Gruppen** den Testbenutzer aus, der aus der Benutzerliste erstellt wurde.
7. Wählen Sie bei Bedarf die Rolle für den zugewiesenen Benutzer in der Dropdown- **Liste Eine Rolle** auswählen aus.
8. Wählen Sie im Fenster „ **Zuweisung** hinzufügen“ die **Option Zuweisen**aus.

ServiceNow konfigurieren

Konfigurieren Sie ServiceNow mit Azure AD-Details, um SSO zu verwenden.

Vorbereitungen
Plugin: Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter

Aktivieren Sie die SSO-Eigenschaften für Mehrfachanbieter:

- Wählen Sie **SSO für mehrere Anbieter aktivieren aus**.
- Wählen Sie **Aktivieren des automatischen Imports von Benutzern aus allen Identitätsanbietern in die Benutzertabelle**.
- Wählen Sie **Debug-Protokollierung für SSO-Integration mit mehreren Anbietern aktivieren aus**.
- Geben Sie **email**ein, das Feld in der Benutzertabelle, das….

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Wählen Sie auf der Seite „Identitätsanbieter“ die Option **Neu**aus.
3. Wählen Sie im Fenster „Identitätsanbieter“ **SAML**aus.
4. Unter „Metadaten des Identitätsanbieters importieren“ haben Sie folgende Möglichkeiten:
   - **URL**: Metadaten-URL des App-Verbunds zum automatischen Ausfüllen der Details auf der Konfigurationsseite des Identitätsanbieters.
   - **Importieren**: Importieren Sie die XML-Datei, um die Details auf der Konfigurationsseite des Identitätsanbieters zu importieren.
5. Klicken Sie mit der rechten Maustaste oben auf dem Bildschirm, klicken Sie auf **sys_id kopieren**, und verwenden Sie diesen Wert für die Anmelde- **URL** im Abschnitt **SAML-Grundkonfiguration**.
6. Füllen Sie die Felder des Formulars aus.

Single Sign-on-Felder für mehrere Anbieter

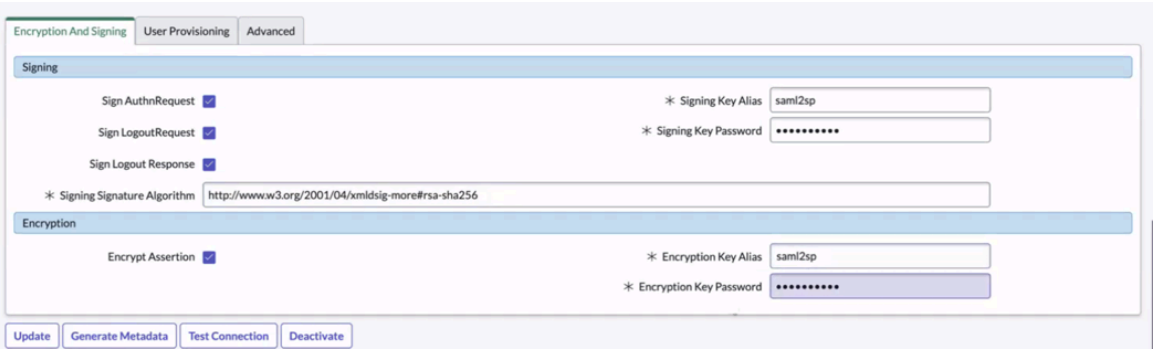
Eigenschaft	Erforderlich	Beschreibung
Name	Ja	Name für den IdP Dieser IdP ist die Sys-ID der automatischen Umleitung.
Aktiv	Ja	Aktiv muss für den IdP, der für die Authentifizierung verwendet werden soll, auf „true“ festgelegt werden. **Hinweis:** Die Option zum Festlegen dieser Eigenschaft ist nur nach einer erfolgreichen Testverbindung verfügbar.
Standard	Nein	IdP mit automatischer Umleitung, früher als primärer IdP bezeichnet, leitet Benutzer automatisch zum Zugriff auf die Basisinstanz-URL um. Diese Eigenschaft legt diese IdP-Konfiguration als Standard fest.
Automatische IdP-Weiterleitung	Nein	IdP-Konfiguration, die Sie als IdP für die automatische Umleitung festlegen können. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Weiterleitung aktivieren, wird das Cookie `glide_sso_id` mit dem neuen IdP für die automatische Weiterleitung aktualisiert. Die automatisch aktivierte Systemeigenschaft `glide.authenticate.sso.update.idp.cookie` steuert diese Funktion.
URL des Identitätsanbieters	Ja	URL zu Ihrem IdP Jede IdP-URL muss eindeutig sein.
AuthnRequest des Identitätsanbieters	Ja	URL zur HTTP-Redirect-Bindung, die vom SingleSignOnService-Element abgerufen wird.
SingleLogoutRequest des Identitätsanbieters	Nein	URL, die aus dem SingleLogoutService-Element abgerufen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Erforderlich	Beschreibung
ServiceNow Homepage	Ja	URL, einschließlich Anmeldeseite, der Instanz, für die sich der IdP authentifiziert Beispiel: https://IhreInstanz.service-now.com/navpage.do
Entitäts-ID/Aussteller	Ja	Basis-URL, ausgenommen die Anmeldeseite der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
Zielgruppen-URI	Ja	Basis-URL, ausgenommen die Anmeldeseite der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
NameID-Richtlinie	Ja	Wert des NameIDFormat-Elements, das die Integration verwendet.
Weiterleitung für externe Abmeldung	Nein	URL, an die die Integration Benutzer nach der Abmeldung umleitet.
Fehlerhafte Anforderungsumleitung	Nein	URL für die Umleitung fehlgeschlagener Authentifizierungsanforderungen. Standardmäßig ist dies der URL-Endpunkt einer Fehlerseite oder Abmeldeseite, die im IdP konfiguriert ist. Sie können diesen Wert im Feld glide.authenticate.failed_requirement_redirect ausfüllen.

7. **Wahlweise:** Registerkarte „Verschlüsselung und Signatur“.

Hinweis:
Verwenden Sie Ihre eigenen Zertifikate für die Verschlüsselung und Signierung.



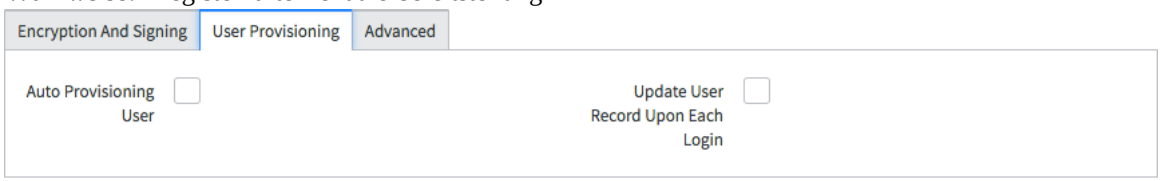
Felder Verschlüsselung und Signieren

Eigenschaft	Beschreibung
Alias zum Signieren/für Verschlüsselungsschlüssel	Alias des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags.
Signaturschlüssel-Passwort	Passwort des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags.
Assertion verschlüsseln	Checkbox zum Verschlüsseln der Assertion in der SAML-Antwort. Die für den IdP generierten Metadaten enthalten das x509-Zertifikat, mit dem der IdP die Assertion in der von ihm generierten SAML-Antwort verschlüsselt.
Signaturalgorithmus für Signieren	URL, die auf den AuthnRequest-Verbraucher des SAML 2.0-Identitätsanbieters für die eSignature-Authentifizierung verweist.
AuthnRequest signieren	Kontrollkästchen, um den Single Sign-on-Service des IdP für den Empfang einer signierten AuthnRequest zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
LogoutRequest signieren	Checkbox, um den Single Sign-on-Service des IdP für den Empfang einer signierten LogoutRequest zu aktivieren.

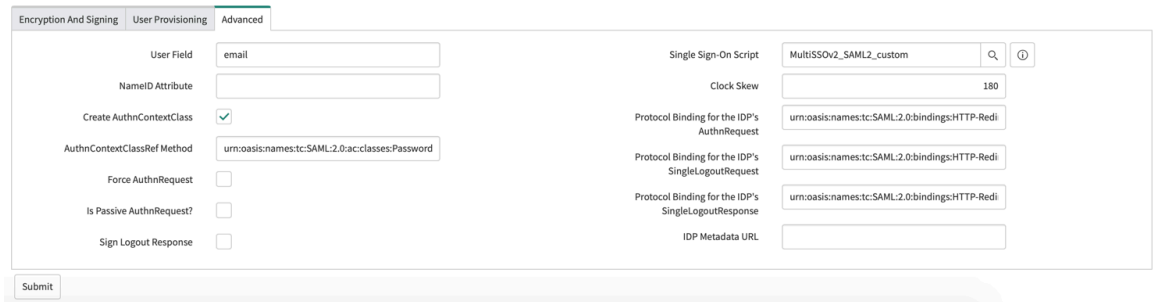
8. **Wahlweise:** Registerkarte Benutzerbereitstellung



Benutzerbereitstellungsfelder

Eigenschaft	Beschreibung
Automatische Bereitstellung von Benutzer	Bei der automatischen Benutzerbereitstellung werden Benutzer basierend auf den vom IdP bereitgestellten Informationen erstellt, wenn der Benutzer nicht in der Benutzertabelle der Instanz vorhanden ist.
Benutzerdatensatz bei jeder Anmeldung aktualisiere	Aktualisieren Sie jedes Mal, wenn sich der Benutzer mit SAML anmeldet, die Benutzerinformationen in der Benutzertabelle der Instanz mit den Informationen im IdP.

9. **Wahlweise:** Registerkarte „Erweitert“



Erweiterte Felder

Eigenschaft	Beschreibung
Benutzerfeld	Feld in der Benutzertabelle, das den Wert enthält, den der IdP zum Identifizieren des Benutzers benötigt. Diese eindeutige ID ist Teil der Antwort. Zum Beispiel ein Benutzername, eine Mitarbeiter-ID usw. In der Sys-Benutzertabelle wird diese eindeutige ID mit den Benutzerdetails abgeglichen.
Attribut NameID	Feld, das Sie leer lassen, es sei denn, Sie konfigurieren eine neue NameID-Richtlinie. Wenn Sie eine neue Richtlinie konfigurieren, benötigt das System die Benutzertabelle, die zum Identifizieren des Benutzers verwendet werden muss, der sich anmeldet. Das System gleicht das NameID-Token mit dem Namen dieses Benutzertabellenfelds ab.
AuthnContextClass erstellen	Kontrollkästchen, um eine bestimmte Kontextklasse anzugeben, z. B. Passwortgeschützte Übertragung. Wenn das Kontrollkästchen deaktiviert ist, wählt der IdP die am besten geeignete Kontextklasse aus.
AuthnContextClassRef-Methode	URN des Anmeldemechanismus, den der IdP zur Authentifizierung von Benutzern verwenden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
AuthnRequest erzwingen	Kontrollkästchen, um das Auftreten von AuthnRequests zu erzwingen.
Ist „Passive AuthnRequest“.	Checkbox, wenn AuthnRequest passiv ist.
Single Sign-on-Skript	Single Sign-on-Skript. Der Standardwert ist *MultiSSOV2_SAML2_custom*.
Abmeldeantwort signieren	Details zur Abmeldungsantwort in diesem Feld.
Taktversatz	NAnzahl von Sekunden zwischen den beiden Attributen, aus denen die SAMLResponse-Nonce besteht. Der Standardwert ist 60. Eine gültige SAMLResponse muss zwischen den Datums-/Uhrzeitwerten *notBefore* und *notOnOrAfter* liegen. Eine Beispiel-SAMLResponse-Nachricht finden Sie unter SAML 2-Beispielantwort mit den Elementen SubjectConfirmation und SubjectConfirmationData und SAML 2-Beispielantwort mit AudienceRestrictions- und Audience-Elementen.
Protokollbindung für SingleLogoutReuqest des IdP	Einer der unterstützten Werte, die im Bindungsattribut des SingleLogoutService-Elements aufgeführt sind.
Metadaten-URL, aus der IdP-Eigenschaften importiert werden	IdP-Eigenschaften werden von dieser URL importiert. Wenn festgelegt, wird der automatische Import des SAML-Zertifikats vom IdP aktiviert, wenn das vorherige Zertifikat abgelaufen ist. **Hinweis:** Wenn Sie ein Upgrade von SAML2 Update 1 auf Multi-Provider-SSO durchführen oder Ihre SSO-Verbindung manuell einrichten, wird die IdP-Metadaten-URL nicht automatisch ausgefüllt.
Anforderung	Eindeutige ID als Teil der Anforderung. Die ID kann ein Benutzername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Umleitungs- als auch die Nachbindung werden für die Anforderung unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.
Antwort	Eindeutige ID als Teil der Antwort. Die ID kann ein Benutzername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Umleitung als auch die Nachbindung werden für die Antwort unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.

10. Wählen Sie oben rechts auf der Seite **Testverbindung** aus.
11. Geben Sie Ihre Anmeldeinformationen ein.
    Die SSO Logout-Testergebnisse werden angezeigt.
12. Wählen Sie **Aktivieren** aus, um die Konfiguration zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Links mit externer Authentifizierung

Sie können E-Mail-Links verwenden, wenn Sie die externe Authentifizierung mit Digestif-Token verwenden. Sie müssen jedoch festlegen, wie Links in E-Mail-Benachrichtigungen behandelt werden sollen.

Die Standardlinks enthalten eine URL, die Sie zu einem bestimmten Ort in der Instanz führt, z. B. zu einem Incident oder einer Change-Anforderung, ohne SSO-Anmeldeinformationen zu integrieren. Im Folgenden finden Sie Beispiele für die Weiterleitung des Benutzers zum Speicherort in der Instanz, ohne sich auf der Anmeldeseite der Instanz anzumelden.

- Unverschlüsselte HTTP-Technik zur Verbindung mit der /demo-Instanz (es wird nicht zu einem bestimmten Datensatz navigiert):

  ```
  https://<instance
   name>.service-now.com/?
  SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
  ```

- Link (in einer E-Mail-Benachrichtigung) zu einem bestimmten Datensatz, sodass der Benutzer zuerst zum unternehmenseigenen Anmeldeportal wechselt:

  ```
  https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2
  b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true
  ```

  Sie müssen die Eigenschaft *`glide.email.override.url`* in Ihrer Instanz so festlegen, dass sie die URL der Unternehmensportalseite enthält. Wenn diese Eigenschaft nicht vorhanden ist, können Sie sie erstellen.

- Das Unternehmensportal muss dann diese URL verwenden und die Umleitungs-URL für die Instanz erstellen, wobei das für den Zugriff auf den spezifischen Datensatz erforderliche Segment erhalten bleibt und die SSO-Anmeldeinformationen am Ende der URL hinzugefügt werden:

  ```
  https://<instance
   name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2b01ab4eb0942
  23466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true&SM_USER=user_
  name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
  ```

Fügen Sie E-Signatur-Unterstützung für SAML hinzu

Konfigurieren Sie die folgenden Eigenschaften für E-Signatur mit Security Assertion Markup Language (SAML) 2.0 Update 1.

Wenn die E-Signatur mit Multi-SSO aktiv ist, werden die SAML-Eigenschaften nicht verwendet. Das System fügt der Tabelle „SAML2 Update1-Eigenschaften“ [saml2_update1_properties] E-Signatur-Eigenschaften hinzu:

Eigenschaft	Beschreibung	Standard
Assertionen-Verbraucher-Index für eSignatur-Authentifizierung	Eine Indexnummer, die den Endpunkt identifiziert	1
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Die URL, die den Verbraucher identifiziert.	https://IhreInstanz.service-now.com/consumer.do
AuthnRequest-URL für eSignature-Authentifizierung	Die URL für die Authentifizierung	Keine

Wenn Sie E-Signatur mit SAML 1.0 oder SAML 2.0 (ohne Update 1) verwenden, beachten Sie die speziellen Konfigurationsanweisungen: E-Signatur für Mehrfachanbieter-SSO.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie ein Life-Science-Kunde sind, der E-Signatur verwendet, deaktivieren Sie die Geschäftsregel zur Verhinderung der Selbstsperre des Anwenders.

Migrieren einer vorhandenen SAML 1.1-Integration zu SAML 2.0

Wenden Sie sich an den Kundensupport, um von einer SAML 1.1-Integration zu einer SAML 2.0-Integration zu migrieren.

Aktualisieren Sie Ihre vorhandene SAML 2.0-Integration

Aktualisieren Sie Ihre vorhandene SAML 2.0-Integration.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Fordern Sie das Plugin SAML 2.0 Update 1 an. Wenden Sie sich an Kundenservice und Support, um das Plugin „ *SAML 2.0 Single Sign-on - Update 1: Sicherheitserweiterungen* “ anzufordern. Das Plugin wendet aktualisierte Versionen des *SAML2SingleSgnon-* Installationsausgangs (Anmeldeskript), des *SAML2Logout-* Installationsausgangs (Abmeldeskript) und der *SAML2-Skripteinbindung* (Skriptobjekt) an.

Führen Sie Anpassungen aus vorhandenen Installations-Exit-Skripts in neuen Skripts zusammen. Das Update speichert eine inaktive Kopie der ursprünglichen Installations-Exit-Skripts der Integration. Sie können diese Kopien verwenden, um alle Anpassungen, die Sie an den Anmelde- und Abmeldeskripts vorgenommen haben, mit den neuen Versionen dieser Installations-Exits zusammenzuführen.

Führen Sie Anpassungen aus vorhandenen Installations-Exit-Skripts in neue Skripts zusammen

Name des ursprünglichen Installations-Exit-Skripts	Ursprünglicher Skriptstatus	Name des Exit-Skripts für die Neuinstallation	Neuer Skriptstatus
SAML2SingleSign	Inaktiv	SAML2SingleSign_update1	Aktiv
SAML2	Inaktiv	SAML2_update1	Aktiv
SAML2Logout	Inaktiv	SAML2Logout_update1	Aktiv

Sie können über die folgenden Pfade zu den SAML 2.0-Anmelde- und Abmelde-Installations-Exit-Skripts navigieren:

- **SAML 2 Single Sign-on** > **Anmeldeskript**.
- **SAML 2 Single Sign-on** > **Abmeldeskript**.
- **Systemdefinition** > **Installationsausgänge**.

Sie können über die folgenden Pfade zur Skripteinbindung SAML 2.0 Update 1 navigieren:

- **SAML 2 Single Sign-on** > **Skriptobjekt**.
- **Systemdefinition** > **Skripteinbindungen**.

Testen Sie das Update.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Fügen Sie die Systemeigenschaft `glide.authenticate.sso.saml2.debug` mit dem Wert *true*hinzu.
2. Versuchen Sie, sich bei SAML 2.0 anzumelden.
3. Überprüfen Sie das Systemprotokoll.
   SAML2-Validierungsfehler beginnen mit dem Text *SAML2ValidationError*.
4. Identifizieren und beheben Sie typische Anmeldefehler.
   Weitere Informationen finden Sie unter Multi-SSO (SAML 2.0) – Fehler und Korrekturen.

Beispiel für SAML 2-Antworten nach dem Update

In den folgenden Abschnitten werden die neuen erforderlichen Elemente und Attribute veranschaulicht, die der IdP in der SAML-Antwort bereitstellen sollte.

Beispiel einer SAML 2-Antwort mit Ausstellerelement

Die folgende SAML 2-Antwort verwendet das *Issuer*- Element.

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
    ...
  </saml:Assertion></samlp:Response>
```

Beispiel-SAML 2-Antwort mit den Elementen „SubjectConfirmation“ und „SubjectConfirmationData“.

Die folgende SAML 2-Antwort verwendet die Elemente *SubjectConfirmation* und *SubjectConfirmationData* mit den Attributen *NotOnOrAfter* und *Recipient*.

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:Subject
ConfirmationData InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

Beispiel für eine SAML 2-Antwort mit den Elementen „AudienceRestrictions“ und „Audience“.

Die folgende SAML 2-Antwort verwendet die Elemente „ *AudienceRestrictions* “ und „ *Audience* “ mit den Attributen „ *NotBefore*“ und „*NotOnOrAfter*“.

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAML-Benutzerbereitstellung

Wenn Benutzer in Ihrem IdP vorhanden sind, sich aber nicht in Ihrer Instanz befinden, kann die SAML-Benutzerbereitstellung die Benutzer automatisch in der Benutzertabelle [sys_user] Ihrer Instanz erstellen.

Die SAML-Benutzerbereitstellung wird für SAML 2.0 Update 1 unterstützt, wenn Multi-SSO aktiviert ist.

Funktionsweise der SAML-Benutzerbereitstellung

Wenn die SAML-Benutzerbereitstellung aktiviert ist und das System einen neuen Benutzer erkennt, der sich nicht in der Instanz befindet, erstellt die Instanz automatisch einen Datensatz in einer temporären Tabelle mit dem Namen `u_imp_saml_user_`.<suffix> , wobei ist ein automatisch generierter Textbezeichner. Das System erstellt auch eine Transformationszuordnung, die die Datenbeziehungen zwischen der Importtabelle und der Benutzertabelle angibt. Jeder im System identifizierte IdP verfügt über eine eigene Transformationszuordnung. Die Transformationszuordnung wird einmal für jeden IdP erstellt. Administratoren können sie nach Bedarf aktualisieren.

Wenn sich der Benutzer anmeldet, greift er auf einen IdP zu, um sich anzumelden.

- Das System zeigt eine Liste aller IdPs an, die die SAML-Benutzerbereitstellung verwenden können. Wenn nur ein IdP die SAML-Benutzerbereitstellung verwenden kann, wird dieser automatisch verwendet.
- Wenn keine der oben genannten Bedingungen zutrifft, verwendet das System den IdP für die automatische Umleitung.

SAML-Benutzerbereitstellung verwalten

Aktualisieren Sie die Benutzertabelle mit den Benutzern in Ihrem IdP, indem Sie zuerst die Feldzuordnung einrichten und dann die Benutzerbereitstellung über die Multi-SSO-IdP-Einstellungen aktivieren.

Vorbereitungen

Richten Sie Ihre IdP-Zuordnung ein, um zu ermitteln, welche Felder im IdP den richtigen Feldern in der Benutzertabelle zugeordnet sind.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Eigenschaften**.
2. Wählen Sie Aktivieren Sie **den automatischen Import von Benutzern aus allen Identitätsanbietern in die Benutzertabelle** (*`glide.authenticate.multisso.user.autoprovision`*), um diese Funktion zu aktivieren.
3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
5. Öffnen Sie den Identitätsanbieter-Datensatz, den Sie verwenden möchten.
6. Erstellen Sie einen Datensatz in der Benutzertabelle, wenn der Benutzer noch nicht vorhanden ist, indem Sie **Benutzer automatisch bereitstellen**auswählen.
   Wenn Sie ein Upgrade auf diese Version durchgeführt haben, müssen Sie das Formular konfigurieren und dieses Feld hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Aktivieren Sie die Aktualisierung von Benutzerdatensätzen, wenn sich Benutzer beim IdP anmelden und die Informationen auf dem IdP mit den Informationen in der Benutzertabelle veraltet sind, indem Sie **Benutzerdatensatz bei jeder**Anmeldung aktualisieren auswählen.
   Wenn Sie ein Upgrade auf diese Version durchgeführt haben, müssen Sie das Formular konfigurieren und dieses Feld hinzufügen.
8. Klicken Sie auf **Benutzerbereitstellung Transformationszuordnung**, um die Zuordnung anzuzeigen, die das System automatisch erstellt.
9. Nehmen Sie nach Bedarf Änderungen an der Zuordnung vor.

Ergebnisse

Wenn die ersten unbekannten Benutzer versuchen, sich anzumelden, erstellt das System die Felder in der Import Set-Tabelle aus der Datei metadata.xml.

Hinweis:
Sie können die Felder aus der IdP-Tabelle erst zuordnen, wenn sich dieser erste Benutzer anmeldet.

SAML 2.0-Problembehandlung

Bevor Sie sich an den Support wenden, versuchen Sie es mit den Problembehandlungslösungen, die in der Knowledge Base auf Hi verfügbar sind.

Hinweis:
Die Instanz unterstützt keine Lösungen, die von externen Websites bereitgestellt werden.

Weitere Informationen finden Sie im folgenden Knowledge Base-Artikel: KB0540617 '"SAML-Fehlermatrix"' .

Andere häufige Probleme

Fehler oder Symptom	Lösung
Fehlermeldung: „ist keine Funktion“. Dieses Problem kann in einer Umgebung mit mehreren Knoten auftreten. Wenn das Plugin nicht auf allen Knoten aktiviert wird, wird ein Fehler wie der folgende angezeigt: org.mozilla.javascript.EcmaError: `[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]` ist keine Funktion.	Dieser Fehler tritt auf, da das Plugin nicht aktiv war und die JAR-Datei nicht geladen hat. Daher scheint der Code zu fehlen. Wenden Sie sich an den technischen Support, um Knoten neu zu starten, auf denen das Plugin fehlt.
SAML authentifiziert keine Benutzer, die auf CMS-Seiten zugreifen.	Standardmäßig sind CMS-Seiten öffentlich und erfordern daher keine Authentifizierung. Wenn Sie möchten, dass SAML CMS-Seiten authentifiziert, ändern Sie die öffentliche Seite *view_content.do* von *active=true* in *active=false*.
Ein Anwender kann nach der SAML-Authentifizierung nicht zu einer CMS-Seite zurückgeleitet werden.	Standardmäßig verwendet die SSO-Integration einen URL-Parameter namens *URI*, um zu steuern, wohin der Benutzer nach der Authentifizierung beim IdP weitergeleitet wird. SSO ignoriert relative URLs. Beispielsweise kann SSO Benutzer nicht zu einer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere häufige Probleme (Fortsetzung)

Fehler oder Symptom	Lösung
	relativen URL von */ess* umleiten. Stattdessen muss der Benutzer zu einer URL wie */nav_to.do?uri=/ess navigieren*, die Deep-Link-Syntax verwendet. Dadurch wird das ESS-Portal jedoch innerhalb des IFrame des Hauptnavigationsinhalts platziert. Mit anderen Worten, die Site nimmt nicht die gesamte Seite ein, sondern wird als Seite in Ihrer Instanz geladen. Weitere Informationen finden Sie unter CMS-Sites und Single Sign-on. Wenn Sie die CMS-Einstiegsseite ändern, um sie privat zu machen, indem *Sie view_content.do* auf *active=false*setzen, erfordert das Deep-Linking-Verhalten eine Anpassung des Anmeldeskripts für *Installationsende*. Erstellen Sie ein Skript, das nach dem *URI* -Teil der URL sucht und einen *RelayState*- URL-Parameter erstellt, der den relativen URL-Pfad enthält, um Benutzer nach der Authentifizierung beim IdP umzuleiten.
SAML leitet Benutzer nach der Authentifizierung nicht auf die entsprechende Seite um.	Bestimmen Sie, ob der Relaisstatus an den IdP übergeben und dann während der Authentifizierung zurückgegeben wird. Sie können dies mit einem Browser tun, der HTTP-Anforderungskopfzeilen und POST-Informationen speichern kann, z. B. Chrome mit seinen integrierten Entwicklertools oder Firefox mit dem Add-on HTTPfox. Verwenden Sie für Internet Explorer eine Drittanbieteranwendung wie Fiddler. Das Ziel besteht darin, die Anforderungen zu beobachten, die vom Client (Browser) an die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere häufige Probleme (Fortsetzung)

Fehler oder Symptom	Lösung
	Instanz und vom Client an den IdP übergeben werden.

Überwachen Sie die Event-Warteschlange auf Anmeldeaktivitäten

Jede Single Sign-on-Integration erstellt Events für Anmeldeaktivitäten.

Sie können diese Events verwenden, um auf Anmeldefehler zu überwachen und festzustellen, ob Sicherheitsbedenken bestehen.

Überwachen der Event-Warteschlange auf Anmeldefehler

Eventname	Beschreibung	Datensatz	Parameter 1	Parameter 2
external.authentication.succeeded	Externe Authentifizierung erfolgreich, und der Benutzer hat auf die Instanz-URL zugegriffen.	Sitzungs-ID	Anwender-ID des Anwenders, der sich erfolgreich angemeldet hat	Die URL, auf die der Anwender zugegriffen hat (möglicherweise ein Deep-Link)
external.authentication.failed	Die Single Sign-on-Anforderungen sind nicht vorhanden oder fehlen.		Sitzungs-ID	Die fehlenden Authentifizierungsanforderungen
external.authentication.failed	Der Benutzer ist in der Benutzertabelle [sys_user] nicht vorhanden		Anwender-ID	Die Zeichenfolge „Benutzer ist nicht vorhanden“
external.authentication.failed	Der Benutzer ist ausgesperrt.		Anwender-ID	Die Zeichenfolge „Benutzer ausgesperrt.“

Event-Warteschlangen-Anmelde-Events

Die SAML 2.0-Integration erstellt Events für Anmeldeaktivitäten.

Sie können diese Events verwenden, um auf Anmeldefehler zu überwachen und festzustellen, ob Sicherheitsbedenken bestehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisse der Anmeldeaktivitäten

Ereignisname	Beschreibung	Mit Ereignis verwendete ID	Event-Zeichenfolge
saml2.logout.validierung.fehlgeschlagen	Die Abmeldeantwort des IdP konnte nicht anhand Ihrer Abmeldeanforderung validiert werden. Das Event validiert den<inResponseTo> -Element für die Sitzungs-ID (ID-Attribut des<saml2p:LogoutRequest> -Element). Sehen Sie sich beispielsweise den Workflow für die ausgegebene Abmeldeanforderung an.	Sitzungs-ID	Die Zeichenfolge „SAML2 LogoutResponse validation failed.“
external.authentication.succeeded	Externe Authentifizierung erfolgreich.		Die Zeichenfolge „Authentifizierung erfolgreich“
external.authentication.succeeded	Externe Authentifizierung erfolgreich, und der Benutzer hat auf die Instanz-URL zugegriffen.	Sitzungs-ID und Anwender-ID des Anwenders, der sich erfolgreich angemeldet hat	Die URL, auf die der Anwender zugegriffen hat (möglicherweise ein Deep-Link)
external.authentication.failed	Die Single Sign-on-Anforderungen sind nicht vorhanden oder fehlen.	Sitzungs-ID	Die fehlenden Authentifizierungsanforderungen
external.authentication.failed	Der Benutzer ist in der Benutzertabelle [sys_user] nicht vorhanden.	Anwender-ID	Die Zeichenfolge „Benutzer ist nicht vorhanden“
external.authentication.failed	Der Benutzer ist ausgesperrt.	Anwender-ID	Die Zeichenfolge „Benutzer ausgesperrt“

Automatische Übersetzung

Änderungen an SAML 2.0 und Digest-Token-Konfiguration

Mit Single Sign-on für mehrere Anbieter können Administratoren SAML 2.0 Update 1 und Digest-Token als Authentifizierungsmethoden konfigurieren.

Single Sign-on für mehrere Anbieter muss aktiviert sein, bevor Sie die Eigenschaften von SAML 2.0 Update 1 und Digest-Token konfigurieren. Nachdem Sie Mehrfachanbieter-SSO angefordert und aktiviert haben, müssen Sie es einrichten. Nach dem Einrichten von Mehrfachanbieter-SSO können Sie die SAML 2.0 Update 1- und Digest-Token-Konfigurationen erstellen oder aktualisieren. Sie können eine oder beide Authentifizierungslösungen mit Mehrfachanbieter-SSO verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Plugin „Integration – Single Sign-On Installer für mehrere Anbieter“ entfernt die SAML-Anwendung aus dem Navigator. Die erforderlichen SAML-Einstellungen werden in die Multi-Provider-SSO-Anwendung in die Tabelle „SAML2 Migriert“ migriert. Sie können Elemente wie das x509-Zertifikat, IdP-Details usw. weiterhin über die Multi-Provider-SSO-Anwendung ändern.

Eingehende und ausgehende OAuth-Authentifizierung

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensstellung im System herzustellen.

OAuth 2.0 - Open Authorization ist das Branchenstandardprotokoll für Autorisierung, das auf Client-Entwickler-Einfachheit setzt und gleichzeitig spezifische Autorisierungs-Flows für Webanwendungen, Desktop-Anwendungen und Mobilgeräte bereitstellt.

Es handelt sich um einen Standard, der es einer Website oder Anwendung ermöglicht, im Namen eines Benutzers auf Ressourcen zuzugreifen, die von anderen Web-Apps gehostet werden.

Anstatt die Anmeldeinformationen des Ressourcenbenutzers für den Zugriff auf geschützte Ressourcen zu verwenden, erhält der Client ein Zugriffstoken. Zugriffstoken werden mit Genehmigung des Benutzers an Clients von Drittparteien ausgegeben. Der Client verwendet dann das Zugriffstoken für den Zugriff auf die geschützten Ressourcen.

Eingang

Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch werden ein OAuth-Client-Anwendungsdatensatz sowie eine Client-ID und ein Client-Secret erstellt, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt. Weitere Informationen finden Sie unter OAuth eingehend.

Ausgehend

Verwenden Sie einen externen OAuth-Provider, der die Autorisierung für den Zugriff auf Ihre Instanz bereitstellt. Geben Sie ein OAuth-Profil und einen OAuth-Bereich an, wenn Sie eine Verbindung zu einem anderen OAuth-Provider herstellen. Weitere Informationen finden Sie unter OAuth ausgehend.

OAuth 2.0

Mit OAuth 2.0 können Benutzer über externe Clients auf Instanzressourcen zugreifen, indem sie ein Token erhalten, anstatt bei jeder Ressourcenanforderung Anmeldeinformationen einzugeben.

Um die OAuth-Integration zu verwalten, benötigen Sie die Rolle security_admin. Konfigurieren Sie OAuth 2.0 für die folgenden Szenarien:

- **Szenario mit externem OAuth-Client** (eingehend): Ihre Instanz bietet einen Endpunkt für Clients von Drittanbietern, um Daten aus der Instanz abzurufen.
- **OAuth-Provider-Szenario** (ausgehend): Ihre Instanz ruft Daten von einem Drittanbieter ab.

Hinweis:
Sie müssen sich zum ersten Mal als Benutzer authentifizieren, um den Token-Post abzurufen. Sie müssen sich vor Ablauf des Tokens nicht mit einem Benutzerkonto authentifizieren.

Sowohl einfache Sicherheits- als auch Hochsicherheits-Frameworks unterstützen OAuth 2.0. Hohe Sicherheit wird empfohlen. Unter finden Sie Informationen dazu, für welche Versionen bereits hohe Sicherheit aktiv ist und wie hohe Sicherheit aktiviert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselkonzepte der OAuth 2.0-Implementierung

Konzept	Beschreibung
Ressourcenbesitzer	Eine Entität, die Zugriff auf eine geschützte Ressource gewähren kann. Ein Ressourcenbesitzer, der eine Person ist, wird als *Endbenutzer*bezeichnet. Der Ressourcenbesitzer ist immer ein Benutzeraccount.
Client	Eine Anwendung, die mit der Autorisierung des Ressourcenbesitzers Anforderungen für geschützte Ressourcen im Namen des Ressourcenbesitzers sendet.
Ressourcenserver	Der Server, der die geschützten Ressourcen hostet und Anforderungen für geschützte Ressourcen annehmen und beantworten kann.
Autorisierungsserver	Der Server, der nach erfolgreicher Authentifizierung des Ressourcenbesitzers und Erhalt der Autorisierung Zugriffstoken an den Client ausgibt.
Autorisierungsanforderung	Die Berechtigung, die ein Client für den Zugriff auf eine geschützte Ressource benötigt. Die Autorisierungsanforderung ist immer eine HTTP-POST-Nachricht, die die ID des Clients enthält, der im Namen des Ressourcenbesitzers handelt, und Anmeldeinformationen, die die Anforderung autorisieren.
Autorisierung Gewährung	Anmeldeinformationen, die die Autorisierung des Ressourcenbesitzers für den Zugriff auf eine Ressource darstellen. Bei der Autorisierungsgewährung handelt es sich entweder um Anmeldeinformationen des Benutzers oder ein Aktualisierungstoken.
Zugriffs-Token	Eine sichere Zeichenfolge, die ein Client für den Zugriff auf geschützte Ressourcen verwendet. Eine Instanz gibt Zugriffstoken an Clients aus, die über eine gültige Autorisierungsgewährung verfügen. Jedes Zugriffstoken hat einen bestimmten Bereich, eine bestimmte Lebensdauer und andere Attribute. Standardmäßig gibt eine Instanz Zugriffstoken mit einer Lebensdauer von 30 Minuten aus, wenn die Instanz der OAuth-Provider ist. Für Drittanbieter-Token 30 Tage.
Token neu laden	Anmeldeinformationen, die ein Client verwendet, um neue Zugriffstoken zu erhalten, ohne dass eine zusätzliche Benutzerautorisierung erforderlich ist. Eine Instanz gibt ein Aktualisierungstoken an einen Client aus, wenn er zum ersten Mal für ein Zugriffstoken autorisiert wird. Standardmäßig gibt eine Instanz Aktualisierungstoken mit einer Lebensdauer von 100 Tagen aus, wenn die Instanz der OAuth-Provider ist. Für Drittpartei-Token 365 Tage.
Selbstsignierte Zertifikate	Now Platform unterstützt keine selbstsignierten Zertifikate. Der OAuth-Client verwendet den Zertifikat-Truststore nicht und lässt keine Verbindung zu OAuth-Endpunkten zu, die ein selbstsigniertes Zertifikat enthalten.
Benutzeragent	Der Benutzer, der Zugriffsrechte für eine Client-Anwendung delegiert, bei der es sich häufig um eine Website handelt. Die Zugriffsrechte ermöglichen es der Clientanwendung oder Website, auf Daten in der Instanz zuzugreifen, für die der Benutzer Zugriffsrechte hat. Der Benutzeragent wird im Szenario verwendet.

OAuth-Gewährungstypen

Ein *Gewährungstyp* ist die Art und Weise, wie der Client das Zugriffstoken erhält. Die folgenden Gewährungstypen werden unterstützt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Autorisierungscode**: Der Verbraucher erhält zuerst einen Autorisierungscode und verwendet ihn dann, um ein Zugriffstoken zu erhalten. Sie können ein OAuth-Profil angeben und diesen Gewährungstyp angeben. Der Prozess, bei dem der Autorisierungscode verwendet wird, wird auch als Authentifizierungscode *-Flow* oder *Autorisierungscode-Flow bezeichnet*.
- **Passwort-Anmeldeinformationen**des Ressourcenbesitzers: Der Verbraucher der Ressource verfügt bereits über die Anmeldeinformationen des Benutzers, um das Zugriffstoken zu erhalten. Dieser Prozess wird auch als *Passwort-Flow*bezeichnet.
- **Client-Anmeldeinformationen**: Der Verbraucher der Ressource verwendet die Client-ID und den geheimen Clientschlüssel, die bereits in der Anwendungsregistrierung konfiguriert sind.

Speicherung von Authentifizierungsanmeldeinformationen

Der OAuth-Clientschlüssel wird als Feld vom Typ `password2` gespeichert, das mit KMF verschlüsselt ist. Benutzerpasswörter, die zur Überprüfung eingehender Endpunktanforderungen verwendet werden, werden als Hash-Wert in der Benutzertabelle in einem Feld vom Typ `password` (SHA 256) gespeichert. Weitere Informationen zu dieser Verschlüsselung finden Sie unter Password2-Verschlüsselung mit KMF

Richten Sie OAuth ein

Richten Sie OAuth ein und aktivieren Sie es, aktivieren Sie die OAuth-Systemeigenschaft, erstellen Sie einen OAuth-Anwendungsendpunkt, damit externe Clientanwendungen auf die Instanz zugreifen können, und legen Sie OAuth-Parameter fest.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Stellen Sie sicher, dass das OAuth-Plugin aktiv und die OAuth-Aktivierungseigenschaft auf „true“ festgelegt ist.
2. Erstellen Sie eine OAuth-Anwendungsregistrierung mit einer der folgenden Methoden:
   - Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch werden ein **OAuth-Client-Anwendungsdatensatz** sowie eine Client-ID und ein Client-Secret erstellt, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt.
   - Verwenden Sie einen externen OAuth-Provider , der die Autorisierung für den Zugriff auf Ihre Instanz bereitstellt.

     Geben Sie ein OAuth-Profil und einen OAuth-Bereich an, wenn Sie eine Verbindung zu einem anderen OAuth-Provider herstellen.
3. Konfigurieren Sie Ihre Client-Anwendungen, um einen HTTP POST zu erstellen, der ein OAuth-Token anfordert.
   Die Anwendung muss auch in der Lage sein, die JSON-Antwort zu analysieren, um das zurückgegebene Zugriffstoken und das Aktualisierungstoken zu verwenden.

Aktivieren Sie OAuth

Standardmäßig ist das Plugin **„OAuth 2.0“ (com.snc.platform.security.oauth)** in neuen und aktualisierten Instanzen aktiv. Wenn das Plugin in Ihrer Instanz nicht aktiv ist, können Sie es aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Legen Sie die OAuth-Eigenschaft fest

Um OAuth 2.0-Token für registrierte Anwendungen zu generieren, muss die Eigenschaft `com.snc.platform.security.oauth.is.active` für die Instanz aktiv sein.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Um OAuth 2.0 zu verwenden, geben **Sie sys_properties.list** im Filternavigator des Arbeitsbereichs ein, und klicken Sie auf **Neu**.
2. Füllen Sie das Formular mit den folgenden Einstellungen aus:

   - **Name**: com.snc.platform.security.oauth.is.active
   - **Typ**: true | false
   - **Wert**: true

Ändern Sie den OAuth-Passwortparameter

Verwenden Sie diese Eigenschaft, um sicherzustellen, dass nur POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert werden.

Das Senden vertraulicher Informationen über URI-Abfrageparameter kann zur Offenlegung vertraulicher Informationen durch Clients, den Server oder einen Host zwischen den Anforderungen führen. Ab dem Madrid-Release stellt diese neue Eigenschaft sicher, dass nur die POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert werden. Unterstützte Gewährungstypen:

- Autorisierungscode
- Kennwort
- -Client-Anmeldeinformationen
- Aktualisierungstoken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth-Passwortparametereigenschaft

Eigenschaft	Beschreibung
glide.oauth.allow.parameters.in.post.body.only	Diese Eigenschaft ist nur für zBoots als Teil des OAuth 2.0-Plugins auf „true“ festgelegt. Wenn Sie diese Einstellung für Ihre Instanz benötigen, erstellen Sie die Eigenschaft und legen Sie sie auf „true“ fest.

OAuth eingehend

OAuth eingehend bietet einen Endpunkt für Clients von Drittanbietern, um Daten aus der Instanz abzurufen.

Um die OAuth-Integration zu verwalten, benötigen Sie die Rolle security_admin.

Sie können die Integration des **externen OAuth-Client-Szenarios** (eingehend) konfigurieren, wenn Ihre Instanz einen Endpunkt für Clients von Drittanbietern bereitstellen soll, um Daten aus der Instanz abzurufen.

Hinweis:
Sie müssen sich zum ersten Mal als Benutzer authentifizieren, um den Token-Post abzurufen. Sie müssen sich vor Ablauf des Tokens nicht mit einem Benutzerkonto authentifizieren.

Sie können die eingehende OAuth-Konfiguration abhängig vom folgenden Gewährungstyp durchführen:

- **Autorisierungscode**: Für einen vom Benutzer initiierten Gewährungs-Flow, bei dem der Benutzer ohne Eingabe von Benutzername oder Passwort, aber über das Zugriffstoken eine autorisierte URL für die Authentifizierung konfigurieren kann. Weitere Informationen finden Sie unter OAuth-Autorisierungscode-Gewährungs-Flow.
- **Passwort-Anmeldeinformationen des Ressourcenbesitzers**: Für einen vom Benutzer initiierten Gewährungs-Flow, bei dem für die Authentifizierung eine Benutzerinteraktion erforderlich ist. Weitere Informationen finden Sie unter Flow-Konfiguration für Passwortgewährung.

  Hinweis:
  Für den Autorisierungscode-Flow muss der Anwender die Authentifizierung durch lokale Anmeldung, SSO oder MFA abschließen und dann seine Einwilligung erteilen.

- **JWT Bearer**: Für eine System-zu-System-Integration, bei der kein Benutzereingriff erforderlich ist. Weitere Informationen finden Sie unter JWT Bearer Grant-Flow-Konfiguration.
- **ID-Token-Flow**: Für die Verwendung eines ID-Tokens, das von OIDC-Drittanbietern wie Okta und Azure ausgegeben wurde. Weitere Informationen finden Sie unter ID-Token-Flow für Authentifizierung.
- **Implizite OAuth-Gewährungen**: Damit das Zugriffstoken direkt an die Clientanwendung über den Benutzeragenten übergeben werden kann, in der Regel über den Webbrowser oder das Mobilgerät. Weitere Informationen finden Sie unter Implizite OAuth-Gewährungen.
- **Client-Anmeldeinformationen**: Für die Verwendung des Gewährungstyps OAuth-Client-Anmeldeinformationen für eingehende Integrationen von einem OAuth-Client einer Drittpartei zur ServiceNow® -Plattform. Weitere Informationen finden Sie unter Client-Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth-Bereiche

Sie können den Umfang der Unterstützung des OAuth-Authentifizierungsbereichs für die REST-API festlegen. OAuth Scope bietet nur Zugriff auf die jeweiligen REST APIs. Weitere Informationen finden Sie unter REST-API-Authentifizierungsbereich.

OAuth-Autorisierungscode-Gewährungs-Flow

Der Autorisierungscode-Gewährungs-Flow ermöglicht einem Benutzer den Zugriff auf eine Ressource, indem er sich direkt bei einem OAuth-Server authentifiziert, der der Ressource vertraut, im Gegensatz zur Authentifizierung mit Benutzername/Passwort-Anmeldeinformationen.

Diese Implementierung des OAuth-Autorisierungscode-Flows ermöglicht den Zugriff auf eine Ressource über REST. Das Autorisierungscode-Framework ruft das Zugriffstoken über die autorisierte URL ab, die der Benutzer konfiguriert, anstatt dass der Benutzer einen Benutzernamen/ein Passwort eingeben muss. Benutzername/Passwort werden niemals für den Client verfügbar gemacht, der Zugriff auf die Ressource anfordert.

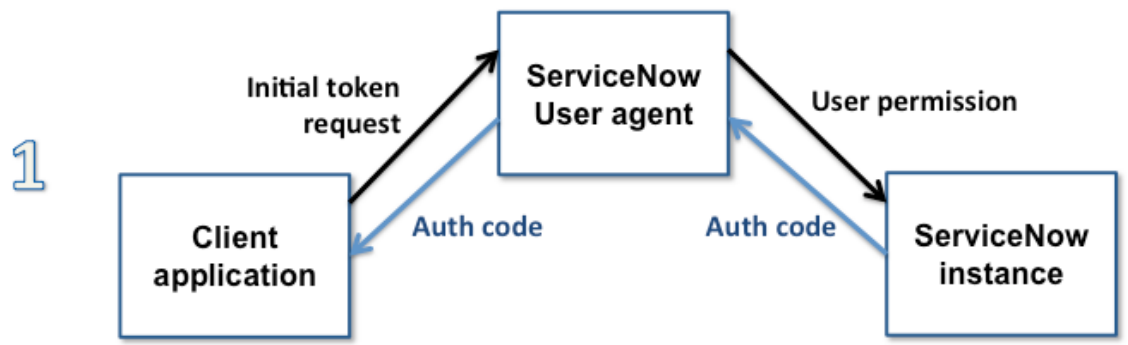
Eine ServiceNow -Instanz als Autorisierungsserver

Der OAuth-Server ist normalerweise ein Autorisierungsserver einer Drittpartei. Sie können auch eine ServiceNow -Instanz als Autorisierungsserver angeben, der die Token für den Autorisierungscode-Flow ausgibt.

Der Benutzer, der die eingeschränkte Ressource besitzt, muss den Zugriff autorisieren. Der Benutzer kann das ausgegebene Zugriffstoken auch jederzeit widerrufen, um den Zugriff zu beenden.

Flow-Prozess für Autorisierungscode-Gewährung

Der Flow-Prozess für die Autorisierungscode-Gewährung besteht aus diesen drei Schritten:



In Schritt 1 initiiert die Clientanwendung oder Website einen REST-API-Aufruf in Form einer GET-Anforderung an die Instanz über den Benutzeragenten. Normalerweise wird der REST-Aufruf initiiert, wenn der Endbenutzer in der Clientanwendung oder auf der Website auf eine Schaltfläche oder einen Link klickt, um ein Zugriffstoken anzufordern. In der Clientanwendung muss der Endbenutzer auch die Autorisierungs-URL, die Token-URL, die Client-ID und den geheimen Clientschlüssel angeben. Eine Erklärung dieser Elemente finden Sie in den Feldbeschreibungen in diesem Thema: OAuth-Drittpartei verwenden . Wenn der Client einen Gewährungstyp anfordert, muss der Endbenutzer **Autorisierungscode**auswählen.

Beispiel für eine GET-Anforderung von der Client-Anwendung an die Instanz:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

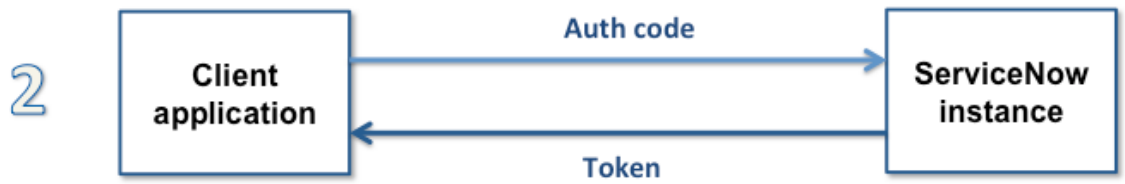
Hinweis:
„ **response_type** “ muss **Code** sein, um den standardmäßigen OAuth-Code-Gewährungs-Flow zu verwenden.

Der Endbenutzer muss den Zugriff auf die eingeschränkte Ressource in der Instanz manuell zulassen. In der ServiceNow -Implementierung muss der Endbenutzer bei der Instanz angemeldet sein. Die Instanz fordert den Endbenutzer auf einer UI-Seite mit den Schaltflächen **Zulassen** und **Ablehnen** auf. Anweisungen finden Sie unter.

Das Element, von dem die Client-Anwendung tatsächlich das Token anfordert, ist der von Ihnen erstellte Registrierungsdatensatz der OAuth-Provider-Anwendung, der auch als Autorisierungsendpunkt bezeichnet wird (siehe OAuth-Drittpartei verwenden). Der Authentifizierungscode wird vom Autorisierungsendpunkt an den Client gesendet. Sie geht nicht direkt an den Client, sondern an die **Umleitungs-URL**, die Sie im Formular „Autorisierungsendpunkt“ angeben. Diese URL wird auch als Rückruf-URL bezeichnet. Sie können diese URL von der Clientanwendung oder der Website abrufen.

Beispielantwort der Instanz an die Clientanwendung mit Bereitstellung eines Autorisierungscodes:

```
https/http://{callbackURL}?code={the actual auth code}
```



Sobald die Client-Anwendung über den Autorisierungscode verfügt, verwendet der Client den Code, um das Zugriffstoken anzufordern. Der Autorisierungscode beweist, dass der Benutzer in Schritt 1 zugestimmt hat.

Beispiel-POST-Anforderung von der Client-Anwendung an die Instanz ServiceNow, die den Authentifizierungscode bereitstellt und das Zugriffstoken anfordert:

```
https://myinstance.service-now.com/oauth_token.do?grant_type=authorization_code&code={the auth
 code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_identifier}&client_secret={client_secret_value}
```

Der Endpunkt in der Instanz gibt ein Zugriffstoken und ein Aktualisierungstoken zurück. Das Aktualisierungstoken kann verwendet werden, um zusätzliche Zugriffstoken anzufordern.

Sie können die Token in der -Instanz verwalten, einschließlich des Widerrufs des Tokens. Siehe OAuth-Token verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Client-Anwendung verwendet das Zugriffstoken, um sich bei der REST-API zu authentifizieren. Nach der Authentifizierung der Client-Anwendung gibt die REST-API die angeforderten Daten in einer JSON-Nutzlast zurück.

Beispiel für eine GET-Anforderung für die JSON-Nutzlast von Daten für die Tabelle „Incident“ [incident]:

```
https://myinstance.service-now.com/api/now/table/incident?access_token={the_token}
```

Hinweis:
Das System unterstützt auch implizite OAuth-Gewährungen, die auch als impliziter Gewährungscode-Flow bezeichnet werden.

Integrationsunterstützung

Der Autorisierungscode-Flow unterstützt die folgenden Integrationen in der Instanz:

- Multi-SSO
- SAML 2.0 Update 1
- Multifaktor-Authentifizierung

Die mobile Schnittstelle wird ebenfalls unterstützt.

Autorisieren Sie den Zugriff auf einen OAuth-Endpunkt mithilfe des Authentifizierungscode-Flows

Endbenutzer, die eine geschützte Ressource in der Instanz ServiceNow besitzen, müssen den Zugriff auf die Ressource autorisieren, bevor die Instanz das Zugriffstoken bereitstellen kann.

Vorbereitungen

Erforderliche Rolle: keine Sie müssen bereits bei der Instanz angemeldet sein, die die geschützte Ressource enthält. Alternativ können Sie sich mit der Authentifizierungsmethode (z. B. Multifaktor-Authentifizierung oder SAML) anmelden, die Ihr ServiceNow -Administrator bereits eingerichtet hat.

Prozedur

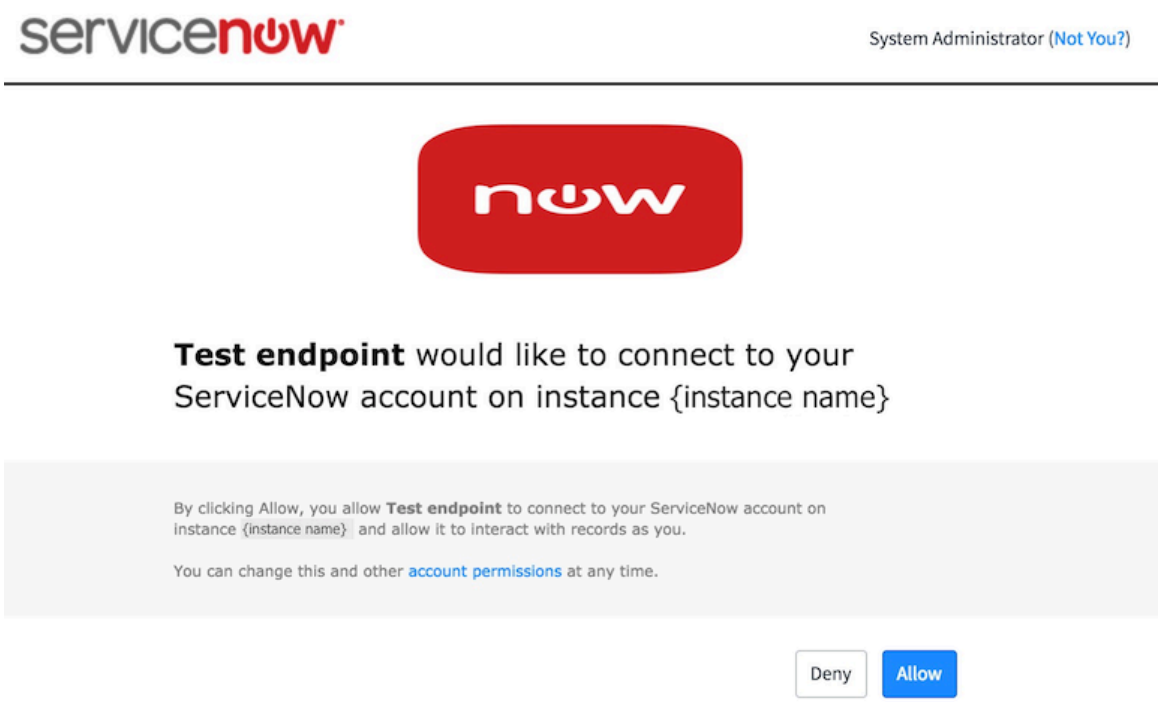
1. Klicken Sie auf den Link oder die Schaltfläche in der Client-Anwendung, in der Sie Zugriff auf die geschützte Ressource in der Instanz anfordern.
   Dadurch wird die Tokenanforderung ausgelöst. Wenn Sie einen REST-Aufruf von einer Instanz zu einer anderen durchführen, lautet der Link **OAuth-Token** abrufen im Formular „REST-Nachricht“.
2. Wenn Sie nicht angemeldet sind, melden Sie sich jetzt an.
   Wenn Sie nicht derselbe Benutzer sind wie der in der rechten oberen Ecke angegebene Benutzer, klicken Sie auf **Nicht Sie?** und melden Sie sich an.
3. Klicken Sie auf Kontoberechtigungen, um die Liste der bereits ausgegebenen Zugriffstoken zu öffnen.
   Dies ist identisch mit **Selfservice** > **Mein verbunden** -App-Token-Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken **Sie** auf Zulassen, um den Zugriff zuzulassen und die Instanz den Autorisierungscode (bei Verwendung des Authentifizierungscode-Flows) oder das Zugriffstoken (bei Verwendung des impliziten Gewährungstyps) auszugeben.

   Wenn Sie auf **Ablehnen klicken**, ist die Autorisierung nicht zulässig, Sie werden jedoch nicht von der Instanz abgemeldet.



   Eine Nachricht, die den Zugriff bestätigt, sollte angezeigt werden. Wenn Sie Zugriff über das Formular „REST-Nachricht“ für eine Instanz anfordern, wird die folgende Meldung oben im Formular angezeigt: OAuth-Aktualisierungstoken ist verfügbar und läuft am {Datum} ab.

Anforderung für Statusparameter des Autorisierungscode-Flows

Die Systemeigenschaft glide.oauth.state.paramater.required ermöglicht es, dass der Parameter State in einer OAuth-Anforderung für den Autorisierungscode-Flow erforderlich ist.

Statusparameter

Erforderliche Rolle: keine

Ab dem Madrid-Release fügt die Systemeigenschaft *`glide.oauth.state.parameter.required`* einen State-Parameter für eine OAuth-Anforderung hinzu. Für Instanzen mit zBoot ist die Eigenschaft true. Bei aktualisierten Instanzen ist die Eigenschaft nicht vorhanden, daher ist der Parameter State nicht aktiviert. Der State-Parameter ist ein Zeichenfolgenwert und darf keine Sonderzeichen enthalten. Der State-Parameter darf nicht leer oder „ “ sein.

Statusparameter werden validiert

Erstellen Sie einen Endpunkt, über den Clients auf die Instanz zugreifen können. Initiieren Sie einen Autorisierungscode-Flow für eine oauth_auth.do. Beispiel:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=
e9dba45b380d1300e676ccc91cef468f&response_type=code
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie den Statusparameter in der Anforderung nicht angeben, erhalten Sie einen Fehler, und der Autorisierungscode wird nicht zurückgegeben.Statusparameter in Anforderung fehlt.

Statusparameter wird der Anforderung hinzugefügt:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```

Durch das Hinzufügen des Parameters State werden Sie zum Anmeldebildschirm weitergeleitet, und der reguläre Autorisierungscode-Flow gibt den Autorisierungscode zurück.

Hinweis:
Die Antwort-URL enthält den in der Anforderung übergebenen Statusparameter. Im Beispiel lautet der hinzugefügte Parameter `state=123`.

Wenn der Autorisierungscode-Flow von oauth_initiator.do beginnt:

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_context=sys_rest_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```

Der State-Parameter wird automatisch hinzugefügt, wenn er von oauth_auth.do umgeleitet wird.

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=-790938844&redirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc91cef468f
```

Beispiel für den Autorisierungscode-Flow: ServiceNow Instanz als Autorisierungsserver

Sie können eine Instanz als Autorisierungsserver verwenden, um mithilfe des Autorisierungscode-Flows Token an einen Client auszugeben.

Vorbereitungen

Erforderliche Rolle: keine

In diesem Beispiel werden zwei Instanzen verwendet: eine als Autorisierungsserver und die andere als Client. Eine Instanz verwendet einen REST-Aufruf, um Token von einer anderen Instanz anzufordern.

Sie müssen Aktivieren Sie OAuth für beide Instanzen verwenden.

Prozedur

1. Navigieren Sie in der Autorisierungsserverinstanz (mit der Istanbul oder höher ausgeführt wird) zu **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken **Sie auf Einen OAuth-API-Endpunkt für externe Clients erstellen**.
3. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz wie in Erstellen Sie einen Endpunkt, über den Clients auf die Instanz zugreifen könnenbeschrieben aus.
   Wenn Sie diese Schritte ausführen, wird ein Autorisierungsserver eingerichtet. Befolgen Sie die nächsten Schritte, um den Client-Server einzurichten.
4. Navigieren Sie in der Client-Instanz zu **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
5. Klicken Sie **auf Verbindung mit einem externen OAuth-Provider herstellen**.
6. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz wie in beschrieben aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie die folgenden Feldwerte:

- **Name**: Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie OAuth-Zugriff benötigen.
- **Client-ID**: Client-ID des Anwendungsregistrierungsdatensatzes, den Sie für den Autorisierungsserver erstellt haben.
- **Geheimer Clientschlüssel**: [Schreibgeschützt] Die automatisch generierte eindeutige ID der Anwendung. Die Instanz verwendet die Client-ID, wenn ein Zugriffstoken angefordert wird.
- **Standardgewährungstyp**: Wählen Sie **Autorisierungscode aus**.
- **Autorisierungs-URL**: URL der Instanz, die der Autorisierungsserver ist. Denken Sie daran, `oauth_auth.do` am Ende der URL anzuhängen.
- **Logo-URL**: Die URL, die ein Bild enthält, das als Anwendungslogo verwendet werden soll. Das Logo wird auf der Genehmigungsseite angezeigt, wenn der Benutzer eine Anforderung erhält, einer Client-Anwendung Zugriff auf eine eingeschränkte Ressource in der Instanz zu gewähren.
- **Token-URL**: URL der Instanz, die der Autorisierungsserver ist. Denken Sie daran, `oauth_token.do` am Ende der URL anzuhängen.
- **Umleitungs-URL**: URL der Instanz: der Client-Server-Instanz. Denken Sie daran, `oauth_redirect.do` am Ende der URL anzuhängen.

7. Erstellen Sie ein Profil für den Datensatz mit dem Gewährungstyp **Autorisierungscode**.
   Der Clientserver ist eingerichtet. Sie können jetzt eine ausgehende REST-Nachricht erstellen und ein OAuth-Token abrufen.

Erstellen Sie einen Endpunkt, über den Clients auf die Instanz zugreifen können

Erstellen Sie einen OAuth-Anwendungsendpunkt für externe Clientanwendungen, um auf die Instanz ServiceNow zuzugreifen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken Sie auf der Interceptor-Seite auf **Einen OAuth-API-Endpunkt für externe Clients erstellen**, und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie OAuth-Zugriff benötigen.
Client-ID	[Schreibgeschützt] Die automatisch generierte eindeutige ID der Anwendung. Die Instanz verwendet die Client-ID, wenn ein Zugriffstoken angefordert wird.
Geheimer Clientschlüssel	[Erforderlich] Die gemeinsame geheime Zeichenfolge, die sowohl die Instanz als auch die Clientanwendung oder Website verwenden, um die Kommunikation untereinander zu autorisieren. Die Instanz verwendet den geheimen Clientschlüssel, wenn sie ein Zugriffstoken anfordert. Lassen Sie dieses Feld leer, damit die Instanz automatisch einen geheimen Clientschlüssel generiert. Um vorhandene geheime Clientschlüssel anzuzeigen, klicken Sie auf das Sperrsymbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Umleitungs-URL	Die Rückruf-URL, an die der Autorisierungsserver umleitet. Geben Sie die vollständigen URLs der Clients ein, die Zugriff auf die Ressource anfordern, und fügen Sie /oauth_redirect.do hinzu. Beispiel: http://token_consumer:port/oauth_redirect.do. Geben Sie so viele URLs wie erforderlich für alle möglichen Token-Verbraucher ein. Die Instanz gleicht die URL der eingehenden Anforderung mit einer der Umleitungs-URLs ab. Wenn keine Übereinstimmung gefunden wird, verwendet die Instanz die erste Umleitungs-URL.
Logo-URL	Die URL, die ein Bild enthält, das als Anwendungslogo verwendet werden soll. Das Logo wird auf der Genehmigungsseite angezeigt, wenn der Benutzer eine Anforderung erhält, einer Client-Anwendung Zugriff auf eine eingeschränkte Ressource in der Instanz zu gewähren.
Aktiv	Aktivieren Sie die Checkbox, um die Anwendungsregistrierung zu aktivieren.
Lebensdauer von Aktualisierungstoken	Die Anzahl der Sekunden, für die ein Aktualisierungstoken gültig ist. Die Instanz verwendet den Lebensdauerwert, wenn ein Aktualisierungstoken angefordert wird. Standardmäßig laufen Aktualisierungstoken in 100 Tagen (8640000 Sekunden) ab.
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur die Verwendung von Token mit APIs zuzulassen, die so festgelegt sind, dass sie das Authentifizierungsprofil zulassen. Sie können den Gewährungszugriff mithilfe einer API-Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter REST API-Zugriffsrichtlinien erstellen. Standard: Deaktiviert.
Mobile-Client	Stellt die Entität für Mobile-App oder Web dar. Diese Informationen werden verwendet, um die Anmeldeinformationen für Mobilgeräte oder das Web zu analysieren.
Lebensdauer von Zugriffstoken	Die Anzahl der Sekunden, für die ein Zugriffstoken gültig ist. Die Instanz verwendet den Lebensdauerwert, wenn ein Zugriffstoken angefordert wird. Standardmäßig laufen Zugriffstoken in 30 Minuten (1800 Sekunden) ab.
Kommentare	Die der Anwendung zuzuordnenden Informationen.

3. Klicken Sie auf **Absenden**.

Ergebnisse

Das System erstellt in der Tabelle „Anwendungsregistrierungen“ [oauth_entity] einen Datensatz vom Typ OAuth-Client. Wenn die Instanz tatsächlich Token und Autorisierungscodes ausgibt, werden diese in der Tabelle gespeichert. Weitere Informationen finden Sie unter OAuth-Token verwalten.

OAuth-API-Antwortparameter

Die OAuth 2.0-API erzeugt eine JSON-Antwort, die die folgenden Parameter als name:value-Paare enthält.

Antwortparameter für Zugriffstoken

Antwortparameter	Beschreibung
scope	Umfang des vom Zugriffstoken gewährten Zugriffs. Der Bereich ist immer **useraccount**, was bedeutet, dass das Zugriffstoken dieselben Rechte hat wie der Benutzeraccount, der das Token autorisiert hat. Wenn Abel Tuter beispielsweise eine Anwendung durch Bereitstellung von Anmeldeinformationen autorisiert, gewährt das

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortparameter für Zugriffstoken (Fortsetzung)

Antwortparameter	Beschreibung
	resultierende Zugriffstoken dem Token-Bearer dieselben Zugriffsberechtigungen wie Abel Tuter.
token_type	Typ des von der Anforderung ausgegebenen Tokens, wie im OAuth-RFC definiert. Der Tokentyp ist immer **Bearer**, was bedeutet, dass jeder, der im Besitz des Zugriffstokens ist, auf eine geschützte Ressource zugreifen kann, ohne einen kryptografischen Schlüssel anzugeben. Unter RFC6750 finden Sie weitere Informationen darüber, wie OAuth 2.0 Bearer-Token verwendet.
läuft ab_in	Lebensdauer des Zugriffstokens in Sekunden.
refresh_token	Zeichenfolgenwert des Aktualisierungstokens.
access_token	Zeichenfolgenwert des Zugriffstokens. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Zugriffstokens gestellt werden, geben immer das aktuelle Zugriffstoken zurück.
format	[Optional] Ausgabeformat der Antwort. Dieser Wert ist immer JSON.

Hinweis:
Wenn ein OAuth-Provider den Antworttext als „Inhaltstyp“ anstelle von „Inhaltstyp“ sendet, analysiert der OAuth-HTTP-Client die Antwort möglicherweise nicht richtig. Um dieses Problem zu beheben, erstellen Sie eine Systemeigenschaft mit diesen Parametern.

Feld	Wert
Name	glide.oauth.inhouse.httpclient.enabled
Typ	Wahr|Falsch
Wert	false

Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaften hinzufügen

Das folgende Beispiel zeigt die JSON-Zeichenfolge, die von einer Zugriffstokenanforderung zurückgegeben wird. (Leerzeichen wurden hinzugefügt, um die Lesbarkeit zu verbessern).

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FM
xHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyxshU9mMQ
13gJHtxD2fy"}
```

OAuth-API-Anforderungsparameter

Erfahren Sie mehr über die OAuth-API-Anforderungsparameter, die von Zugriffstokenanforderungen verwendet werden.

Hinweis:
Der Inhaltstyp der OAuth-API muss `application/x-www-form-urlencoded sein`. Ein Inhaltstyp von `application/json` führt zu einem nicht angegebenen Fehler.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungsparameter für Zugriffstoken

Anforderungsparameter	Beschreibung
grant_type	[Erforderlich] Der Typ der Anmeldeinformationen, die die Anforderung für ein Zugriffstoken autorisieren. Dieser Parameter muss einen der folgenden Werte haben: • **password**: Eine Reihe von Benutzeranmeldeinformationen zum Autorisieren der Zugriffstokenanforderung. Geben Sie die Benutzeranmeldeinformationen in den Parametern username und password an. • **refresh_token**: Ein vorhandenes Aktualisierungstoken autorisiert die Zugriffstokenanforderung. Geben Sie das Aktualisierungstoken im Parameter refresh_token an.
client_id	[Erforderlich] Automatisch generierte eindeutige ID der Clientanwendung, die das Zugriffstoken anfordert.
client_secret	[Erforderlich] Zeichenfolge des gemeinsamen geheimen Schlüssels, die die Instanz und die OAuth-Anwendung verwenden, um die Kommunikation miteinander zu autorisieren.
username	Name des Benutzerkontos, der die Zugriffstoken-Anforderung autorisiert. Dieser Parameter ist für Zugriffstokenanforderungen mit **grant_type** von **password**erforderlich.
Kennwort	Passwort für das Benutzerkonto, das die Zugriffstoken-Anforderung autorisiert. Dieser Parameter ist für Zugriffstokenanforderungen mit **grant_type** von **password**erforderlich.
refresh_token	Vorhandenes Aktualisierungstoken, das die Zugriffstokenanforderung autorisiert. Dieser Parameter ist für Zugriffstokenanforderungen mit einem **grant_type** von **refresh_token erforderlich**.

Anforderungen mit Benutzeranmeldeinformationen

Für die Instanz müssen Clients Anmeldeinformationen angeben, wenn sie den Client zum ersten Mal autorisieren oder die Erstellung eines neuen Aktualisierungstokens autorisieren. Dieser Anforderungstyp gibt immer zwei Token zurück:

- Ein Zugriffstoken
- Ein Aktualisierungstoken

Die Instanz überprüft, ob der Benutzer aktiv und derzeit nicht ausgesperrt ist und eine interaktive Sitzung hat. Wenn eine dieser Bedingungen „falsch“ ist, generiert die Instanz kein Zugriffstoken. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Zugriffstokens gestellt werden, geben immer das aktuelle Zugriffstoken zurück.

Hinweis:
Diese Art der Autorisierung basiert auf der TLS-Verschlüsselung, um die Benutzeranmeldeinformationen während der Übertragung zu schützen.

Das folgende Beispiel zeigt die Anforderung eines Zugriffstokens mit einem Satz von Benutzeranmeldeinformationen (Leerzeichen wurden hinzugefügt, um die Lesbarkeit zu verbessern).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

Anforderungen mit einem Aktualisierungstoken

Die Instanz kann ein vorhandenes Aktualisierungstoken verwenden, um ein neues Zugriffstoken zu erstellen. Dieser Anforderungstyp gibt nur ein Zugriffstoken zurück. Die Instanz bestätigt, dass das Aktualisierungstoken nicht abgelaufen ist, bevor ein neues Zugriffstoken generiert wird. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Aktualisierungstokens gestellt werden, geben immer das aktuelle Aktualisierungstoken zurück. Die Übertragung von Aktualisierungstoken ist im Allgemeinen sicherer als die Übertragung von Benutzeranmeldeinformationen. Das folgende Beispiel zeigt die Anforderung eines Zugriffstokens mit einem vorhandenen Aktualisierungstoken (Leerzeichen wurden hinzugefügt, um die Lesbarkeit zu verbessern).

```
$ curl -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FM
xHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

Einen OAuth-JWT-API-Endpunkt für externe Clients erstellen

Erstellen Sie einen OAuth-JSON-Web-Token-API-Endpunkt (JWT), um externen Clients den Zugriff auf Ihre ServiceNow -Instanz mit Web-Token zu ermöglichen.

Vorbereitungen

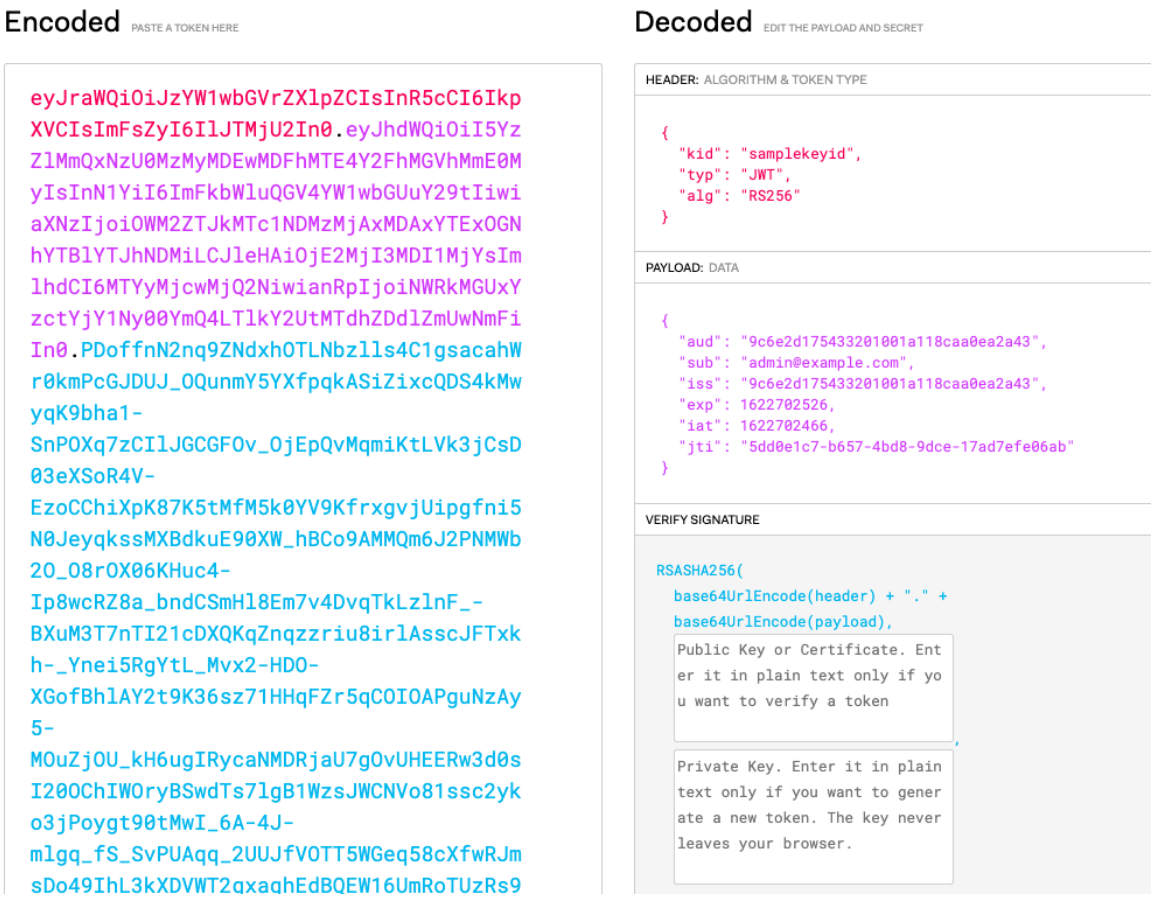
Erforderliche Rolle: admin

Generieren Sie ein JSON-Web-Token (JWT) mit den folgenden Ansprüchen:

- `aud`: Muss mit dem Wert der Client-ID übereinstimmen.
- `sub`: Muss ein Benutzerbezeichner sein, z. B. die E-Mail-Adresse des Benutzers, dem Sie das Token zuordnen möchten.
- `iss`: Empfohlen, um dem Wert der Client-ID zu entsprechen.
- `exp`: Beliebiger Ablauf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für decodiertes JSON-Web-Token



Weitere Informationen zu JSON-Web-Token finden Sie unter https://jwt.io/ .

Warum und wann dieser Vorgang ausgeführt wird

Lassen Sie zu, dass sich externe Webanwendungen nahtlos mit dem eingehenden JWT-Gewährungstyp bei Ihrer Instanz authentifizieren, anstatt dass sich der Endbenutzer manuell anmelden muss. Bei Verwendung des JWT-Gewährungstyps wird das Passwort nicht in die Anforderung aufgenommen, was eine höhere Sicherheit zwischen Webservices ermöglicht. Sie können beispielsweise eine externe Anwendung entwickeln und Token verwenden, um eingehende Anforderungen an Ihre Instanz ServiceNow zu authentifizieren.

Prozedur

1. Erstellen Sie ein Schlüsselpaar, und fügen Sie den öffentlichen Schlüssel der Tabelle „X.509-Zertifikate“ (sys_certificate) hinzu.
2. Richten Sie die Konfiguration in Ihrer Instanz ServiceNow ein, um das eingehende JWT zu überprüfen.
   a. Navigieren zu **System-OAuth** > **Applikationsregistrierung**.
   b. Wählen **Sie OAuth-JWT-API-Endpunkt für externe Clients erstellen aus**.
   c. Füllen Sie das Formular mit Informationen zu Ihrem Token aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth-JWT-Tabelle

Feld	Beschreibung
Name	Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie JWT OAuth-Zugriff benötigen.
Client-ID	Automatisch generierte eindeutige ID der Anwendung. Das System verwendet den Wert dieses Felds, um den öffentlichen oder freigegebenen Schlüssel abzurufen und das JWT zu validieren. Der Wert dieses Felds muss mit dem Wert der Aussteller- und Zielgruppenansprüche im JWT übereinstimmen.
Geheimer Clientschlüssel	Die gemeinsame geheime Zeichenfolge, die sowohl die Instanz als auch die Clientanwendung oder Website verwenden, um die Kommunikation miteinander zu autorisieren. Lassen Sie dieses Feld leer, damit die Instanz automatisch einen geheimen Clientschlüssel generiert. Um vorhandene geheime Clientschlüssel anzuzeigen, klicken Sie auf das Sperrsymbol. **Hinweis:** Wenn **Öffentlicher Client** ausgewählt ist, können Sie den **geheimen**Clientschlüssel auslassen.
Logo-URL	Die URL, die ein Bild enthält, das als Anwendungslogo verwendet werden soll. Das Logo wird auf der Genehmigungsseite angezeigt, wenn der Benutzer eine Anforderung erhält, einer Client-Anwendung Zugriff auf eine eingeschränkte Ressource in der Instanz zu gewähren.
Benutzerfeld	Feld in der Benutzertabelle (sys_user), das vom System verwendet wird, um den Wert des betreffenden Anspruchs im JWT abzugleichen. Wenn Sie beispielsweise ein Token hinzufügen, dessen Anspruchswert user.name@example.com lautet, legen Sie das **Benutzerfeld** auf E-**Mail**fest. Dieses Feld weist das System an, das E-Mail-Feld nach dem Wert user.name@example.com zu durchsuchen und den übereinstimmenden Benutzerdatensatz in der eingehenden Anforderung zu verwenden.
JTI-Verifizierung aktivieren	Wählen Sie diese Option aus, um bei jedem Token-Austausch ein neues Token zu erfordern. Standard: Ausgewählt.
Anwendung	Schreibgeschützter Anwendungsbereich.
Zugänglich von	Bereichsübergreifende Zugriffsrichtlinie. Weitere Informationen finden Sie unter Anwendungszugriffseinstellungen .
Lebensdauer von Zugriffstoken	Zeitraum, für den das Token gültig ist. Einheit: Sekunden
Taktversatz	Zulässige Zeitdifferenz zwischen den Server- und Clientuhren bei der Validierung der Ansprüche „ exp “ und „nbf“ im JWT. Einheit: Sekunden Standard: 300
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur die Verwendung von Token mit APIs zuzulassen, die so festgelegt sind, dass sie das Authentifizierungsprofil zulassen. Sie können den Gewährungszugriff mithilfe einer API-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter REST API-Zugriffsrichtlinien erstellen. Standard: Deaktiviert.
Kommentare	Die der Anwendung zuzuordnenden Informationen.
Öffentlicher Client	Fügen Sie dieses Feld dem Formular hinzu, wenn der JWT-Client öffentlich ist. Wenn diese Option ausgewählt ist, müssen Sie keinen **geheimen Clientschlüssel angeben**. Standard: Deaktiviert.

d. Speichern Sie das Formular.

e. Fügen Sie der zugehörigen Liste „JWT-Verifizierungszuordnungen“ Datensätze hinzu, um die JWT-Signatur zu überprüfen.

Tabelle „JWT-Verifizierungszuordnungen“.

Feld	Beschreibung
Name	Name des JWT-Zuordnungsdatensatzes.
Kind	Schlüssel-ID aus dem JWT.
Freigegebener Schlüssel	Der freigegebene Schlüssel für die angegebene Schlüssel-ID.
Anwendung	Schreibgeschützter Anwendungsbereich.
Sys-Zertifikat	Zertifikatdatensatz in der Tabelle „X.509-Zertifikate“ (sys_certificate).

f. Fügen Sie alle benutzerdefinierten Ansprüche, die Ihrem JWT zugeordnet sind, der zugehörigen Liste „OAuth-JWT-Anspruchsvalidierungen“ hinzu.

Für die folgenden erforderlichen Ansprüche müssen Sie keine Datensätze hinzufügen:

- ist
- aud
- Sub
- ab

Tabelle „OAuth-JWT-Anspruchsvalidierungen“.

Feld	Beschreibung
Mein externer Client	Wird automatisch mit dem OAuth-JWT-Datensatz ausgefüllt.
Anspruchwerttyp	Datentyp des Anspruchswerts.
Anspruchname	Name des Anspruchs, den Sie hinzufügen möchten.
Anspruchwert	Wert des Anspruchs.
Anwendung	Schreibgeschützter Anwendungsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Senden Sie eine cURL-Anforderung, die das JWT-Token enthält, um ein Zugriffstoken von Ihrer Instanz zu erhalten.

Example

Das Folgende ist ein cURL-Beispielbefehl, der ein Zugriffstoken anfordert:

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

Wenn der JWT-Client ein öffentlicher Client ist, z. B. Mobile SDK, können Sie die Parameter client_id und client_secret in der Anforderung weglassen. Das Folgende ist ein Beispiel für einen cURL-Befehl, der ein Zugriffstoken anfordert, bei dem client_id und client_secret ausgelassen werden:

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

Die Instanz gibt das Zugriffstoken in ihrer Antwort zurück:

```
{
   "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxNA",
   "scope": "useraccount",
   "token_type": "Bearer",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "expires_in": 1799
}
```

Hinweis:
Der eingehende JWT-Gewährungstyp enthält keine Aktualisierungstoken.

4. Führen Sie einen REST-API-Aufruf durch, um mit dem Zugriffstoken auf eine Ressource zuzugreifen.

Example

Das Folgende ist ein cURL-Befehl für den Zugriff auf die Incident-Tabelle mit dem Token.

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

Ergebnisse
Das System ruft das Zugriffstoken im REST-Aufruf ab und ermöglicht den Zugriff auf die angeforderte Ressource.

Konfigurieren Sie einen OAuth-OIDC-Provider auf der Now Platform

Sie können einen OAuth-OIDC-Provider so konfigurieren, dass Identitätstoken akzeptiert werden, die von einem OIDC-Provider einer Drittpartei mithilfe eingehender API-Aufrufe oder unserer Single Sign-on-Option (Mehrfachanbieter-SSO) generiert wurden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Now Platform unterstützt OIDC durch unsere externe SSO-Implementierung (Single Sign-on) zusätzlich zu eingehenden API-Aufrufen. Ein Beispiel für eine OIDC-Provider-Konfiguration finden Sie unter Azure AD einrichten. Ein SSO-spezifisches Beispiel für eine OIDC-Provider-Konfiguration finden Sie unter OpenID Connect (OIDC)-Konfigurationen für Single Sign-on (SSO) erstellen.

Prozedur
1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**.
   - Klicken Sie auf **Neu**, klicken Sie auf **Konfigurieren Sie einen OIDC-Provider, um ID-Token zu überprüfen**, und füllen Sie dann das Formular aus.
   - Wählen Sie eine vorhandene Vorlage für einen OIDC-Provider aus (ADFS, Auth0, Azure AD, Google, Okta), und füllen Sie das Formular aus.

Hinweis:
OIDC-Provider-Vorlagen sind nach dem Laden von Demodaten mit dem Plugin OAuth 2.0 verfügbar.

Feld	Beschreibung
Name	Ein eindeutiger Name, der die OAuth-OIDC-Entität identifiziert.
Client-ID	Client-ID der Anwendung, die beim OAuth-OIDC-Server des Drittanbieters registriert ist. Die Instanz verwendet die Client-ID, wenn ein Zugriffstoken angefordert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim OAuth-OIDC-Server des Drittanbieters registriert ist.
OAuth-API-Skript	Ein Skript, mit dem Sie Anforderungen und Antworten an einen externen OAuth-Provider anpassen können.
OAuth-OIDC-Providerkonfiguration	Der OIDC-Provider (ADFS, Auth0, Azure AD, Google, Okta) kann zur Validierung des JWT-Tokens verwendet werden. Klicken Sie auf den Datensatz Ihrer **OIDC** -Provider-Konfiguration, um zu überprüfen, ob der **Benutzeranspruch** und das Benutzerfeld ordnungsgemäß festgelegt sind. Wenn Sie **JTI-Anspruchsverifizierung aktivieren**, validiert die JWT-Tokenvalidierung ServiceNow auch die vom Provider gesendete JTI. **Hinweis:** Wenn die Validierung nicht aktiviert ist, kann die JTI nicht validiert werden, unabhängig davon, ob sie im JWT-Token vorhanden ist.
Taktversatz	Die Anzahl in Sekunden, nach der die Einschränkung als gültig betrachtet wird. Der Standardwert ist 300.
Kommentare	Die der Anwendung zuzuordnenden Informationen.
Anwendung	Der Name der Anwendung, die diese Entität enthält.
Zugänglich von	Wählen Sie eine Option aus, um den Zugriff aus allen Anwendungsbereichen oder nur aus diesem Anwendungsbereich zu ermöglichen.
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur die Verwendung von Token mit APIs zuzulassen, die so festgelegt sind, dass sie das Authentifizierungsprofil zulassen. Sie können den Gewährungszugriff mithilfe einer API-Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter REST API-Zugriffsrichtlinien erstellen. Standard: Deaktiviert.
Aktiv	Aktivieren Sie die Checkbox, um die OAuth-Anwendung zu aktivieren.
Umleitungs-URL	Die URL der OAuth-Anwendung zum Empfangen des Autorisierungscodes.
Endpunkt-URL von „Sitzung beenden“	Der URL-Endpunkt, der nach Beendigung einer Sitzung aktiviert wird.
Aktivieren Sie die Authentifizierung	Option zum Erzwingen der Authentifizierung für Benutzer.

2. Klicken Sie auf **Absenden**.
   Der Datensatz wird in der Tabelle der Anwendungs-Registrys [oauth_entity] gespeichert.
   Wenn Ihre Instanz Token und Autorisierungscodes ausgibt, wird in der Tabelle „Anwendungsregistrierungen“ [oauth_entity] ein Datensatz vom Typ **Externer OIDC-Provider erstellt**.
   Weitere Informationen finden Sie unter .
3. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsprofile“, um ein vom System generiertes Standardprofil für den neuen OAuth-Provider ohne Bereich zu validieren.
   Sie können ein OAuth-Provider-Profil ändern oder hinzufügen, einschließlich Name, Gewährungstyp und OAuth-Bereich.
4. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz OAuth-Entitätsbereiche, um alle verfügbaren OAuth-Bereiche für diesen OAuth-Provider zu definieren.
   Die definierten Bereiche können ausgewählt werden, wenn Sie ein Profil erstellen oder aktualisieren.
   Jeder definierte OAuth-Bereich enthält einen Namen und einen Bereich, den Sie der Anbieterspezifikation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

entnehmen müssen, z. B. einen Lesebereich oder einen Schreibbereich. Jeder Bereich muss separat definiert werden.

5. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz Benutzerbereitstellung, um die automatische Benutzerbereitstellung zu aktivieren.

Option	Bezeichnung
Benutzer automatisch bereitstellen	Option zum Erzwingen der Authentifizierung für Benutzer.
Bereitstellungsdatenquelle	Die Datenquelle, die zum Transformieren eines OIDC-Tokens in einen ServiceNow -Benutzer verwendet werden soll. Verwenden Sie die **Nachschlageliste**, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Transformationstabellenzuordnung zu konfigurieren. Bei der Konfiguration der Transformationszuordnung stammen die Quellfelder aus der Tabelle *JWT token*, die Zielfelder aus der Tabelle *sys_user*.
Auf bereitgestellte Benutzer angewendete Benutzerrollen	Die Benutzerrollen, die auf die neu bereitgestellten ServiceNow Benutzer angewendet werden.

Implizite OAuth-Gewährungen

ServiceNow -Instanzen unterstützen die implizite Gewährung eines Zugriffstokens.

Der implizite Gewährungstyp, auch bekannt als *implicit grant code flow*, ermöglicht die direkte Weitergabe des Zugriffstokens an die Clientanwendung über den Benutzeragenten, in der Regel den Webbrowser oder das Mobilgerät. Es werden keine Aktualisierungstoken gewährt. Der Endbenutzer muss weiterhin Zugriff auf die geschützte Ressource in der Instanz gewähren, genau wie bei Standard.

Flow-Prozess für implizite OAuth-Gewährung

Genau wie beim standardmäßigen Autorisierungscode-Flow fordert die Clientanwendung die Verwendung der eingeschränkten Ressource für die Instanz an und der Endbenutzer genehmigt sie. Die Anforderung wird in Form einer URL an die Instanz gesendet. Die URL muss die folgenden Parameter enthalten:

- client_id =<the necessary client ID> . Dies ist obligatorisch, um zu identifizieren, auf welche geschützte Ressource die Clientanwendung zugreifen möchte.
- response_type = Token. Dies ist obligatorisch, um das Zugriffstoken direkt anzufordern (im Gegensatz zur Anforderung eines Autorisierungscodes). Der Wert muss für implizite Gewährungen token sein. Im Beispiel des standardmäßigen Autorisierungscode-Flows lautet der Antworttyp code.
- routing_uri =<a URL>: Der Speicherort, an den das Token gesendet wird.

Der Autorisierungsserver sendet das Zugriffstoken anstelle eines Autorisierungscodes über den Benutzeragenten an die Clientanwendung.

Hier ist ein Beispiel für eine GET-Anforderung zum Empfangen der JSON-Nutzlast von Daten für die Incident-Tabelle [incident]:

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Benutzer Zugriff gewährt, wird das Token in die Umleitungs-URL (Rückruf-URL) aufgenommen:

```
https/http://{callbackURL}?access_token={the_token}
```

Verwalten Sie OAuth-Token

Öffnen Sie OAuth-Token, um Zugriff auf eingeschränkte Ressourcen bereitzustellen.

Vorbereitungen
Erforderliche Rolle: beliebiger Benutzer oder Administrator

Warum und wann dieser Vorgang ausgeführt wird
Von der Instanz und dem OAuth-Drittanbieter ausgegebene OAuth-Token werden in der Tabelle oauth_credential gespeichert.

Einige der wichtigen Spalten in dieser Tabelle:

- Token: Wert des von der Instanz ServiceNow ausgegebenen Tokens.
- Typ: Bestimmt, ob das Token ein Zugriffstoken oder ein Aktualisierungstoken ist.
- Ablauf: Datum/Uhrzeit, zu dem das Zugriffs- oder Aktualisierungstoken abläuft.
- Token erhalten: Wert des Tokens, das von einem OAuth-Provider einer Drittpartei ausgegeben wurde. Dieser Wert liegt in einem verschlüsselten Format vor.

Token-Ablauf und -Gültigkeit lauten wie folgt:

- Zugriffstoken: Standardmäßig gibt eine Instanz Zugriffstoken mit einer Lebensdauer von 30 Minuten aus, wenn die Instanz der OAuth-Provider ist.
- Aktualisierungstoken: Standardmäßig gibt eine Instanz Aktualisierungstoken mit einer Lebensdauer von 100 Tagen aus, wenn die Instanz der OAuth-Provider ist.

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - **Selfservice** > **Meine verbundenen Apps** , um die Token anzuzeigen, die die Instanz erstellt hat, als Sie Zugriff auf eine Ressource in der Instanz gewährt haben.
   - **System-OAuth** > **Tokens verwalten** , um alle Token anzuzeigen. Nur Administratoren können auf dieses Modul zugreifen.
2. Klicken Sie auf den **Namen**, um das Token zu öffnen.
3. Klicken Sie auf **Zugriff widerrufen**, um den Zugriff auf die eingeschränkte Ressource zu verhindern.
4. Sie können auch andere Informationen zum Token anzeigen, einschließlich des Bereichs, in dem der Zugriff zulässig ist, und des Ablaufdatums.

Widerrufen Sie ein OAuth-Token

Möglicherweise möchten Sie ein OAuth-Zugriffs- oder -Aktualisierungstoken aus Sicherheitsgründen widerrufen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das Widerrufen des Tokens bezieht sich auf die Situation, in der Ihre Instanz als OAuth-Ressourcenserver fungiert. Sie können das Token über eine URL oder per widerrufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Greifen Sie mit oauth_revoke_token.do auf Ihre Instanz zu, und hängen Sie das Zugriffs- oder Aktualisierungstoken an.

Beispiel: https://[Your_ServiceNow_Instance]:[port]/oauth_revoke_token.do?token=[access or refresh token] ohne die Klammern [ ].

Ergebnisse

Dieser Endpunktzugriff erfordert keine Authentifizierung. Das Token in dieser Anforderung ist als abgelaufen markiert.

Client-Anmeldeinformationen

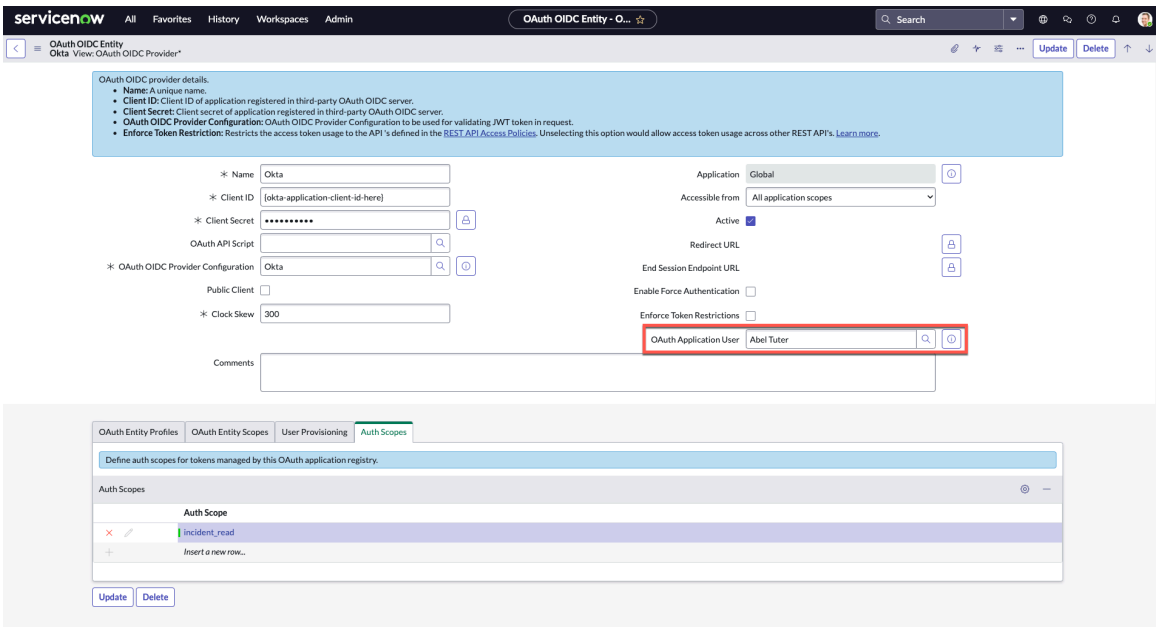
Verwenden Sie den Gewährungstyp OAuth-Client-Anmeldeinformationen für eingehende Integrationen von einem OAuth-Client einer Drittpartei zur ServiceNow® -Plattform.

Administratoren können den Gewährungstyp Client-Anmeldeinformationen (CC) verwenden, um die Integration von einem OAuth-Client einer Drittpartei in die Plattform ServiceNow zu ermöglichen.

Der Gewährungstyp für eingehende Client-Anmeldeinformationen ist eine Fähigkeit, die über eine Systemeigenschaft gesteuert werden kann. Standardmäßig ist die Systemeigenschaft „false“.

Um den Gewährungstyp für Client-Anmeldeinformationen zu verwenden, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie die Systemeigenschaft glide.oauth.inbound.client.credential.rant_type.enabled.
- Fügen Sie dem OAuth-Entitätsformular das Feld OAuth- **Anwendungsbenutzer** hinzu.



Erstellen Sie die Systemeigenschaft „Client-Anmeldeinformationen“.

Erstellen Sie die Systemeigenschaft glide.oauth.inbound.client.credential.rant_type.enabled, um den Gewährungstyp Client-Anmeldeinformationen für eingehende OAuth-Integrationen zu verwenden.

Vorbereitungen

Erforderliche Rolle: admin

Automatische Übersetzung

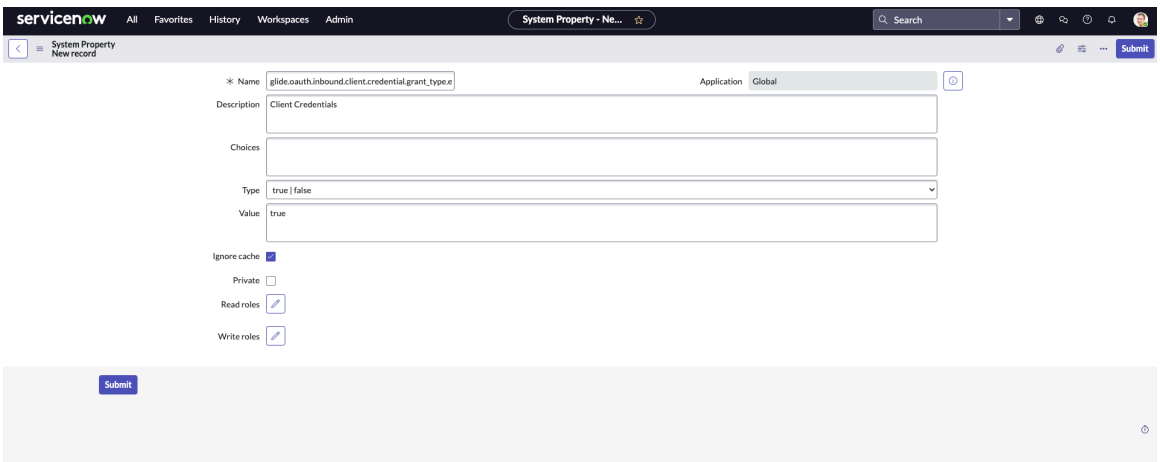
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliches Plugin: OAuth 2.0.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein.
   Die gesamte Liste der Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties] wird angezeigt.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die folgenden Felder aus.

Feld	Beschreibung
Name	Name der Eigenschaft, die Sie erstellen. In diesem Fall glide.oauth.inbound.client.credential.gewähren_typ.aktiviert.
Beschreibung	Geben Sie einen kurzen, beschreibenden Ausdruck ein, der die Funktion der Eigenschaft beschreibt.
Typ	Wählen Sie den entsprechenden Datentyp aus der Liste aus. In diesem Fall `true | false`.
Wert	Legen Sie den gewünschten Wert für die Eigenschaft fest. In diesem Fall „ `true` “, um den Gewährungstyp für Client-Anmeldeinformationen für eingehende OAuth-Integrationen zu aktivieren.



Hinweis:
Andere Felder im Formular wie Auswahlmöglichkeiten, Cache ignorieren, Privat, Leserollen und Schreibrollen können entsprechend Ihren Anforderungenskonfiguriert werden.

4. Wählen Sie **Absenden**.

Hinweis:
Wenn die **Checkbox Cache ignorieren aktiviert** ist, leert das System den Servercache, wenn der Parameter geändert wird.

Als Nächstes müssen Sie einen OAuth-Client erstellen (OAuth-API-Endpunkt für externen Client) und das Feld OAuth-Anwendungsbenutzer zum OAuth-Client-Datensatz hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie den OAuth-Anwendungsbenutzer hinzu

Fügen Sie dem Formular „OAuth-Entität“ das Feld OAuth-Anwendungsbenutzer hinzu, um den Gewährungstyp „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen zu verwenden.

Vorbereitungen

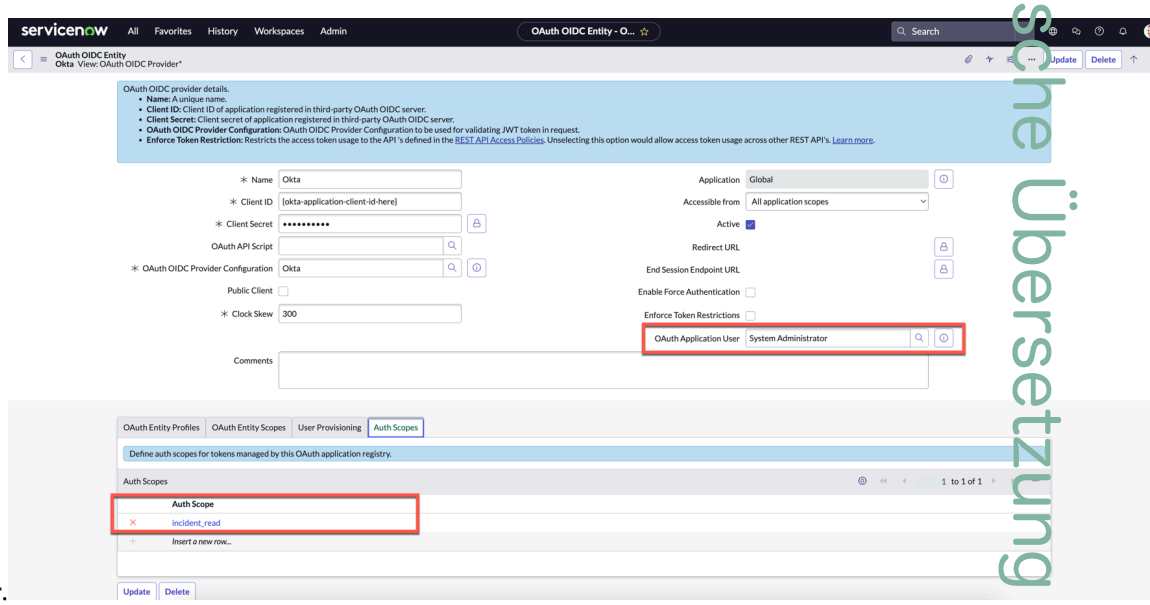
Erforderliche Rolle: admin

Erforderliches Plugin: OAuth 2.0.

Sie müssen einen OAuth-Client erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Endpunkt, über den Clients auf die Instanz zugreifen können.

Prozedur

1. Öffnen Sie den erstellten OAuth-Client-Datensatz.
2. Symbol „Weitere Optionen auswählen“ im Seiten-Header.
3. Auswahlvorgang **Konfigurieren** > **Formulardesign**.
4. Fügen Sie auf der Seite „Formulardesign“ **OAuth-Anwendungsbenutzer** aus der Liste der Felder hinzu.
5. Speichern oder aktualisieren Sie das Formular.
6. Wählen Sie den Benutzer für den **OAuth-Anwendungsbenutzer**aus.
   Beispiel:



Systemadministrator.

> **Hinweis:**
> Sie müssen den REST-API-Auth-Bereich mit dem Gewährungstyp „Client-Anmeldeinformationen“ verwenden, um den Zugriff für den Drittanbieter-Client zu steuern.

7. Speichern oder aktualisieren Sie das Formular.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jede Autorisierungsanforderung mit dem **GewährungstypClient-Anmeldeinformationen**, **Client-ID**und **Geheimnis** wird für den zugeordneten OAuth-Anwendungsbenutzer in ServiceNow®übergeben.

Hinweis:
Wenn der OAuth-Anwendungsbenutzer im OAuth-Client-Datensatz nicht ausgewählt ist oder die Eigenschaft Client-Anmeldeinformationen auf `false`festgelegt ist, wird die Autorisierungsanforderung nicht übergeben.

OAuth ausgehend

Mit OAuth ausgehend können Sie Daten von einem Drittanbieter in Ihre Instanz abrufen.

Um die OAuth-Integration zu verwalten, benötigen Sie die Rolle security_admin.

Sie können ausgehendes OAuth 2.0 für die folgenden Gewährungstypen konfigurieren:

- **Verbindung mit Drittanbieter herstellen: Verwenden Sie die Client-ID und den geheimen Schlüssel, um sie an den OAuth-**Provider zu senden. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu einem externen OAuth-Provider her.
- **JWT Bearer**: Ein Autorisierungsserver validiert ein JWT-Token, das die Weitergabe von Identitäts- und Sicherheitsinformationen zwischen Sicherheitsdomänen ermöglicht. Weitere Informationen finden Sie unter Richten Sie den OAuth-Provider mit dem Gewährungstyp JWT Bearer ein.
- **SAML2 Bearer**: Generiert die SAML2-Assertion und tauscht dann die Assertion für die Zugriffstoken mit dem Provider aus.

  Hinweis:
  Verwenden Sie für ausgehende Anforderungen an SuccessFactors**SAML2 Bearer** als Standardgewährungstyp. Weitere Informationen zur Konfiguration von **SAML2 Bearer**finden Sie im Beispiel in Set up the v4.x.x .

- **Autorisierungscode**: Der Code, der dem Client gewährt wird, um ein Zugriffstoken zu erhalten, das dann verwendet wird, um Zugriff auf die Ressource zu erhalten. Wenn Sie diese Option auswählen, benötigen Sie eine Autorisierungs-URL (die URL des Autorisierungsservers).
- **Anmeldeinformationen des Ressourcenbesitzers**: Der Benutzername und das Passwort des Benutzers, der versucht, auf die Ressource zuzugreifen.
- **Client-Anmeldeinformationen**: Die Client-ID und der Client-Secret, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt.

Sie können das **OAuth-Provider-Szenario** (ausgehend) konfigurieren: Ihre Instanz ruft Daten von einem Drittanbieter ab.

Hinweis:
Sie müssen sich zum ersten Mal als Benutzer authentifizieren, um den Token-Post abzurufen. Sie müssen sich vor Ablauf des Tokens nicht mit einem Benutzerkonto authentifizieren.

Stellen Sie eine Verbindung zu einem externen OAuth-Provider her

Konfigurieren Sie, wie die Client-ID und der geheime Schlüssel an Ihren OAuth-Provider gesendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken Sie auf der Interceptor-Seite **auf Verbindung mit einem OAuth-Drittanbieter herstellen**, und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Eindeutiger Name für die OAuth-Drittpartei-Verbindung
Client-ID	Die Client-ID der Anwendung, die beim OAuth-Server des Drittanbieters registriert ist.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim OAuth-Server des Drittanbieters registriert ist.
OAuth-API-Skript	Das zum Anpassen von Anforderung und Antwort an den externen OAuth-Provider verwendete Skript.
Logo-URL	Die OAuth-Anwendungslogo-URL.
Standardgewährungstyp	Standardgewährungstyp, der zum Erstellen des Tokens verwendet wird. Zur Auswahl stehen: ○ **Autorisierungscode**: Der Code, der dem Client gewährt wird, um ein Zugriffstoken zu erhalten, das dann verwendet wird, um Zugriff auf die Ressource zu erhalten. Wenn Sie diese Option auswählen, benötigen Sie eine Autorisierungs-URL (die URL des Autorisierungsservers). ○ **Anmeldeinformationen des Ressourcenbesitzers**: Der Benutzername und das Passwort des Benutzers, der versucht, auf die Ressource zuzugreifen. ○ **Client-Anmeldeinformationen**: Die Client-ID und der Client-Secret, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt. ○ **JWT Bearer**: Ein Autorisierungsserver validiert ein JWT-Token, das die Weitergabe von Identitäts- und Sicherheitsinformationen zwischen Sicherheitsdomänen ermöglicht. ○ **SAML2 Bearer**: Generiert die SAML2-Assertion und tauscht dann die Assertion für die Zugriffstoken mit dem Provider aus. **Hinweis:** Verwenden Sie für ausgehende Anforderungen an SuccessFactors**SAML2 Bearer** als Standardgewährungstyp.
Lebensdauer von Aktualisierungstoken	Zeit in Sekunden, die das Aktualisierungstoken gültig ist. Die Standardzeit beträgt 8.640.0000 Sekunden.
Öffentlicher Client	Ermöglicht öffentlichen Clients, PKCE für eine Autorisierung zu erfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie können nur den Autorisierungscode als *Default Grant type* verwenden, wenn PKCE aktiviert ist.
Abfragecodemethode	Die im OAuth-PCKE-Workflow verwendete Codeabfragemethode. Zur Auswahl stehen: ○ S256 [Standard] ○ Einfach ○ Keine
Kommentare	Fügen Sie Kommentare zur OAuth-App hinzu.
Anwendung	Anwendung und Bereich, die diesen Datensatz enthalten.
Zugänglich von	Machen Sie diese App aus allen Anwendungsbereichen oder nur aus diesem Bereich zugänglich.
Aktiv	Aktivieren Sie die Checkbox, um die App zu aktivieren.
Autorisierungs-URL	Der OAuth-Autorisierungscode-Endpunkt.
Token-URL	Der OAuth-Servertoken-Endpunkt.
Token-Sperr-URL	Der Endpunkt des OAuth-Server-Tokenwiderrufs.
Umleitungs-URL	Der OAuth-Rückrufendpunkt. Wenn dieses Feld leer ist, generiert die Instanz automatisch einen Eintrag.
Gegenseitige Authentifizierung aktivieren	Aktivieren Sie das Kontrollkästchen, um die gegenseitige Authentifizierung für die Anforderung und den Widerruf von Token zu verwenden. Für diese Funktion muss ein Profil für die gegenseitige Authentifizierung angegeben werden.
Anmeldeinformationen senden	Der OAuth-Client füllt die Client-Anmeldeinformationen in die Anforderung: ○ In Anforderungstext (URL-codiertes Formular) ○ Basic Authorization-Header ○ Als Private Key JWT

Das System erstellt einen Datensatz in der Tabelle „Anwendungsregistrierungen“ [oauth_entity] mit dem Typ OAuth-Provider.

3. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsprofile“, um ein vom System generiertes Standardprofil für den neuen OAuth-Provider ohne Bereich zu validieren.
   Sie können ein OAuth-Provider-Profil ändern oder hinzufügen, einschließlich Name, Gewährungstyp und OAuth-Bereich.
4. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz OAuth-Entitätsbereiche, um alle verfügbaren OAuth-Bereiche für diesen OAuth-Provider zu definieren.
   Sie können die Bereiche auswählen, wenn Sie ein Profil erstellen oder aktualisieren. Jeder OAuth-Bereich enthält einen Namen und einen Bereich, den Sie der Spezifikation des Anbieters entnehmen müssen, z. B. einen Lesebereich oder einen Schreibbereich. Jeder Bereich muss separat definiert werden.

JWT Bearer

JSON Web Tokens (JWTs) ermöglichen die Konfiguration von Server-zu-Server-API-Interaktionen zwischen ServiceNow und externen API-Providern, ohne dass ein Benutzereingriff erforderlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der JSON Web Token (JWT) Bearer Grant ist eine JSON-Zeichenfolge, die Anspruchswerte enthält, die von den JWT Grant Handlern am Ende des Autorisierungsservers ausgewertet und validiert werden, bevor ein Zugriffstoken ausgegeben wird.

Mit dem Gewährungstyp JWT Bearer können Sie den OAuth 2.0 JWT Bearer Gewährungs-Flow für ausgehende REST-Nachrichten konfigurieren.

Richten Sie den OAuth-Provider mit dem Gewährungstyp JWT Bearer ein

JSON Web Tokens (JWTs) ermöglichen die Konfiguration von Server-zu-Server-API-Interaktionen zwischen ServiceNow und externen API-Providern, ohne dass ein Benutzereingriff erforderlich ist. Diese Unterstützung ermöglicht IntegrationHub oder anderen automatisierten Aufgaben mithilfe von JWTs die Konfiguration von API- und Serviceintegrationen mit verschiedenen Anbietern.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Aufgaben zeigen, wie ServiceNow für die Verwendung von JWTs für die OAuth 2.0-Clientauthentifizierung und -Autorisierung eingerichtet werden kann. ServiceNow ist der OAuth-Client, und Sie können einen OAuth-Provider wie Box oder DocuSign konfigurieren.

Prozedur

1. Laden Sie das Java Key Store-Zertifikat hoch
   Hängen Sie ein JKS-Zertifikat an Ihre Instanz an, um die JWT-Client-Authentifizierung zu aktivieren.
2. Konfigurieren Sie einen JWT-Signierschlüssel
   Erstellen Sie einen JWT-Signierschlüssel, um ihn Ihrem JKS-Zertifikat (Java KeyStore) zuzuweisen.
3. Erstellen Sie einen JWT-Provider mit einem JWT-Signierschlüssel
   Fügen Sie Ihrer Instanz ServiceNow einen JWT-Provider hinzu.
4. Stellen Sie eine Verbindung zu einem externen OAuth-Provider her
   Erstellen Sie einen OAuth-Drittpartei-Provider mit einem JWT Bearer als Standardgewährungstyp in der Anwendungs-Registrierung ServiceNow.
5. OAuth-Profile angeben
   Öffnen Sie das OAuth-Entitätsprofil des OAuth-Providers, und weisen Sie einen JWT-Provider zu.

Laden Sie das Java Key Store-Zertifikat hoch

Sie können ein Java KeyStore-Zertifikat (JKS) an Ihre Instanz anhängen, um die JWT-Client-Authentifizierung zu aktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **x509-Zertifikat**.
2. Füllen Sie das Formular nach Bedarf aus.

Option	Bezeichnung
Name	Ein eindeutiger Name für Ihr Zertifikat.
Benachrichtigung bei Ablauf	Legen Sie fest, wer benachrichtigt werden soll, wenn das Zertifikat abläuft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Tage vor Ablauf benachrichtigen	Senden Sie eine E-Mail-Benachrichtigung an Ihren Zertifikatmanager, bevor Ihr Zertifikat abläuft.
Aktiv	Aktiviert die Verwendung des Zertifikats für Token-anforderungen.
Typ	Der Typ des Zertifikats, das Sie hochladen.
Läuft in Tagen ab	Die Anzahl der Tage, bis das Zertifikat abläuft.
Schlüsselspeicher-Passwort	Das dem Zertifikat zugeordnete Passwort.
Kurzbeschreibung	

3. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen JWT-Signierschlüssel

Erstellen Sie einen JWT-Signierschlüssel (JSON Web Token), um ihn Ihrem JKS-Zertifikat (Java KeyStore) zuzuweisen.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis:
Wenn Sie dem Header **X.509-Zertifikat SHA-1-Fingerabdruck int (x5t)** als Teil des JWT-Schlüssels hinzufügen möchten, müssen Sie das Formular konfigurieren und das Feld **X.509-Zertifikat SHA-1-Fingerabdruck int (x5t) hinzufügen**.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Schlüssel**.
2. Füllen Sie das Formular nach Bedarf aus.

Option	Bezeichnung
Name	Ein eindeutiger Name für die JWT-Schlüsselsignaturkonfiguration.
Signatur-Schlüsselspeicher	Der beim Signieren des JWT angegebene Schlüsselspeicher.
Schlüssel-ID	Die Schlüssel-ID (KID) hilft bei der Identifizierung des verwendeten Schlüssels, wenn mehrere Schlüssel zum Signieren von Token verwendet werden. **Hinweis:** Wenn Sie dieses Feld konfigurieren, ist der Schlüssel-ID-Anspruch im JWT enthalten. Wenn Sie dieses Feld nicht konfigurieren, hat Ihr JWT keinen Schlüssel-ID-Anspruch.
Signaturalgorithmus	Der zum Signieren mit dem JWT-Schlüssel zu verwendende Algorithmus. RSA 256 ist der einzige verfügbare Algorithmus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Signaturschlüssel-Passwort	Das dem Signaturschlüssel zugeordnete Passwort.
Aktiv	Legen Sie fest, dass der JWT-Schlüsselalias aktiv von einem JWT-Provider referenziert wird.

3. Klicken Sie auf **Absenden**.

Erstellen Sie einen JWT-Provider mit einem JWT-Signierschlüssel

Fügen Sie Ihrer ServiceNow -Instanz einen JSON-Web-Token-Provider (JWT) hinzu.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Anbieter**.
2. Füllen Sie das Formular aus, und klicken Sie auf **Absenden**.

Option	Bezeichnung
Name	Ein eindeutiger Name für die JWT-Provider-Konfiguration.
Ablaufintervall (Sek.)	Die Lebensdauer der vom JWT-Provider generierten Token in Sekunden.
Signierkonfiguration	Die anzuwendende JWT-Signierschlüsselkonfiguration ServiceNow.

JSON-Web-Token (JWT) generieren

Erstellen Sie ein JSON-Web-Token (JWT), um Ansprüche zwischen zwei Parteien auf der Now Platformsicher darzustellen.

Die GlideJWT-API ist eine bereichsbezogene, skriptfähige API, die ein JWTgeneriert. Vor dem Generieren des JWT sind drei Argumente erforderlich:

- Sys_id des JWT -Providers
- Serialisierter JSON-Header
- Serialisierte JSON-Nutzlast

Es gibt zwei JWT-API-Skripts, JWTTokenInternal und JWTTokenRestricted, die Sie beim Konfigurieren eines JWT-Providers verwenden können. Mit dem Skript JWTTokenRestricted können Administratoren konfigurieren, wer ein JWT generieren kann. Das JWTTokenInternal-Skript ist schreibgeschützt und ermöglicht nur angemeldeten Benutzern das Generieren eines JWT.

So generieren Sie ein JWT:

- JWT-Schlüssel mit einem freigegebenen Schlüssel (HMAC) oder einem Signaturschlüsselspeicher (RSA) erstellen
- Ordnen Sie einen JWT-Provider der Signaturkonfiguration zu, die auf einen JWT-Schlüssel verweist

Sie können die API verwenden, um Ihr Token zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können standardmäßige und benutzerdefinierte Ansprüche verwenden, wenn Sie einen JWT-Provider konfigurieren. Sie können dynamische Header- und Nutzlastansprüche als Teil der generateJWT-API-Signatur übergeben.

Beispielskript zum Testen der API:

```
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = { "jti": "testjti", "iss": "testiss", "sub": "testsub" };
var payload = JSON.stringify(payloadJSON);

var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

OAuth-Client-APIs

Die OAuth-Client-API stellt Methoden zum Anfordern und Widerrufen von OAuth-Token bereit.

Der OAuth-Client stellt diese Klassen bereit:

- GlideOAuthClient : Methoden zum Anfordern und Widerrufen der Aktualisierungs- und Zugriffstoken.
- GlideOAuthClientRequest : Methoden zur Behandlung von Client-Anforderungen.
- GlideOAuthClientResponse : Methoden für die Verarbeitung von Client-Antworten.
- GlideOAuthToken : Methoden zum Abrufen des Zugriffstokens und Informationen zum Zugriffstoken.

Sie können auch die OAuthUtil-Skripteinbindung anpassen, um die Anforderungsparameter abzufangen und auch die Antworten von externen OAuth-Providern zu analysieren.

Wenn Sie OAuth-Klassen in einem bereichsbezogenen Skript verwenden, verwenden Sie den Namespace-Identifier `sn_auth`.

OAuth-Parameter für die Unterstützung von Standardprofilen

Für das Standardprofil-Feature ist ein Parametersatz erforderlich, den Sie mit dem API *`setParameter()`* zur Angabe des OAuth-Anforderers, eines Kontexts für die Anforderung und des Anbieterprofils verwenden können.

Im OAuth-Provider-Szenario müssen drei Parameter festgelegt werden, die dem OAuth-Provider mitteilen, welches OAuth-Profil standardmäßig verwendet werden soll. Wenn diese drei Parameter festgelegt sind, wird das Zugriffs-Token in der Instanzdatenbank gespeichert. Verwenden Sie die Parameter mit *`GlideOAuthClientRequest`*.

OAuth-Parameter für die Unterstützung von Standardprofilen

Parameter	Beschreibung
`oauth_requestor`	Die sys_id des Objekts. Dies kann ein Benutzerdatensatz oder ein E-Mail-Account sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth-Parameter für die Unterstützung von Standardprofilen (Fortsetzung)

Parameter	Beschreibung
`oauth_requestor_context`	Deskriptor, der den Kontext für den OAuth-Anforderer bereitstellt. Verwenden Sie als bewährte Methode den Namen der Tabelle, in der das Objekt `oauth_requestor` gespeichert wird.
`oauth_provider_profile`	Die sys_id des OAuth-Profildatensatzes, der der Standard ist (siehe OAuth-Profil angeben).

Sie müssen keine Parameter zum Festlegen von Grant-Typ und Gültigkeitsbereich verwenden, da die Werte im OAuth-Profildatensatz konfiguriert sind. Wenn Sie die Parameter nicht verwenden, können Sie die GlideOAuthClientRequest-API-Methoden `setScope` und `setGrantType` verwenden. Weitere Informationen finden Sie unter setScope und setGrantType.

JWT-Unterstützung für private Schlüssel für OAuth 2.0-Client-Authentifizierung

JWT-Support für OAuth 2.0-Client-Authentifizierung.

Die JWT-Clientauthentifizierung mit privatem Schlüssel ist eine Authentifizierungsmethode, die von Clients zur Authentifizierung beim Autorisierungsserver verwendet werden kann, wenn der Tokenendpunkt verwendet wird.

Bei diesem Authentifizierungsmechanismus können sich nur Clients authentifizieren, die einen öffentlichen Schlüssel registriert und ein JWT mit diesem Schlüssel signiert haben.

Das JWT muss ERFORDERLICHE Anspruchswerte enthalten und kann OPTIONALE Anspruchswerte enthalten. Weitere Informationen zu den Anspruchswerten, die für die JWT-Authentifizierung für die private_key_jwt- Authentifizierung erforderlich sind, finden Sie im Abschnitt „Client-Authentifizierung“ in der OpenID Connect-Kerndokumentation.

Hinweis:
Das Authentifizierungstoken muss als Wert des Parameters client_assertion gesendet werden. Der Wert des Parameters **client_assertion_type** muss urn:ietf:params:oauth:client-assertion-type:jwt-bearer lauten.

Für die OAuth 2.0-Client-Authentifizierung mit JWT-Token erforderliche Plugins:

- **OAuth 2.0 (com.snc.platform.security.oauth)**: Dieses Plugin ist in neuen und aktualisierten Instanzen aktiv. Wenn das Plugin in Ihrer Instanz nicht aktiv ist, können Sie es aktivieren.
- **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer)**: Für OIDC-basierten Single Sign-on-Anwendungsfall.

Sie können die OAuth 2.0-Clientauthentifizierung mit privatem Schlüssel JWT für Folgendes verwenden:

- OIDC-basiertes Single Sign-on
- Ausgehende OAuth-Integrationen

Konfigurieren Sie Private Key JWT für OIDC-basiertes SSO

Konfigurieren Sie Private Key JWT für OIDC-basierte SSO-Integrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen die folgenden Aufgaben ausführen, bevor Sie Private Key JWT für OIDC-basiertes SSO auswählen.

- Laden Sie das Java Key Store-Zertifikat hoch: Hängen Sie ein JKS-Zertifikat an Ihre Instanz an, um die JWT-Client-Authentifizierung zu aktivieren.
- Konfigurieren Sie einen JWT-Signierschlüssel: Erstellen Sie einen JWT-Signierschlüssel, um ihn Ihrem JKS-Zertifikat (Java KeyStore) zuzuweisen.

  Hinweis:
  Wenn Sie dem Header **X.509-Zertifikat SHA-1-Fingerabdruck int (x5t)** als Teil des JWT-Schlüssels hinzufügen möchten, müssen Sie das Formular konfigurieren und das Feld **X.509-Zertifikat SHA-1-Fingerabdruck int (x5t) hinzufügen**.

- Erstellen Sie einen JWT-Provider mit einem JWT-Signierschlüssel: Fügen Sie Ihrer Instanz ServiceNow] einen JWT-Provider hinzu.

Um einen JWT-Schlüssel für einen OIDC-basierten Identitätsanbieter einzuschließen, müssen Sie:

- Installieren Sie das Plugin „ **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter** “ (com.snc.integration.sso.multi.installer).
- Aktivieren Sie die Eigenschaften für **SSO-Eigenschaften für mehrere Anbieter**. Weitere Informationen finden Sie unter SSO-Eigenschaften, -Tabellen und -Skripts für mehrere Anbieter.
- Erstellen Sie einen OIDC-Identitätsanbieter. Weitere Informationen finden Sie unter OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen.

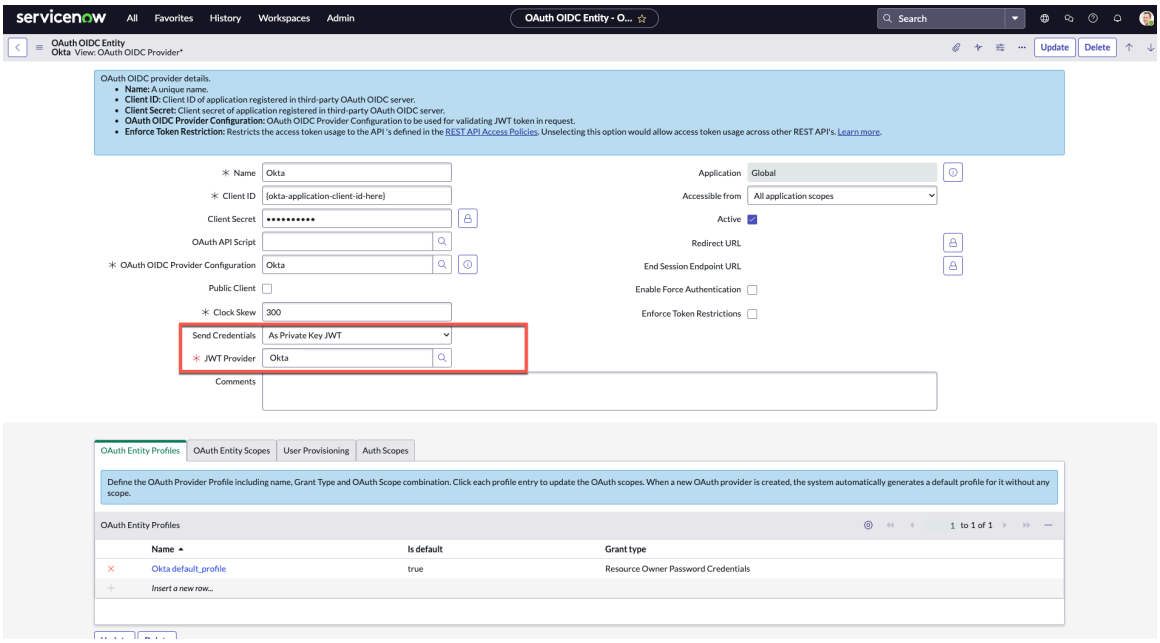
Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**.
2. Wählen Sie den von Ihnen erstellten OIDC-Identitätsanbieter aus.
3. Wählen Sie oben im Formular aus **Konfigurieren** > **Formulardesign**.

   Hinweis:
   Sie müssen dem Formular die Felder **Anmeldeinformationen senden** und **JWT-Provider** hinzufügen, um den privaten Schlüssel JWT für OIDC-basierte Identitätsanbieter-Authentifizierungsanforderungen zu verwenden.

4. Wählen Sie für Anmeldeinformationen senden die Option **Als privaten Schlüssel JWT** aus.
5. Wählen Sie den **JWT-Provider aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn sich der Benutzer authentifiziert, bietet die Authentifizierungsseite Optionen zur Anmeldung über Okta.

Konfigurieren Sie Private Key JWT für ausgehende OAuth

Konfigurieren Sie Private Key JWT für ausgehende OAuth-Integrationen.

Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie Private Key JWT für ausgehende OAuth-Integrationen konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- Laden Sie das Java Key Store-Zertifikat hoch: Hängen Sie ein JKS-Zertifikat an Ihre Instanz an, um die JWT-Client-Authentifizierung zu aktivieren.
- Konfigurieren Sie einen JWT-Signierschlüssel: Erstellen Sie einen JWT-Signierschlüssel, um ihn Ihrem JKS-Zertifikat (Java KeyStore) zuzuweisen.

> **Hinweis:**
> Wenn Sie dem Header **X.509-Zertifikat SHA-1-Fingerabdruck int (x5t)** als Teil des JWT-Schlüssels hinzufügen möchten, müssen Sie das Formular konfigurieren und das Feld **X.509-Zertifikat SHA-1-Fingerabdruck int (x5t) hinzufügen**.

- Erstellen Sie einen JWT-Provider mit einem JWT-Signierschlüssel: Fügen Sie Ihrer Instanz ServiceNow] einen JWT-Provider hinzu.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken Sie auf der Interceptor-Seite **auf Verbindung mit einem OAuth-Drittanbieter herstellen**, und füllen Sie das Formular aus.

> **Hinweis:**
> Sie müssen dem Formular die Felder **Anmeldeinformationen senden** und **JWT-Provider** hinzufügen, um den JWT-Privatschlüssel für ausgehende OAuth-Authentifizierungsanforderungen zu verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Eindeutiger Name für die OAuth-Drittpartei-Verbindung
Client-ID	Client-ID der Anwendung, die beim OAuth-Server des Drittanbieters registriert ist
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim OAuth-Server des Drittanbieters registriert ist.
OAuth-API-Skript	Das zum Anpassen von Anforderungen und Antworten an den externen OAuth-Provider verwendete Skript.
Logo-URL	Die OAuth-Anwendungslogo-URL.
Standardgewährungstyp	Wählen Sie: **Client-Anmeldeinformationen**: Die Client-ID und der geheime Clientschlüssel, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt.
Lebensdauer von Aktualisierungstoken	Zeit in Sekunden, die das Aktualisierungstoken gültig ist. Die Standardzeit beträgt 8.640.000 Sekunden.
Öffentlicher Client	Ermöglicht öffentlichen Clients, PKCE für eine Autorisierung zu erfordern. **Hinweis:** Sie können nur den Autorisierungscode als `Default Grant type` verwenden, wenn PKCE aktiviert ist.
Kommentare	Fügen Sie Kommentare zur OAuth-App hinzu.
Anwendung	Anwendung und Bereich, die diesen Datensatz enthalten.
Zugänglich von	Machen Sie diese App aus allen Anwendungsbereichen oder nur aus diesem Bereich zugänglich.
Aktiv	Aktivieren Sie die Checkbox, um die App zu aktivieren.
Autorisierungs-URL	Der OAuth-Autorisierungscode-Endpunkt.
Token-URL	Der OAuth-Servertoken-Endpunkt.
Token-Sperr-URL	Der Endpunkt des OAuth-Server-Tokenwiderrufs.
Umleitungs-URL	Der OAuth-Rückrufendpunkt. Wenn dieses Feld leer ist, generiert die Instanz automatisch einen Eintrag.
Gegenseitige Authentifizierung aktivieren	Aktivieren Sie das Kontrollkästchen, um die gegenseitige Authentifizierung für die Anforderung und den Widerruf von Token zu verwenden. Für diese Funktion muss ein Profil für die gegenseitige Authentifizierung angegeben werden.
Anmeldeinformationen senden	Wählen Sie: **Als Privater Schlüssel JWT**
JWT-Anbieter	JWT-Provider-Details. Sie können die Suche verwenden, um den JWT-Provider auszuwählen.

Das System erstellt einen Datensatz in der Anwendungsregistrierungstabelle [oauth_entity] mit dem Typ OAuth-Provider, der für die Authentifizierung mit dem privaten JWT-Schlüssel verwendet werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine ausgehende REST-Nachricht

Erstellen Sie eine ausgehende REST-Nachricht, um die Instanz als Autorisierungsserver zu autorisieren.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **System-Webservices** > **Ausgehend** > **REST-Nachricht** und klicken Sie dann auf **Neu**.
2. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz wie in beschrieben aus.
   Beachten Sie die folgenden Feldwerte:
   - **Endpunkt**: URL der Instanz, die der Autorisierungsserver ist.
   - **Authentifizierungstyp**: **OAuth 2.0**.
   - **OAuth-Profil**: OAuth-Profil, das Sie für den Clientserver erstellt haben.
3. Klicken Sie im REST-Nachrichtendatensatz auf **OAuth-Token abrufen**.
4. Authentifizieren Sie sich bei der Instanz, die das Token bereitstellt. Die Methode hängt von der Single Sign-on-Integration ab.
   Sie können Folgendes verwenden:
   - Ihr Benutzername und Ihr Passwort, mit denen Sie sich bei der Instanz authentifizieren.
   - Der Benutzername und das Passwort für den IdP, sofern aktiviert. Klicken Sie auf **Externe Anmeldung verwenden**, um auf den IdP-Anmeldebildschirm zuzugreifen.

     Hinweis:
     Um automatisch zur IdP-Anmeldeseite umgeleitet zu werden, müssen Sie die Systemeigenschaft glide.authenticate.external festlegen.

   - Ihr Code, wenn MFA aktiviert ist.
5. Klicken Sie auf **Zulassen** oder **Verweigern**, um die Autorisierung abzuschließen und die Token auszugeben.
   Der folgende Prozess wird in OAuth-Autorisierungscode-Gewährungs-Flowbeschrieben.

Anforderungen an die Passwortkomplexität

Passwörter in Ihrer ServiceNow® -Instanz müssen die Komplexitätsanforderungen erfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

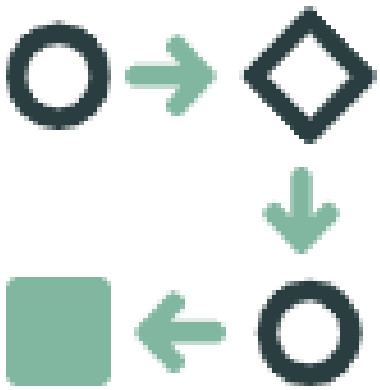
Erkunden

Machen Sie sich mit den Funktionen und dem Geschäftsnutzen von Anforderungen an die Passwortkomplexität vertraut.

Aktivieren

Machen Sie sich damit vertraut, wie Sie die Anforderungen an die Passwortkomplexität aktivieren.

Konfigurieren



Konfigurieren Sie die Komplexitätsanforderungen für Passwörter.

Referenz: Nicht unterstützte Passwortzeichen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informieren Sie sich über die nicht unterstützten Passwortzeichen.

Erkunden der Anforderungen an die Passwortkomplexität

Passwörter in Ihrer ServiceNow® -Instanz müssen die Komplexitätsanforderungen erfüllen.

Die Richtlinieneinstellung „Passwort-Komplexitätsanforderungen“ legt fest, ob Passwörter eine Reihe von Richtlinien für sichere Passwörter erfüllen müssen.

Anforderungen an die Passwortkomplexität werden erzwungen, wenn ein Passwort geändert oder erstellt wird.

Die Anforderungen an die Passwortkomplexität werden erfüllt und funktionieren basierend auf Folgendem:

- Wenn die Eigenschaft `glide.apply.password_policy.on_login` aktiviert ist, wird die Passwortrichtlinienprüfung für den Benutzer während der Anmeldung erzwungen. Während der Anmeldung muss der Benutzer die Passwortrichtlinie einhalten und das Passwort für die Instanz ändern.
- Die Anforderungen der Passwortrichtlinie basieren auf der Basic Multilanguage Plane (BMP), die Zeichen für alle modernen Sprachen enthält. ServiceNow Instanzen werden mit BMPs mit etwa 10.000 Zeichen geliefert.
- Für Ihre Instanz können Passwörter innerhalb der zulässigen BMPs festgelegt werden. Passwörter, die nicht diesen BMPs entsprechen, sind nicht zulässig.

Bei Bedarf können Sie verlangen, dass Passwörter regelmäßig, mindestens alle 90 Tage, geändert werden.

Anforderungen und gesperrte Zeichen

Um eine sichere Netzwerkumgebung zu ermöglichen, müssen Benutzer sichere Passwörter verwenden, die eine Kombination aus Buchstaben, Zahlen und Symbolen enthalten. Diese Kombinationen helfen, nicht autorisierte Benutzer zu verhindern, die normalerweise manuelle oder automatisierte Methoden verwenden, um schwache Passwörter zu erraten.

Das Passwort für Ihre Instanz muss die folgenden Anforderungen erfüllen:

- Mindestens 8 Zeichen.
- Maximal 100 Zeichen.
- Enthält Klein- und Großbuchstaben
- Enthält Sonderzeichen.
- Enthält Ziffern.

Sie können eine Liste häufig falscher Passwörter sperren, z. B.:

- Vorhersehbare und sich wiederholende Sequenzen wie „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw.
- Name oder Benutzernamen des Mitarbeiters.
- Relevante Marken- oder Produktnamen.
- Standorte, z. B. Unternehmenszentrale, Stadt, Land usw.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unternehmensspezifische interne Begriffe oder Abkürzungen.
- Emojis

Hinweis:
Benutzer-, marken- oder unternehmensspezifische Zeichen, die im Passwort nicht verwendet werden können, können auf der Seite „Passwortrichtlinie“ oder „Passwort ausschließen“ konfiguriert werden.

Passwortrichtlinien für Ihre Instanz aktivieren

Implementieren Sie Passwortrichtliniensteuerungen bei der Anmeldung. Zwingen Sie Benutzer, ihr Passwort zu ändern, wenn das Passwort die Kriterien der Passwortrichtlinie nicht erfüllt.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das Plugin „Password Policy“ (com.glide.password_policy) ist standardmäßig aktiviert. Die Richtlinie tritt in Kraft, wenn ein Benutzer das Passwort ändert oder zurücksetzt.
Das Feld **Vorgegebene Passwortstärke** wird automatisch auf **Standard stark**gesetzt. Wenn Sie neue Kriterien hinzufügen möchten, können Sie das folgende Verfahren ausführen.

Wenn Sie Ihre Instanz über den Installations-Exit `ValidatePasswordStronger` oder die Eigenschaft „Passwortzurücksetzungs-Anmeldeinformationsspeicher `pwd_cred_store` “ angepasst haben, lesen Sie die Eigenschaften der Passwortrichtlinie, um zu erfahren, wie Sie eine Passwortrichtlinie für Ihre Instanz implementieren.

Hinweis:
Die aktive Passwortrichtlinie wird für die Instanz wie gezeigt hervorgehoben.

Um die Passwortrichtlinie zu ändern, navigieren Sie zu **Alle** > **Passwortzurücksetzung** > **Anmeldeinformationsspeicher**, wählen Sie die Anmeldeinformationen aus, und ändern Sie das Feld **Password policy** (Passwortrichtlinie) in die erforderliche Richtlinieneingabe.

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Passwortrichtlinien**.
2. Klicken Sie auf **Neu**.
   Das Formular „Passwortrichtlinie“ wird angezeigt.
3. Geben Sie den **Namen** für Ihre Passwortrichtlinie an.
4. Wählen Sie im Abschnitt Password Policy Criteria (Kriterien für Passwortrichtlinie) eine der folgenden Voreinstellungen aus dem Feld **Password Stärke Preset** (Voreinstellung für Passwortstärke) aus.

   Hinweis:
   Die Passwortrichtlinie wird basierend auf der ausgewählten Voreinstellung angewendet.

5. Füllen Sie die verbleibenden Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Passwortrichtlinie“.

Feld	Beschreibung
Mindestlänge von Passwörtern	Mindestlänge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. Legen Sie dieses Feld auf mindestens 8–10 Zeichen fest.
Maximale Passwortlänge	Maximale Länge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. Legen Sie dieses Feld auf maximal 100 Zeichen fest.
Mindestanzahl der Großbuchstaben	Mindestanzahl von Großbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der Kleinbuchstaben	Mindestanzahl der Kleinbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der numerischen Zeichen	Mindestanzahl von Zeichen im Passwort, von 0 bis 10.
Mindestanzahl der Sonderzeichen	Mindestanzahl von Sonderzeichen im Passwort, von 0 bis 10.
Eingeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Wenn Sie beispielsweise `$,!`eingeben , dann können Benutzer nur „$“ und „!“ verwenden. als Sonderzeichen im Passwort. Es können keine anderen Sonderzeichen verwendet werden. Ein Passwort mit anderen Sonderzeichen ist nicht zulässig.
Ausgeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Wenn Sie beispielsweise `@$!`eingeben , dann können Benutzer „@“, „$“ und „!“ nicht verwenden. als Sonderzeichen in Passwörtern verwenden. **Hinweis:** Diese Option ist verfügbar, wenn die Eigenschaft `glide.password_policy.use_excluded_special_ch` aktiviert ist.
Anwenderdaten nicht zulassen	Option zum Sperren von Benutzerdaten, die sich auf die Authentifizierung beziehen.
Schwellenwert für Sequenzlänge	Die Sequenzlänge Ihres Passworts.
Schwellenwert für Wiederholungslänge	Die Wiederholungslänge Ihres Passworts.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Sowohl der Schwellenwert für die Sequenzlänge als auch der Schwellenwert für die Wiederholungslänge dürfen maximal acht Zeichen haben. Mit diesen Feldern können Sie schwache Kombinationen von Passwörtern einschränken, die vorhersehbare und sich wiederholende Sequenzen aufweisen, z. B. „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw. ○ Wenn die Voreinstellung der **Passwortstärke** auf **Standardmäßig stark**festgelegt ist, wird die Länge für den Schwellenwert für die Sequenzlänge und den Schwellenwert für die Wiederholungslänge auf vier Zeichen festgelegt.
Passwort testen	Geben Sie in dieses Feld Ihr tatsächliches Passwort ein.

6. Klicken Sie **auf Ihr Passwort testen**.
7. Nachdem das Passwort als gültig getestet wurde, klicken Sie auf **Absenden**, um das Passwort zu übermitteln.

Hinweis:
Testen Sie Ihr Passwort immer, bevor Sie es absenden.

Eigenschaften der Passwortrichtlinie

Mit den Eigenschaften der Passwortrichtlinie können Sie Passwortrichtlinien verwalten, Listenpasswörter ausschließen und während der Anmeldung eine Passwortrichtlinie anwenden.

Navigieren zu **Passwortrichtlinie** > **Eigenschaften** , um die Eigenschaften der Passwortrichtlinie anzuzeigen und zu bearbeiten.

Eigenschaft	Beschreibung
glide.enable.password_policy	Aktiviert eine Passwortrichtlinie für Ihre Instanz. Die Richtlinie tritt in Kraft, wenn ein Benutzer ein Passwort ändert oder zurücksetzt. Diese Eigenschaft wird automatisch auf **true**festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: • Wenn Ihre Instanz über den Installations-Exit `ValidatePasswordStronger` oder Ihren Anmeldeinformationsspeicher für die Passwortzurücksetzung [pwd_cred_store] angepasst wird, müssen Sie diese Eigenschaft erstellen und zu Ihren Systemeigenschaften hinzufügen. • Wenn Ihre Instanz vor dem `ValidatePasswordStronger`Orlando -Release mit dem Installations-Exit von [] angepasst wurde, mussten Sie die Eigenschaft „Passwortrichtlinie“ erstellen, damit die Passwortrichtlinie funktioniert. • Ab Release Orlando gibt es keine Anpassung des Installationsausgangs. Die Eigenschaften der Passwortrichtlinie funktionieren standardmäßig. Diese Eigenschaften können manuell deaktiviert werden.
glide.enable.blacklist_password	Verbietet die Verwendung bestimmter Passwörter. Der Administrator kann Passwörter in die Tabelle „Ausgeschlossenes Passwort“ einfügen. Diese Eigenschaft wird automatisch auf **true**festgelegt.
glide.apply.password_policy.on_login	Erzwingt, dass Benutzer die Passwörter bei der nächsten Anmeldung ändern, wenn die vorhandenen Passwörter nicht der aktuellen Passwortrichtlinie entsprechen. Diese Eigenschaft wird automatisch auf **„false**“ festgelegt. Wenn Sie den Wert auf **true** setzen, wird während der Anmeldung eine Passwortrichtlinie erzwungen. **Hinweis:** Durch Aktivieren dieser Eigenschaft kann eine erhebliche Anzahl von Benutzern, die nicht der neuen Passwortrichtlinie entsprechen, gezwungen werden, ihre Passwörter zu ändern.
glide.password_policy.user_excluded_special_char	Ermöglicht Benutzern die Verwendung der Option „Ausgeschlossenes Sonderzeichen“ im Formular „Passwortrichtlinie“.
glide.validate.sys_user.password.field	Aktiviert die Validierung des Benutzerpassworts anhand der Passwortrichtlinie, wenn ein Administrator das sys_user-Formular oder die Listenansicht bearbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
glide.password.policy.generate.password.field.disabled	Deaktiviert das Feld **Passwort** im Popup „Passwort festlegen“ im Formular „sys_user“.
glide.user.show.password.field	Aktiviert das Feld **Passwort** im sys_user-Formular.
glide.password_policy.debug	Aktiviert die Debug-Protokollierung für die Passwortrichtlinie.

Passwortrichtlinie konfigurieren

Mit Passwortrichtlinienkriterien können Sie Ihr Passwort sichern und die Mindestanforderungen an die Passwortkomplexität einhalten.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Das Plugin „Passwortrichtlinie“ [com.glide.password_policy] ist standardmäßig aktiviert. Sie tritt in Kraft, wenn ein Benutzer das Passwort ändert oder zurücksetzt. Wenn Sie Ihre Instanz über den Installations-Exit von ValidatePasswordStronger oder Ihren Anmeldeinformationsspeicher für die Passwortzurücksetzung [pwd_cred_store] angepasst haben, finden Sie weitere Informationen unter Eigenschaften der Passwortrichtlinie.

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Passwortrichtlinien**.

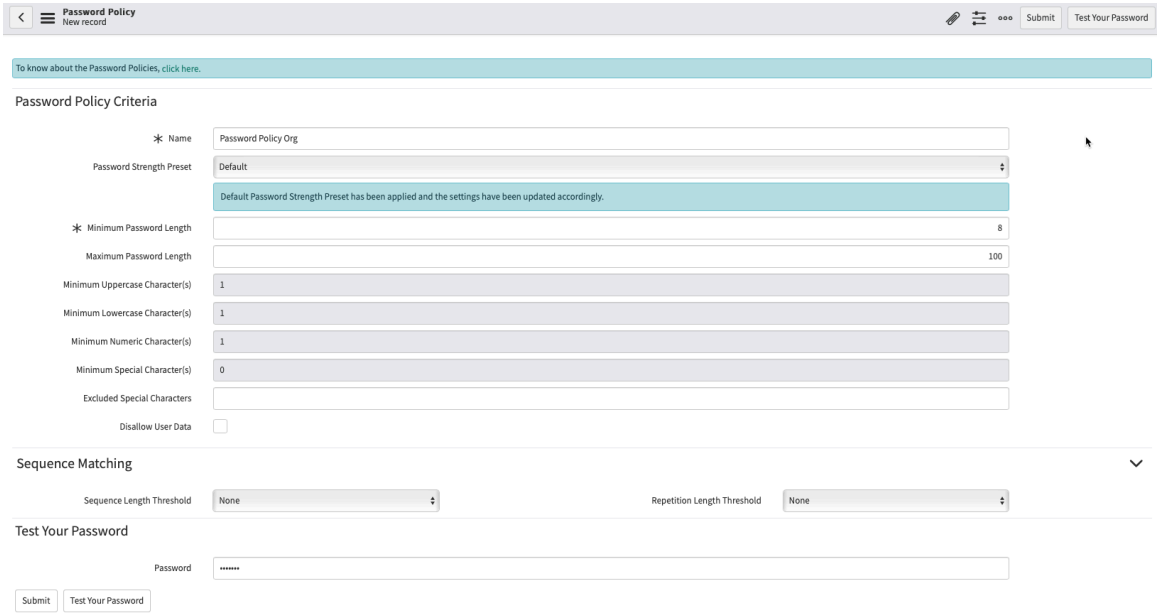
   Hinweis:
   Standardmäßige starke Voreinstellung ist als Standard-Passwortakzeptanzkriterium aktiviert. Wenn Sie neue Kriterien hinzufügen möchten, können Sie die folgenden Schritte ausführen.

2. Klicken Sie auf **Neu**.

   Die Datensatzseite „Password Policy New“ (Neue Passwortrichtlinie) enthält die folgenden Abschnitte, die Sie zum Festlegen Ihres Passworts angeben müssen:

   - **Passwortrichtlinienkriterien**
   - **Sequenzabgleich**
   - **Passwort testen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Geben Sie den **Namen** für Ihre Passwortrichtlinie an.
4. Wählen Sie im Abschnitt **„Kriterien für Passwortrichtlinie“** die Voreinstellung aus der Voreinstellung für die **Passwortstärke aus**.
   Folgende Voreinstellungen sind verfügbar:

Vorgegebene Passwortstärke und ihre Beschreibung

Vorgegebene Passwortstärke	Beschreibung
Standard	Wenn Sie **Standard** auswählen, werden die erforderlichen Passwortzeichen automatisch wie folgt ausgefüllt: ○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen
Mittel	Wenn Sie **Mittel** auswählen, werden die erforderlichen Passwortzeichen basierend auf den folgenden Zeichen automatisch ausgefüllt: ○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen ○ Mindestens ein Sonderzeichen
Hoch	Wenn Sie **Hoch** auswählen, werden die Passwortzeichen automatisch wie folgt ausgefüllt: ○ Mindestens ein Großbuchstabe ○ Mindestens zwei Kleinbuchstaben ○ Mindestens ein numerisches Zeichen ○ Mindestens drei Sonderzeichen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgegebene Passwortstärke	Beschreibung
Standardmäßig stark	Wenn Sie „ **Standard stark** “ auswählen, werden die erforderlichen Passwortzeichen basierend auf den Zeichen wie folgt automatisch ausgefüllt: ○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen ○ Mindestens ein Sonderzeichen
Benutzerdefiniert	Wenn Sie **Benutzerdefiniert** auswählen, werden die erforderlichen Passwortzeichen basierend auf den folgenden Zeichen automatisch ausgefüllt: ○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen ○ Mindestens ein Sonderzeichen Sie können auch das angezeigte **Passwortrichtlinienskript** anpassen.
Erweitert	Wenn Sie **Erweitert** auswählen, werden **Passwortregelskript** und **Passwortstärkeskript**angezeigt. Basierend auf Ihren Anforderungen können Sie diese Skripts anpassen.

Hinweis:
Die Passwortrichtlinie wird basierend auf der ausgewählten Voreinstellung angewendet.

5. Geben Sie die in der Tabelle beschriebenen Felder an:

Formular „Passwortrichtlinie“.

Feld	Beschreibung
Mindestlänge von Passwörtern	Mindestlänge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. **Hinweis:** **Die Mindestlänge des Passworts** ist ein Pflichtfeld. Es wird empfohlen, es auf mindestens 8 bis 10 Zeichen festzulegen.
Maximale Passwortlänge	Maximale Länge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. **Hinweis:** **Maximale Passwortlänge** ist ein optionales Feld. Es wird empfohlen, es auf maximal 100 Zeichen festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Mindestanzahl der Großbuchstaben	Mindestanzahl von Großbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der Kleinbuchstaben	Mindestanzahl der Kleinbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der numerischen Zeichen	Mindestanzahl von Zeichen im Passwort, von 0 bis 10.
Mindestanzahl der Sonderzeichen	Mindestanzahl von Sonderzeichen im Passwort, von 0 bis 10.
Eingeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Wenn Sie beispielsweise „$,!“ eingeben. -Benutzer können nur „$“ und „!“ verwenden. als Sonderzeichen im Passwort. Es können keine anderen Sonderzeichen verwendet werden, und ein Passwort mit anderen Sonderzeichen ist nicht zulässig.
Ausgeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Beispiel: Wenn '@$!' eingegeben wird, sollten Benutzer „@“, „$“ und „!“ nicht verwenden können. als Sonderzeichen in Passwörtern verwenden. **Hinweis:** Diese Option ist verfügbar, wenn die Eigenschaft glide.password_policy.use_excluded_special_char aktiviert ist.
Anwenderdaten nicht zulassen	Es ist aktiviert, um die Benutzerdaten nicht zuzulassen.

6. Geben Sie im Abschnitt „ **Sequenzabgleich“ den Schwellenwert** für die Sequenzlänge und den Schwellenwert für die **Wiederholungslänge**an.

   Hinweis:

   - Sowohl der Schwellenwert für die Sequenzlänge als auch der Schwellenwert für die Wiederholungslänge dürfen maximal acht Zeichen haben. Mit diesen Feldern können Sie schwache Kombinationen von Passwörtern einschränken, die vorhersehbare und sich wiederholende Sequenzen aufweisen, z. B. „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw.
   - Für **Standard stark**wird die Länge sowohl für den Schwellenwert für die Sequenzlänge als auch für den Schwellenwert für die Wiederholungslänge als vier Zeichen ausgewählt.

7. Geben Sie im Abschnitt „Passwort **testen“ Ihr** Passwort an.
8. Klicken Sie **auf Ihr Passwort testen**.
9. Nachdem das Passwort gültig ist, klicken Sie auf **Absenden**, um das Passwort zu übermitteln.

   Hinweis:

   Testen Sie Ihr Passwort immer, bevor Sie es absenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Passwort für einen Benutzer konfigurieren

Legen Sie das Passwort Ihres Benutzers für die Instanz basierend auf der konfigurierten Passwortrichtlinie fest.

Vorbereitungen

Benutzer, die für die Festlegung des Passworts für ihre erste Anmeldung erstellt wurden. Weitere Informationen finden Sie unter Benutzer erstellen .

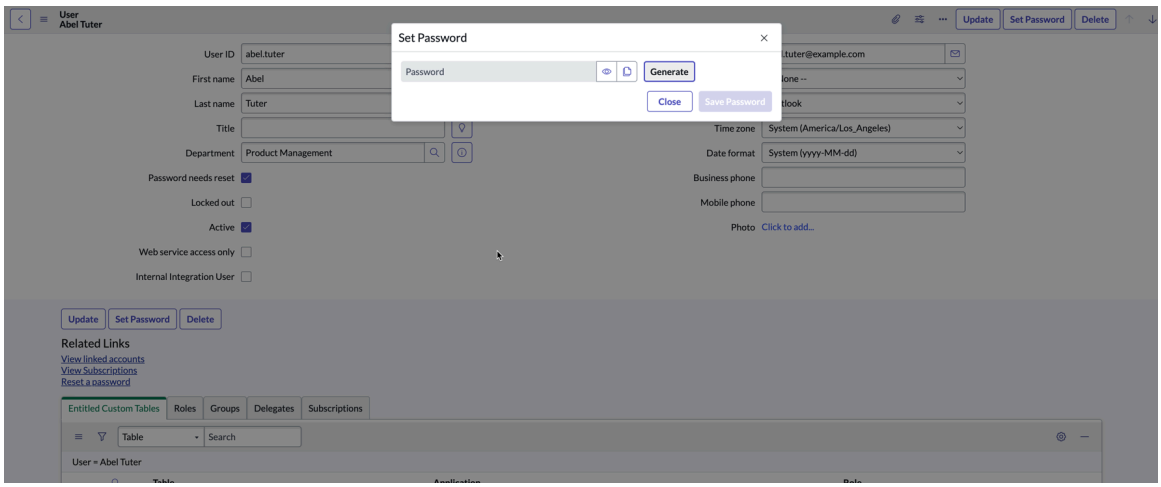
Um das Feld **Passwort** direkt im Benutzerformular auszufüllen, aktivieren Sie die Option Aktivieren, **um das Passwortfeld im sys_user-Formular** anzuzeigen (glide.user.show.password.field). Weitere Informationen zu den Eigenschaften finden Sie unter Eigenschaften der Passwortrichtlinie.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Benutzer**.
2. Wählen Sie den Benutzer aus der Liste auf der Seite „Benutzer“ aus.
3. Um das Passwort basierend auf der Passwortrichtlinie festzulegen, klicken Sie auf **Passwort**festlegen.

   Das Popup „Passwort festlegen“ wird angezeigt.

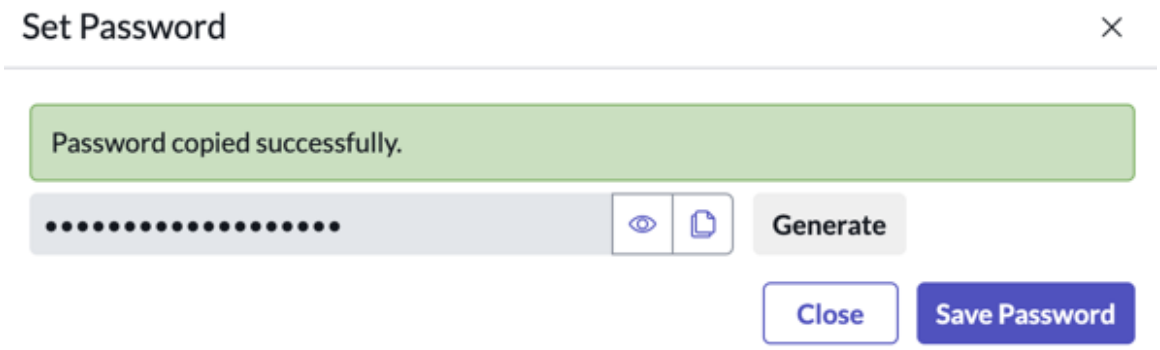


4. Führen Sie in „Passwort festlegen“ die folgenden Schritte aus.
   a. Klicken Sie auf **Generieren**, um das Passwort zu generieren.

   b. **Klicken** Sie auf das Symbol Anzeigen, um das Passwort anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie auf das Symbol **Kopieren**, um das Passwort zu kopieren und für den Benutzer freizugeben.



5. Klicken **Sie auf Passwort speichern**.

Das Passwort wird für den Benutzer festgelegt. Außerdem wird automatisch das Kontrollkästchen Passwort erforderlich Rest aktiviert.

Der Benutzer muss bei der ersten Anmeldung dasselbe Passwort für die Anmeldung verwenden und das Passwort bei der Anmeldung gemäß der von den Administratoren konfigurierten Passwortrichtlinie ändern.

Ausschließen von Passwörtern durch Passwortrichtlinien in Ihrer Instanz

Fügen Sie der Tabelle „Ausgeschlossenes Passwort“ Passwörter hinzu, um die Verwendung bestimmter Passwörter durch Benutzer in Ihrer Instanz zu verhindern.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können beliebig viele Passwörter sperren. Einige der Beispiele:

- Vorhersehbare und sich wiederholende Sequenzen, z. B. „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw.
- Name oder Benutzernamen des Mitarbeiters.
- Relevante Marken- oder Produktnamen.
- Standorte, z. B. Unternehmenszentrale, Stadt, Land usw.
- Unternehmensspezifische interne Begriffe oder Abkürzungen.
- Emojis

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Ausgeschlossene Passwörter**.
2. Um ein Passwort zu Ihrer Ausschlussliste hinzuzufügen, klicken Sie auf **Neu**, und geben Sie das Passwort ein.
3. Navigieren zu **Passwortrichtlinie** > **Ausschlusslistenverwaltung** , um das Passwort Ihrer Benutzer zu steuern und zu verhindern, dass Benutzer ein falsches Passwort für die Instanz verwenden.

   Die **Ausschlusslistenverwaltung** verfügt über etwa 5.000 häufig verwendete Passwörter.

Nicht unterstützte Passwortzeichen

Einige Passwortzeichen werden nicht unterstützt. Benutzer können diese Zeichen aufgrund der Anforderungen an die Passwortkomplexität ServiceNow nicht verwenden.

Um eine sichere Netzwerkumgebung zu ermöglichen, müssen Benutzer sichere Passwörter verwenden, die eine Kombination aus Buchstaben, Zahlen und Symbolen enthalten. Diese Kombinationen helfen, nicht autorisierte Benutzer zu verhindern, die normalerweise manuelle oder automatisierte Methoden verwenden, um schwache Passwörter zu erraten.

- Die Anforderungen der Passwortrichtlinie basieren auf der Basic Multilanguage Plane (BMP), die Zeichen für alle modernen Sprachen enthält. Die Instanz ServiceNow wird mit BMPs mit etwa 10.000 Zeichen geliefert.
- Passwortzeichen innerhalb dieser zulässigen BMPs können für Ihre Instanz festgelegt werden. Passwortzeichen, die nicht innerhalb dieser BMPs liegen, sind nicht zulässig.

Hinweis:
Benutzer- oder unternehmensspezifische Zeichen, die im Passwort nicht verwendet werden können, können in der Liste „Passwort ausschließen“ konfiguriert werden.

Weitere Informationen zu den Eigenschaften der Passwortrichtlinie finden Sie unter Eigenschaften der Passwortrichtlinie.

Selbstregistrierung bei Instanz ServiceNow .

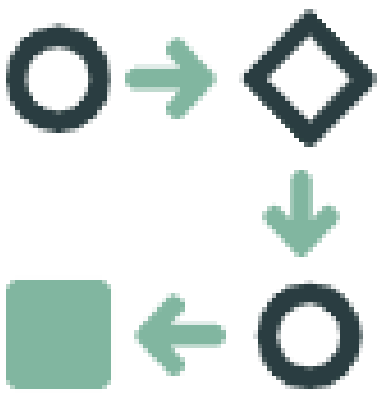
Verwenden Sie die Selbstregistrierung externer Benutzer, um das Onboarding einer großen Anzahl externer Benutzer in Ihre Instanz durchzuführen. Diese Funktion verbessert die Identitätsverifizierung, um die Kunden-Experience zu verbessern, und unterstützt häufig verwendete Registrierungs-Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lernen Sie die Funktionen und den Geschäftsnutzen der Selbstregistrierung kennen.

Machen Sie sich damit vertraut, wie Sie die externe Selbstregistrierung aktivieren.

Konfigurieren



Konfigurieren Sie die Selbstregistrierung.

Aktivieren

Machen Sie sich mit den Eigenschaften der Selbstregistrierung vertraut.

Automatische Übersetzung

Erkunden Selbstregistrierung

Verwenden Sie die Selbstregistrierung externer Benutzer, um das Onboarding einer großen Anzahl externer Benutzer in Ihre Instanz durchzuführen. Diese Funktion verbessert die Identitätsverifizierung, um die Kunden-Experience zu verbessern, und unterstützt häufig verwendete Registrierungs-Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Selbstregistrierung externer Benutzer ermöglicht es einer großen Gruppe von Benutzern, sich ohne die Hilfe eines Administrators bei einer ServiceNow -App zu registrieren. Zum Beispiel könnte sich eine Universität mit einer großen Gruppe von Studenten, die auf dem Campus parken muss, in der Campus-Parkplatz-App registrieren. Jeder Student erhält eine begrenzte Anzahl spezifischer Parkberechtigungen und durchläuft einen automatisierten Registrierungsprozess. Dieses System könnte eine für jeden Studenten eindeutige Parkplatznummer generieren und sicherstellen, dass er über einen Parkplatz verfügt.

Ein Selbstregistrierungs-Flow besteht aus einer benutzerdefinierten ServiceNow -App, in diesem Fall einer Campus-Parkplatz-App. Nach der Konfiguration einer App mit den erforderlichen Tabellen konfiguriert ein Administrator die Registrierung, einschließlich eines Vorregistrierungs-Flows, einer Feldzuordnung, einer Zuordnung nach der Registrierung, eines Captcha, einer Rollenzuordnung und eines Flows nach der Registrierung.

Aktivieren der Selbstregistrierung für externe Benutzer

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „External User Self-Registration“ (com.snc.external_user_self_registration) aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Externe Rollen in der Selbstregistrierung

Um zu verhindern, dass externen Benutzern versehentlich Zugriff gewährt wird, können Sie allen externen Benutzern die Rolle snc_external zuweisen.

Externen Benutzern, die sich selbst registrieren, muss die Rolle snc_external mit den geringsten Berechtigungen zugewiesen werden. Die Rolle snc_external gibt an, dass es sich um einen für Ihre Organisation externen Benutzer handelt, der keinen Zugriff auf Ressourcen hat, solange der Rolle snc_external oder anderen Rollen, die die Rolle snc_external übernehmen, keine expliziten Zugriffsrechte über ACLs erteilt wurden.

Standardmäßig haben Benutzer mit der Rolle snc_external keinen Zugriff auf:

- Scripted REST API-Ressourcen, die nicht als extern markiert sind
- Tabellen ohne die Rolle, die die Rolle snc_external oder public erbt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ressourcen, die keine Datensatztypen sind, z. B. Prozessoren und UI-Seiten ohne die Rolle snc_external oder eine Rolle, die die Rolle snc_external erbt
- Now Intelligence-Dashboards.

Ab dem Paris-Release müssen Sie eine Ausschlusslisten-Eigenschaft aktivieren, um die explizite Zuweisung von snc_external-Rollen zu erzwingen. Informationen zum Aktivieren der Eigenschaft finden Sie unter Zukünftige interne Rollenzuweisungen für externe Benutzer verhindern .

Konfigurieren einer Benutzerregistrierungskonfiguration für externe Benutzer

Erstellen Sie einen Konfigurationsdatensatz für die Benutzerregistrierung, um den Onboarding-Prozess externer Benutzer für benutzerdefinierte ServiceNow Anwendungen zu starten. Dieses Formular führt die externen Benutzer durch den Selbstregistrierungsprozess.

Vorbereitungen

- Erforderliche Rolle: admin
- Aktivieren der Selbstregistrierung für externe Benutzer

Prozedur

1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Konfigurationen der Benutzerregistrierung** und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.

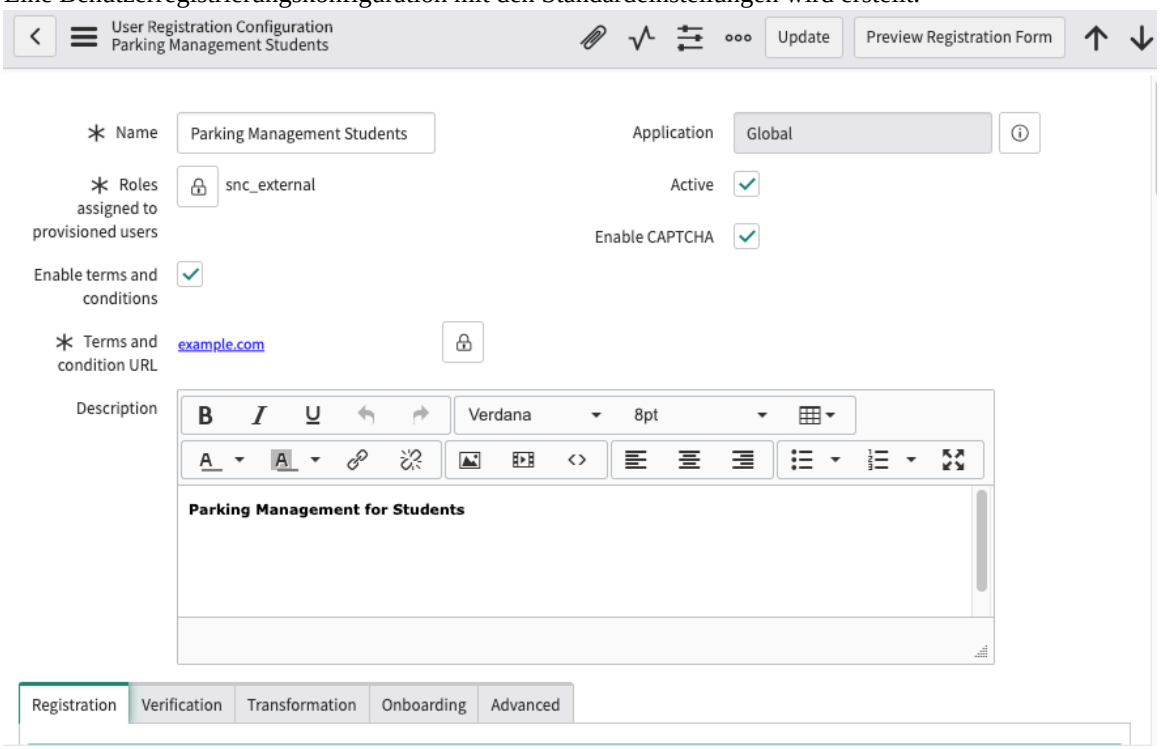
Konfigurationsformular der Benutzerregistrierung

Feld	Beschreibung
Name	Name des Registrierungsformulars. Zum Beispiel könnte eine Studenten-Parkplatzregistrierung „Parkplatzverwaltung Studenten“ sein.
Bereitgestellten Anwendern zugewiesene Rollen	Rollen, die den bereitgestellten Benutzern zugewiesen sind. Die angegebenen Rollen müssen die Rolle `snc_external` erweitern oder enthalten. Die angegebene Rolle kann auch die Rolle `snc_external` sein. Für externe Benutzer muss jede Rolle `snc_external` haben, um einen externen Benutzer zu kennzeichnen. Wenn Sie vorkonfigurierte Rollen haben, sollten die Rollen zugänglich sein, wenn Sie die Rollen entsperren und nach Benutzern suchen.
Nutzungsbedingungen aktivieren	Option zum Hinzufügen einer URL mit allgemeinen Bedingungen zur Registrierungsseite.
URL der Nutzungsbedingungen	Die öffentlich zugängliche URL, die die Nutzungsbedingungen des Registrierungsformulars enthält. Dieses Feld wird nur angezeigt, wenn **Allgemeine Bedingungen aktivieren** ausgewählt ist.
Beschreibung	Die Beschreibung des Registrierungsformulars. Dieses Feld wird nur angezeigt, wenn Sie die Konfiguration speichern oder absenden. In diesem Feld können Sie weitere Informationen zum Registrierungsformular hinzufügen. **Hinweis:** Sie können eine Beschreibung nur hinzufügen, nachdem Sie eine Benutzerregistrierungskonfiguration gespeichert oder aktualisiert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Anwendung, die diesen Datensatz enthält. Die Anwendung wird automatisch auf Globalfestgelegt.
Aktiv	Option, die die Benutzerregistrierungskonfiguration aktiviert. Diese Option ist standardmäßig ausgewählt.
CAPTCHA aktivieren	Option zum Hinzufügen eines CAPTCHA zum Registrierungsformular. Der standardmäßige CAPTCHA-Provider ist Google reCAPTCHA. **Hinweis:** Führen Sie die Schritte in Konfigurieren Sie Google reCAPTCHA für die Selbstregistrierung externer Benutzeraus, um CAPTCHA für die Benutzerregistrierung zu aktivieren.

3. Klicken Sie auf **Absenden**.
Eine Benutzerregistrierungskonfiguration mit den Standardeinstellungen wird erstellt.



4. **Wahlweise:** Konfigurieren Sie die Registerkarte **Registrierung**, um Felder und die Reihenfolge anzuzeigen, in der sie angezeigt werden:

Registrierungsformularfelder

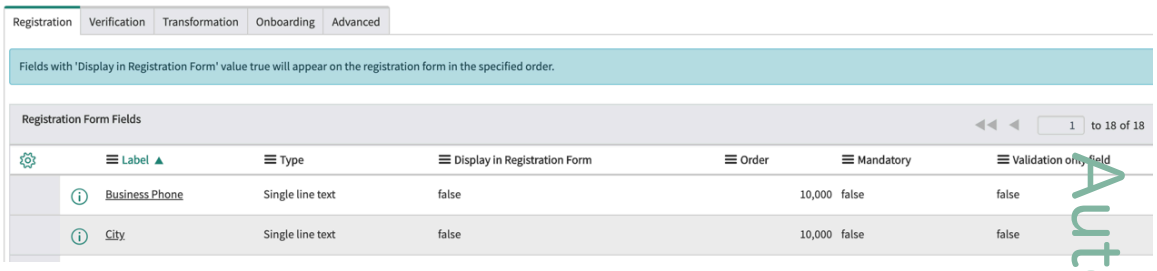
Spalte	Beschreibung
Im Registrierungsformular anzeigen	Legen Sie jedes Feld, das Sie anzeigen möchten, als True fest.
Reihenfolge	Legen Sie eine Nummer für die Reihenfolge fest, um Felder in Ihrem Formular anzuzeigen.
Obligatorisch	Legen Sie jedes Feld, das Sie als Pflichtfeld festlegen möchten, auf True fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Nur Validierungsfeld	Legen Sie ein beliebiges Feld fest, das nur zur Validierung verwendet werden soll. Beispiel: Registrierungscode.

Sie können die Standardformularfelder anzeigen oder dem Registrierungsformular benutzerdefinierte Formularfelder hinzufügen. Weitere Informationen finden Sie unter Standardfelder des Registrierungsformulars.

Registerkarte „Registrierung“.



Sie können auch benutzerdefinierte Registrierungsformularfelder hinzufügen. Weitere Informationen finden Sie unter Fügen Sie ein benutzerdefiniertes Registrierungsformularfeld hinzu.

5. **Wahlweise:** Konfigurieren Sie die Registerkarte **Verifizierung**, um die Identität der registrierten Benutzer zu überprüfen. Wenn der Benutzerverifizierungs-Flow ausgelöst wird, wird ein Aktivierungslink an die registrierte E-Mail-Adresse des Benutzers gesendet.

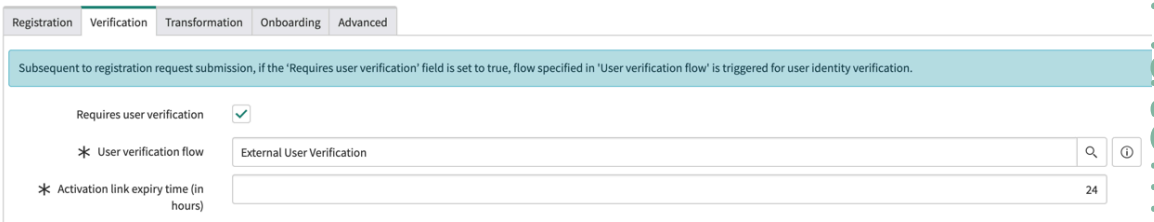
Felder der Registerkarte „Überprüfung“.

Feld	Beschreibung
Anwenderverifizierung erforderlich	Option zum Auslösen eines Benutzerverifizierungs-Subflows, der nach der Benutzerregistrierung ausgeführt wird. Der Subflow dient der Überprüfung der Benutzeridentität.
Flow der Anwenderverifizierung	Der zur Überprüfung der Identität des Benutzers verwendete Subflow. Der Subflow wird nur ausgelöst, wenn Sie die Benutzerverifizierung aktivieren. (Optional) Der Subflow „ **Verifizierung externer Benutzer** “ ist standardmäßig verfügbar. Sie können eine Kopie des Standard-Subflows in Flow Designer erstellen und ihn entsprechend Ihren Anforderungen ändern. Weitere Informationen finden Sie unter Flow Designer .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

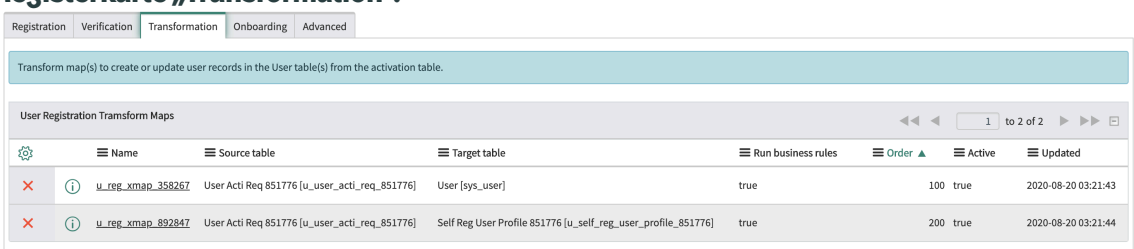
Feld	Beschreibung
	Hinweis: Um eine Vorschau des Subflows „ **Externe Benutzerverifizierung** “ auf einer neuen Registerkarte anzuzeigen, verwenden Sie die folgenden Kurzbefehle: ○ Macintosh: Befehlstaste + Klicken ○ Windows: Strg + Klicken
Ablaufzeit des Aktivierungslinks (in Stunden)	Die Anzahl der Stunden, nach denen ein Aktivierungslink abläuft. Der Standardwert ist 24.

Registerkarte „Überprüfung“.



6. **Wahlweise:** Konfigurieren Sie die Registerkarte **Transformation**, um selbst registrierte Benutzer und aktivierte Benutzer zuzuordnen.
   Es gibt zwei Transformationszuordnungen (u_reg_xmap_[Nummer]), die die registrierten Benutzer automatisch aus der Tabelle „Anwender-Aktiv.-Anforderung“ [Nummer] der Tabelle „Selbst registrierter Benutzer“ [Nummer] zuordnen. Sie können eine Kopie dieser Standard-Transformationszuordnungen erstellen und die Zuordnung entsprechend Ihren Anforderungen ändern. Weitere Informationen finden Sie unter Transformationszuordnungen .

Registerkarte „Transformation“.



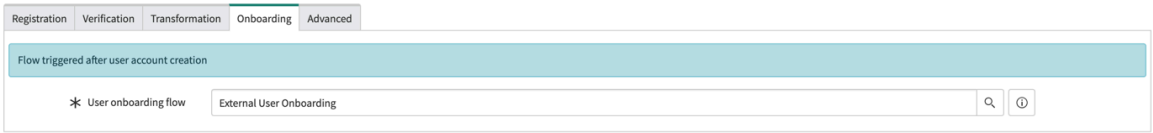
7. Konfigurieren Sie die Registerkarte Onboarding, um **Subflows** für das Onboarding aktivierter Benutzer auszulösen.
   Der standardmäßige **Subflow** für das Onboarding externer Benutzer sendet eine E-Mail an den Benutzer, die einen Link zum Zurücksetzen des Passworts enthält. Sie können eine Kopie des Standard-Subflows erstellen und ihn entsprechend Ihren Anforderungen ändern.

   Hinweis:
   Wenn der **Subflow „Onboarding externer Benutzer“** ausgelöst wird, sendet der Subflow eine E-Mail an den Benutzer, die einen Link zum Zurücksetzen des Passworts enthält.

Automatische Übersetzung

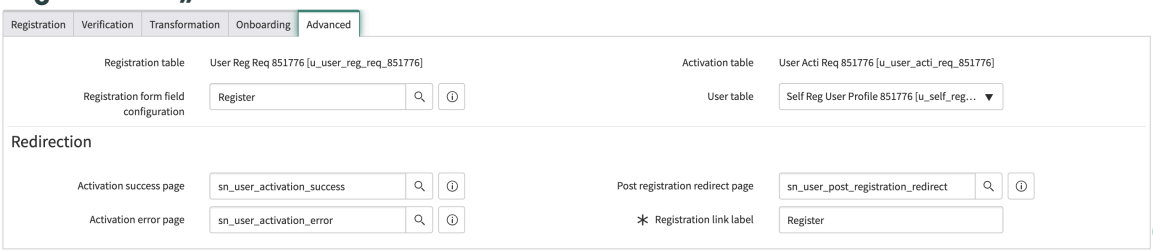
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Onboarding-Registerkarte



8. **Wahlweise:** Konfigurieren Sie die Registerkarte **Erweitert**, um Benutzertabellen und Umleitungsseiten des Registrierungsformulars zuzuordnen.

Registerkarte „Erweitert“



Registerkarte „Erweitert“

Feld	Beschreibung
Registrierungstabelle	Name der Tabelle, in der die Registrierungsformularinformationen gespeichert werden.
Konfiguration des Registrierungsformularfelds	Der Datensatz, der dem Registrierungsformular im Datensatzersteller zugeordnet ist.
Aktivierungstabelle	Bezeichnung und Name der für die Benutzeraktivierung verwendeten Tabelle. Die Aktivierungstabelle enthält Datensätze der Benutzer, die die Verifizierung abgeschlossen haben.
Anwendertabelle	Bezeichnung und Name der Benutzerprofiltabelle.
Aktivierungserfolgsseite	Die Seite, auf die ein Benutzer nach einer erfolgreichen Aktivierung umgeleitet wird.
Aktivierungsfehlerseite	Die Seite, zu der ein Benutzer weitergeleitet wird, wenn die Aktivierung fehlschlägt.
Weiterleitungsseite nach Registrierung	Die Seite, zu der der Anwender nach der Registrierung weitergeleitet wird.
Registrierungslinkbezeichnung	Der Name der Schaltfläche, die für die Registrierung über das Service Portal verwendet wird. Der Standardwert ist Register.

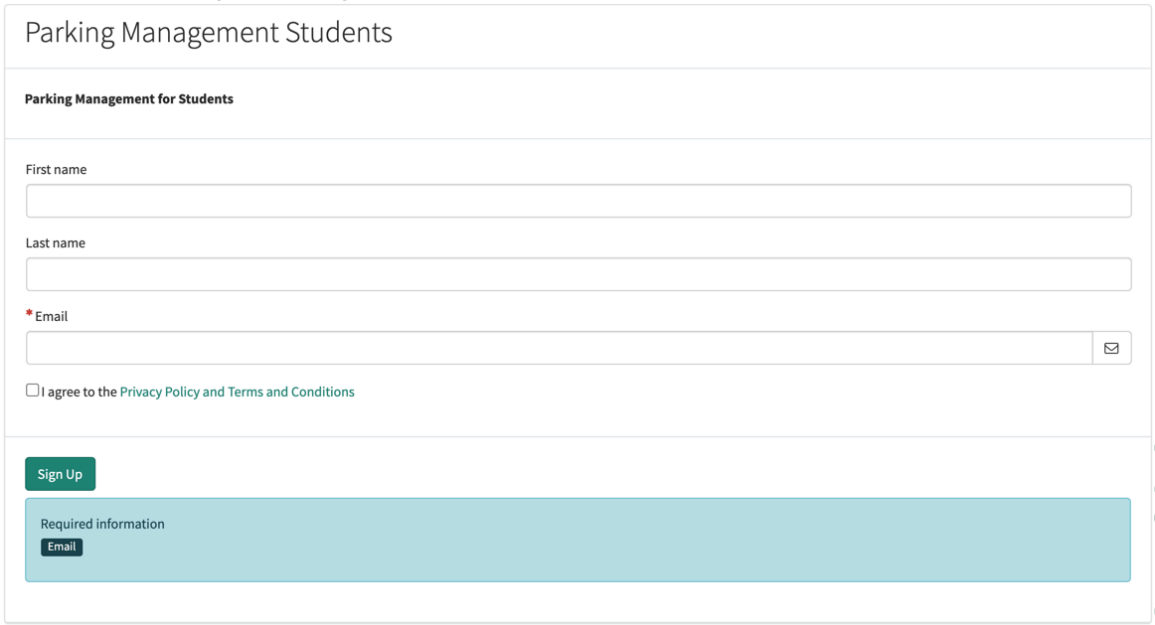
Während Sie Änderungen vornehmen oder nachdem Sie alle Änderungen an der Benutzerregistrierungskonfiguration vorgenommen haben, können Sie die Schaltfläche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorschau des **Registrierungsformulars** verwenden, um eine Vorschau der Änderungen im Registrierungsformular anzuzeigen.

Vorschau auf Registrierungsformular



Konfigurieren Sie Google reCAPTCHA für die Selbstregistrierung externer Benutzer

Um den Service Google reCAPTCHA zu verwenden, müssen Sie ein API-Schlüsselpaar von Google anfordern und dann die zugehörigen Systemeigenschaften konfigurieren.

Vorbereitungen

- Fordern Sie ein API-Schlüsselpaar (einen Site-Schlüssel und ein Geheimnis) von Google unter https://www.google.com/recaptcha an.
- Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach den folgenden Eigenschaften, und legen Sie die Werte fest:

Eigenschaft	Wert
glide.user.registration.google.recaptcha.secret	Das Geheimnis autorisiert die Kommunikation zwischen der Anwendung und dem reCAPTCHA-Server. Typ: password2
glide.user.registration.google.recaptcha.site_key	Der Websiteschlüssel, der zum Aufrufen des reCAPTCHA-Service auf Ihrer Registrierungsseite verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Wert
	Typ: Zeichenfolge
glide.user.registration.captcha.widget	Die Sys_ID des Captcha-Widgets. Typ: Zeichenfolge

Standardfelder des Registrierungsformulars

Sie können die standardmäßigen Registrierungsformularfelder verwenden oder benutzerdefinierte Registrierungsformularfelder erstellen.

Felder des Registrierungsformulars

Die folgenden Formularfelder werden standardmäßig im Registrierungsformular hinzugefügt.

Feldbezeichnung	Typ
Geschäftstelefon	Einzeiliger Text
Stadt	Einzeiliger Text
Land	Auswahlfeld
EDU-Status Wird verwendet, um Mitarbeiter, Studenten und Besucher zu unterscheiden. **Hinweis:** Dieses Feld ist nützlich, wenn das Registrierungsformular für eine Bildungseinrichtung gilt.	Auswahlfeld
E-Mail	E-Mail
Vorname	Einzeiliger Text
Geschlecht	Einzeiliger Text
Telefon (privat)	Einzeiliger Text
Sprache	Auswahlfeld
Nachname	Einzeiliger Text
Zweiter Vorname	Einzeiliger Text
Mobiltelefon	Einzeiliger Text
Name	Einzeiliger Text
Präfix Titel des Benutzers. Beispiel: Herr, Dr.	Auswahlfeld
Bundesland/Region	Einzeiliger Text
Straße	Breite einzeilige Textzeile

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Typ
Titel: Stellenbezeichnung	Auswahlfeld
Postleitzahl	Einzeiliger Text

Hinweis:
Sie können die Standardfelder des Registrierungsformulars nicht löschen.

Fügen Sie ein benutzerdefiniertes Registrierungsformularfeld hinzu

Sie können benutzerdefinierte Felder im Selbstregistrierungsformular des Benutzers hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Konfigurationen der Benutzerregistrierung**.
2. Öffnen Sie den Datensatz für die erforderliche Benutzerregistrierungskonfiguration.
3. Navigieren Sie zum Ende des Abschnitts „Registrierungsformularfelder“, und klicken Sie auf **Neue Zeile einfügen...**.
4. Geben Sie den Feldnamen unter der **Spalte** Bezeichnung ein, und klicken Sie auf das Häkchen.
   Eine neue Zeile mit den Standardwerten wird hinzugefügt. Sie können das benutzerdefinierte Registrierungsformularfeld entsprechend Ihren Anforderungen konfigurieren.

Feldspalten des Registrierungsformulars

Spalte	Beschreibung
Bezeichnung	Der Feldname, der im Registrierungsformular angezeigt wird.
Typ	Der Typ des Benutzeroberflächenelements. Im Folgenden sind die unterstützten Typen aufgeführt: ○ Einzeiliger Text ○ E-Mail ○ Datum ○ Datum/Uhrzeit ○ Ja/Nein ○ Breite einzeilige Textzeile ○ Multiple-Choice ○ Auswahlfeld
Im Registrierungsformular anzeigen	Option zum Anzeigen des Felds im Registrierungsformular.
Reihenfolge	Die Reihenfolge, in der die Formularfelder im Registrierungsformular angezeigt werden. Das Feld mit dem niedrigsten Reihenfolgewert wird zuerst und das Feld mit dem höchsten Reihenfolgewert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	wird zuletzt angezeigt. Der Standardwert beträgt 10.000.
Obligatorisch	Option, um ein Feld im Registrierungsformular obligatorisch zu machen.
Nur Validierungsfeld	Option, um ein Feld nur zu Validierungszwecken zu verwenden. Beispiel: Registrierungscode. Bei „true“ wird dieses Feld nicht in der Benutzertabelle (sys_user) gespeichert.

5. Speichern oder aktualisieren Sie die Änderungen.

Aktivieren der Selbstregistrierung externer Benutzer für Serviceportal

Ermöglichen Sie externen Benutzern die Registrierung für ServiceNow-Apps über Serviceportal.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Serviceportal** > **Portale**.
2. Öffnen Sie einen Portaldatensatz.
3. Füllen Sie im Formular das Feld **Konfiguration der Registrierung externer Benutzer** aus.

   Wählen Sie eine Benutzerregistrierungskonfiguration aus.
4. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Das Anmelde-Widget enthält einen Link zu dem Registrierungsformular, das Sie zuvor konfiguriert haben.

Externe Rollen in der Selbstregistrierung

Um zu verhindern, dass externen Benutzern versehentlich Zugriff gewährt wird, können Sie allen externen Benutzern die Rolle snc_external zuweisen.

Externen Benutzern, die sich selbst registrieren, muss die Rolle snc_external mit den geringsten Berechtigungen zugewiesen werden. Die Rolle snc_external gibt an, dass es sich um einen für Ihre Organisation externen Benutzer handelt, der keinen Zugriff auf Ressourcen hat, solange der Rolle snc_external oder anderen Rollen, die die Rolle snc_external übernehmen, keine expliziten Zugriffsrechte über ACLs erteilt wurden.

Standardmäßig haben Benutzer mit der Rolle snc_external keinen Zugriff auf:

- Scripted REST API-Ressourcen, die nicht als extern markiert sind
- Tabellen ohne die Rolle, die die Rolle snc_external oder public erbt
- Ressourcen, die keine Datensatztypen sind, z. B. Prozessoren und UI-Seiten ohne die Rolle snc_external oder eine Rolle, die die Rolle snc_external erbt
- Now Intelligence-Dashboards.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab dem Paris-Release müssen Sie eine Ausschlusslisten-Eigenschaft aktivieren, um die explizite Zuweisung von snc_external-Rollen zu erzwingen. Informationen zum Aktivieren der Eigenschaft finden Sie unter Zukünftige interne Rollenzuweisungen für externe Benutzer verhindern .

Überprüfen Sie die Anforderungen der Benutzer-Selbstregistrierung

Nachdem sich ein Benutzer über Serviceportalregistriert hat, wird dem Modul „Registrierungsanforderungen“ ein Benutzerdatensatz hinzugefügt. Sie können die Liste der registrierten Benutzer anzeigen, die sich erfolgreich im Serviceportalregistriert haben.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Anforderungen zur Registrierung**.
   Die Liste der Benutzerdatensätze wird angezeigt.
2. **Wahlweise:** Überprüfen Sie die einzelnen Benutzerdatensätze, und ändern Sie sie entsprechend Ihren Anforderungen.
   Sie können beispielsweise den Status eines Benutzerdatensatzformulars **Ausstehend** in **Verarbeitet**ändern.

Tokenbasierte Authentifizierung (Benutzeranmeldungen)

Verbessern Sie den Sicherheitsmechanismus für Benutzer, um über die tokenbasierte Authentifizierung auf ein Netzwerk zuzugreifen.

Zeitlich begrenzte Authentifizierung

der Digest-Token-Authentifizierung

Die Digest-Token-Authentifizierung übergibt Benutzeranmeldeinformationen und ein Digest-Token in einem unverschlüsselten HTTP-Header.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die tokenbasierte Authentifizierung ist ein Protokoll, mit dem Benutzer ihre Identität überprüfen und im Gegenzug ein eindeutiges Zugriffstoken erhalten können.

Sie trägt dazu bei, den Sicherheitsmechanismus für den Zugriff von Benutzern auf ein Netzwerk zu verbessern.

Zeitlich begrenzte Authentifizierung

Support der zeitlich begrenzten Authentifizierung für Ihre ServiceNow -Instanz.

Erkunden

Lernen Sie die Funktionen und den Geschäftsnutzen der zeitlich begrenzten Authentifizierung kennen.

Aktivieren

Machen Sie sich mit der Aktivierung der zeitlich begrenzten Authentifizierung vertraut.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tutorial: Zeitlich begrenzte Authentifizierung

Informieren Sie sich über die Eigenschaften in Zero Trust Access.

Zeitlich begrenzte Authentifizierung erkunden

Support der zeitlich begrenzten Authentifizierung für Ihre ServiceNow -Instanz.

Hinweis:
Die zeitlich begrenzte Authentifizierung ist sehr spezifisch für die Instanz ServiceNow, die benutzerdefinierten Links für Benutzer können nur innerhalb von ServiceNowerstellt werden.

Administratoren können die linkbasierte Authentifizierung für die Instanz ServiceNow konfigurieren. Der konfigurierte Link kann per E-Mail oder SMS für den Benutzer freigegeben werden, und der Benutzer kann sich über diese Links bei der Instanz anmelden.

Die Anmeldung bei der Instanz mit diesem Authentifizierungsschema wird über Richtlinien für adaptive Authentifizierung gesteuert, die in der Instanz ServiceNow konfiguriert sind.

Mit der zeitbasierten Authentifizierung können Sie Folgendes ausführen:

- Der Administrator kann die linkbasierte Authentifizierung so konfigurieren, dass sie innerhalb einer Ablaufzeit verwendet wird.
- Das Anwendungsteam kann Nonce abrufen, die mit dem Link für das spezifische Konfigurationselement über die verfügbar gemachte skriptfähige API verwendet werden soll. Die Linkgenerierung erfolgt durch das Anwendungsteam.
- Das Anwendungsteam kann den Link generieren und über einen vorhandenen Kanal an den Benutzer senden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Benutzer mit dem Link können sich einmal und innerhalb der im Rahmen der Konfiguration angegebenen Ablaufzeit bei der Instanz anmelden.
- Administratoren können die Rollen mit geringen Berechtigungen für das Authentifizierungsschema konfigurieren.
- Administratoren können MFA für das Authentifizierungsschema als zweiten Faktor für die Authentifizierung mit dem TLA-Link erzwingen.

Aktivieren Sie die zeitlich begrenzte Authentifizierung

Die zeitlich begrenzte Authentifizierung wird über das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“ aktiviert.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis:
Die zeitlich begrenzte Authentifizierung ist sehr spezifisch für die Instanz ServiceNow, die benutzerdefinierten Links für Benutzer können nur innerhalb von ServiceNowerstellt werden.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Time Limited Authentication“ (`com.snc.authenticate.time_limited_authentication`).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

   Hinweis:
   Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Zeitlich begrenzte Authentifizierung mit SMS – Twilio Tutorial

Richten Sie die zeitlich begrenzte Authentifizierung mit MFA-Faktoren wie SMS mit Twilioein.

Vorbereitungen
Erforderliche Rolle: admin

Erforderliche Plugins:

- `com.snc.authenticate.time_limited_authentication` (zeitlich begrenzte Authentifizierung)
- `com.snc.authentication.sms_mfa` (Multifaktor-Authentifizierung mit SMS)

Hinweis:
Die zeitlich begrenzte Authentifizierung (TLA) ist spezifisch für die Instanz ServiceNow, die benutzerdefinierten Links für Benutzer können nur innerhalb von ServiceNowerstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die bereitgestellten Tutorial-Anweisungen ermöglichen es dem Administrator, eine linkbasierte Anmeldung mit SMS als zweiten Faktor (MFA) für Benutzer mit einer bestimmten Rolle bereitzustellen.

Nach einer erfolgreichen Konfiguration generiert das System einen Link und gibt den Link dann über den Benachrichtigungskanal (E-Mail/SMS) für den Benutzer frei. Wenn der Benutzer auf den Link klickt, wird er aufgefordert, die an die E-Mail gesendete Einmalpasswort oder den SMS-Faktor basierend auf der Benutzerrolle (Konfiguration) anzugeben.

Hinweis:

- Auf TLA muss immer MFA folgen, und MFA muss von einem Administrator mithilfe der adaptiven Authentifizierung für die TLA-Anmeldung aktiviert werden. Weitere Informationen zur Konfiguration von MFA mit adaptiver Authentifizierung finden Sie unter MFA-Kontext (Multifaktor-Authentifizierung)..
- TLA sollte für Benutzer mit eingeschränkten Berechtigungen verwendet werden.

Prozedur

1. Erstellen einer Twilio -Konfiguration.

a. Erstellen Sie ein Testkonto Twilio.
Weitere Informationen finden Sie unter Twilio .

b. Navigieren zu **Alle** > **Benachrichtigen** > **Administration** > **Twilio Direct-Konfiguration**.

c. Geben Sie die **Account-SID** und das **Auth-Token** (erstellt aus Twilio) an, und speichern Sie den Datensatz.

Hinweis:
Sie können eine eigene Provider-Konfiguration erstellen und diese für TLA verwenden. In diesem Beispiel ist dies Twilio. Weitere Informationen zum Erstellen einer MFA-Provider-Konfiguration finden Sie unter Konfigurieren Sie den MFA-Provider.

2. Konfigurieren und aktivieren Sie den TLA-Datensatz (Time Limited Authentication).

a. Navigieren zu **Alle** > **Konfigurationsdatensätze für zeitlich begrenzte Authentifizierung** und wählen Sie **Neu**.

b. Füllen Sie die Felder im Formular aus.

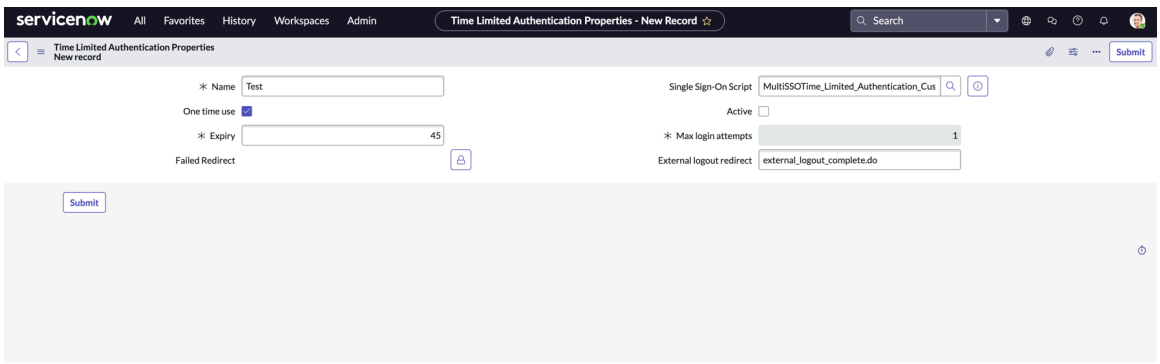
Eigenschaften der zeitlich begrenzten Authentifizierung

Feld	Beschreibung
Name	Name des Datensatzes.
Einmalige Nutzung	Wählen Sie diese Option aus, um den TLA-Link einmal zu verwenden.
Ablauf	Geben Sie die Sekunden für den Linkablauf an. Der Standardwert beträgt 45 Minuten.
Fehlerhafte Umleitung	Geben Sie die URL ein, um Benutzer nach einer fehlgeschlagenen Authentifizierung umzuleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Single Sign-on-Skript	Details des SSO-Skripts, das Sie verwenden möchten.
Aktiv	Option zum Aktivieren der Konfiguration.
Max. Anmeldeversuche	Geben Sie die Anzahl der mit dem generierten TLA-Link für die Anmeldung zulässigen Versuche an. Deaktivieren Sie die Checkbox **Einmalig verwenden**, um die maximale Anzahl von Versuchen anzugeben.
Weiterleitung für externe Abmeldung	Geben Sie die URL ein, um Benutzer nach der Abmeldung umzuleiten.

c. Wählen Sie **Absenden**.



d. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Administration** > **Eigenschaften** und aktivieren Sie die Eigenschaft **SSO für mehrere Anbieter** aktivieren, und klicken Sie auf **Speichern**.

3. Zulassen von TLA nur für eine bestimmte Benutzerpersona mithilfe der Kontextrichtlinie nach der Authentifizierung.

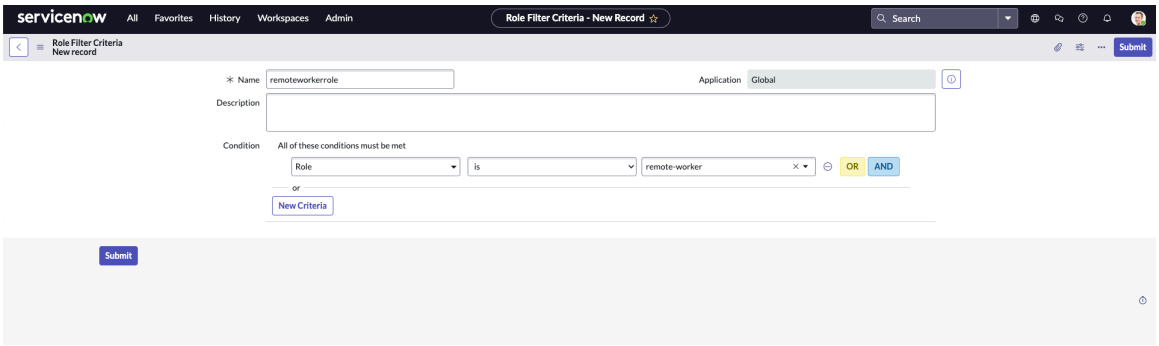
a. Navigieren Sie zu **Rollen**, und erstellen Sie eine Rolle.
Beispiel: remote_worker.

b. Erstellen Sie einen Benutzer mit einer gültigen E-Mail-ID und Mobiltelefonnummer.
Informationen zum Erstellen eines Benutzers finden Sie unter Benutzer erstellen .

c. Weisen Sie die Rolle dem Benutzer zu.
Informationen zum Zuweisen der Rolle an den Benutzer finden Sie unter Einem Benutzer eine Rolle zuweisen.

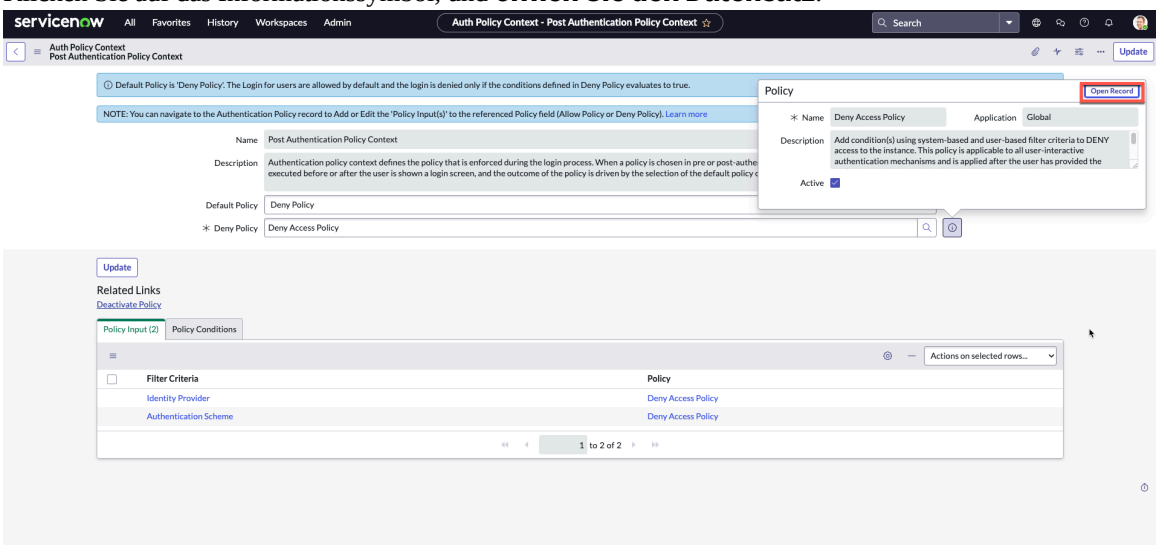
d. Um Rollenfilterkriterien zu erstellen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Rollen-Filterkriterien**, erstellen Sie einen Filter **remoteworkerrole**, und stellen Sie die Bedingung **Rolle auf remote_worker**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

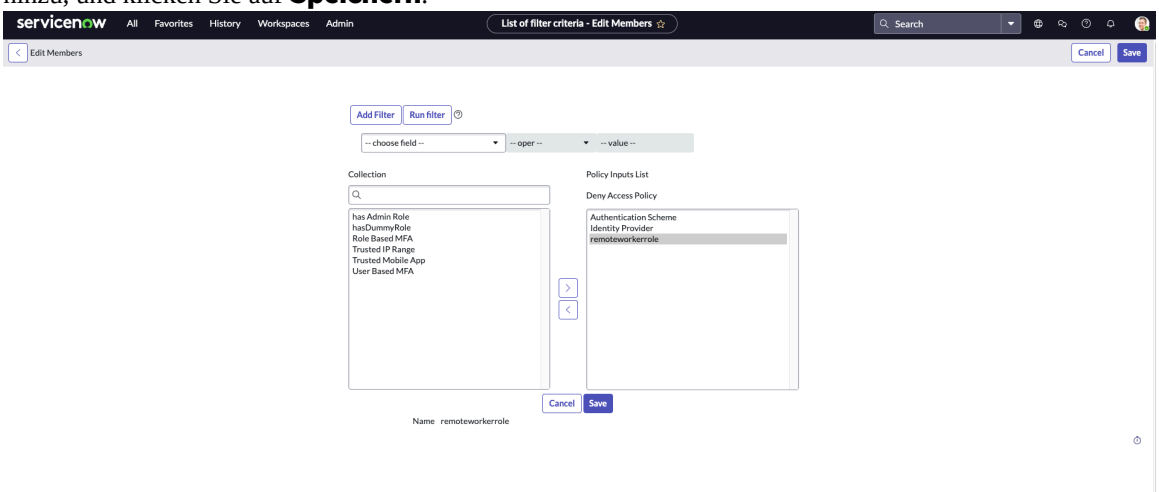


e. Um eine Richtlinienbedingung basierend auf dem Deny-Richtlinienkontext basierend auf den IdP- und Rollenfilterkriterien hinzuzufügen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Kontext nach der Authentifizierung**.

f. Klicken Sie auf das Informationssymbol, und **öffnen Sie den Datensatz**.



g. Wählen Sie in der Richtlinieneingabe die Option **Bearbeiten** aus, fügen Sie die Rolle (remoteworkerrole) hinzu, und klicken Sie auf **Speichern**.



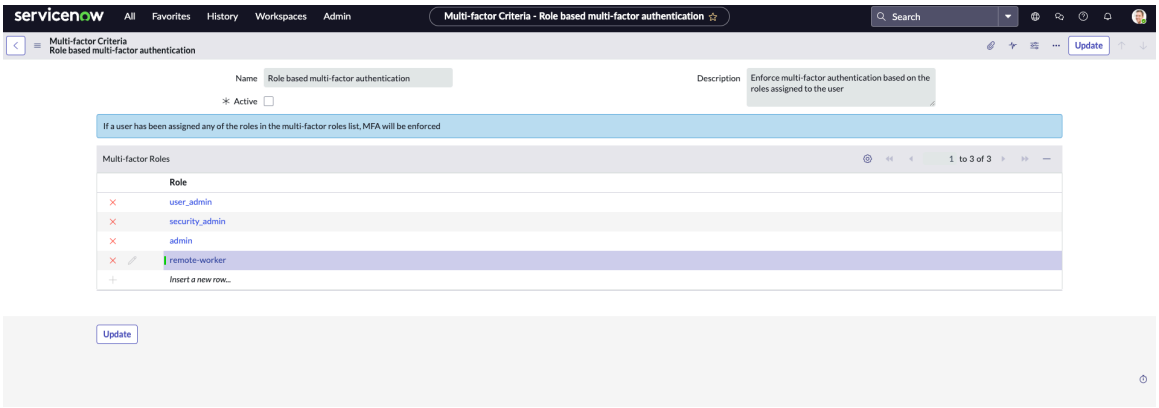
h. Fügen Sie in der Richtlinienbedingung die Bedingung für die Richtlinieneingabe hinzu, und **übermitteln** Sie den Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Konfigurieren Sie die Step-up-Authentifizierungsrichtlinie – MFA-Kontext.

a. Navigieren zu **Alle** > **Multifaktor-Kriterien**.

b. Wählen Sie die **rollenbasierte Multifaktor-Authentifizierung aus**, fügen Sie die Rolle im Abschnitt „Multifaktor-Rollen“ hinzu, und klicken Sie auf **Aktualisieren**.
In diesem Beispiel: **remote_worker**.

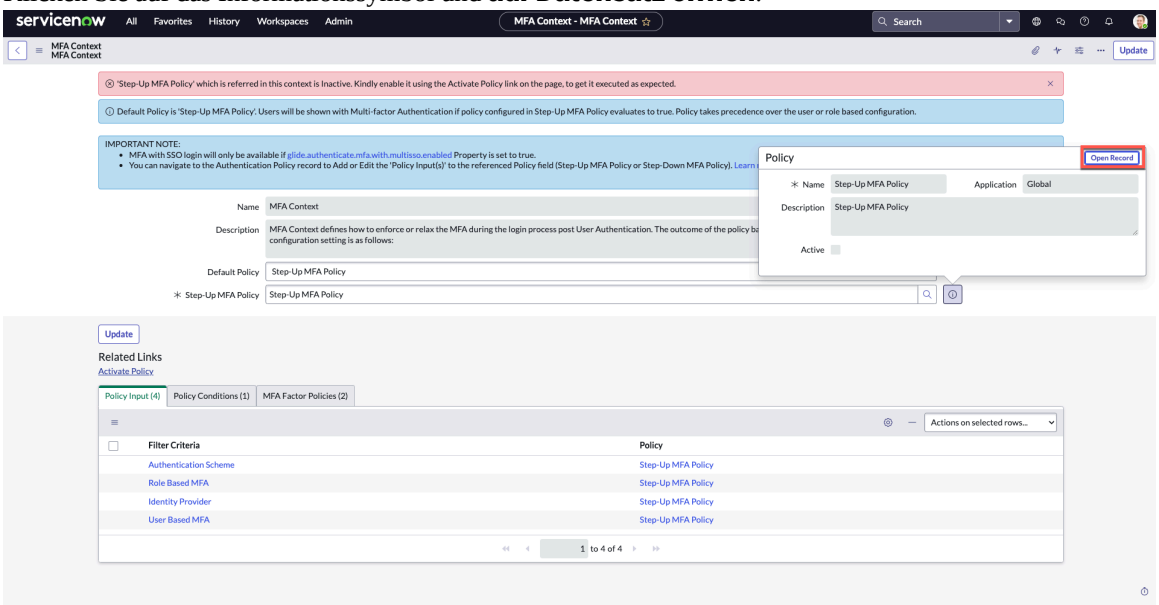


c. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **MFA-Kontext**.

d. Stellen Sie sicher, dass diese Felder wie folgt festgelegt sind:

- Das Feld Standardrichtlinie ist **Step-up-MFA-Richtlinie**
- Step-Up-MFA-Richtlinie ist **Step-Up-MFA-Richtlinie**

e. Klicken Sie auf das Informationssymbol und **auf Datensatz öffnen**.



f. Wählen Sie im Formular „Step-Up-MFA-Richtlinie“ in den Richtlinieneingaben die Option **Bearbeiten**aus.

g. Fügen Sie der Liste die **rollenbasierte Multifaktor-Authentifizierung** hinzu, und klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Beispiel **remoteworkerrole**.

h. Wählen Sie in der Richtlinienbedingung MFA erzwingen, **wenn rollenbasierte oder benutzerbasierte MFA-Einstellungen true sind**.

i. Stellen Sie auf der Seite MFA erzwingen, wenn **rollen-** oder benutzerbasierte MFA-Einstellungen wahr sind sicher, dass rollenbasierte MFA auf **wahr**gesetzt ist.

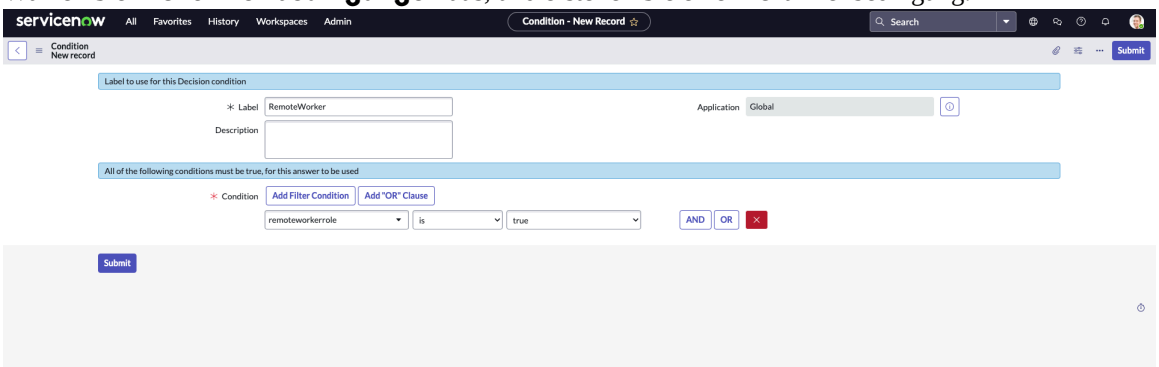
5. Erzwingen Sie die Verwendung von SMS als MFA-Faktorrichtlinie für MFA.

a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **MFA-Kontext**.

b. Wählen Sie auf der Seite „MFA-Kontext“ **MFA-Faktorrichtlinien** und dann eine Richtlinie **SMS-OTP als MFA-Faktorrichtlinie anzeigen aus**.

c. Wählen Sie **Bearbeiten** aus, und fügen Sie die **Rolle remoteworker** in den **Richtlinieneingaben**hinzu.

d. Wählen Sie **Richtlinienbedingungen** aus, und erstellen Sie eine Richtlinienbedingung.



e. Wählen Sie **Absenden**.

Der TLA-Link, der generiert und für die Benutzer freigegeben wird, denen die Rolle „ **remoteworkerrolle** “ zugewiesen ist, wird heraufgestuft, um den SMS-Code als zweiten Faktor für die Anmeldung bei der Instanz zu verwenden.

6. Aktivieren Sie die anderen erforderlichen Eigenschaften.

a. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Eigenschaften**.

b. Aktivieren Sie die folgenden Checkboxen.

- **Multi-Faktor-Authentifizierung aktivieren**
- **Aktivieren Sie die Multifaktor-Authentifizierung mit SSO**

c. Speichern Sie den Datensatz.

d. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Aktivieren Sie das Kontrollkästchen **Authentifizierungsrichtlinie aktivieren**.

f. Speichern Sie den Datensatz.

7. TLA-Link generieren – Beispiel.

a. Navigieren zu **Alle** > **Systemdefinition** > **Skripts – Hintergrund**.

b. Verwenden Sie die folgende API, indem Sie die Benutzer-sys_id und die Konfigurations-ID angeben.
`var tla=new global.TimeLimitedAuthentication(); gs.info(tla.generateNonce("user_sysid", "config1_sys_id","IAR2"));`

> **Hinweis:**
> Die Quelle (IAR2) ist kein erforderlicher Parameter.

c. Der Abfrageparameter wird wie gezeigt zurückgegeben:
`nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d344351110f8779b5`

d. Erstellen Sie eine URL im folgenden Format:
`https://<instance-url> /login_with_sso.do?uri=<encoded url> & nonce=2olIQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf037102000044e0bfc8`

8. Wählen Sie die URL aus, und der folgende MFA-Bildschirm wird für die Anmeldung angezeigt.

Digest-Token-Authentifizierung

Die Digest-Token-Authentifizierung übergibt Benutzeranmeldeinformationen und ein Digest-Token in einem unverschlüsselten HTTP-Header.

Erkunden

Konfigurieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lernen Sie die Funktionen und den Geschäftsnutzen der Digest-Token-Authentifizierung kennen.	Machen Sie sich mit der Konfiguration der Digest-Token-Authentifizierung vertraut.

Digest-Tokenauthentifizierung erkunden

Die Instanz liest den HTTP-Header-Wert und vergleicht den berechneten Hash-Wert des Digest-Tokens. Wenn der berechnete Hash-Wert mit dem Digest-Token-Wert übereinstimmt, sucht die Instanz nach einem übereinstimmenden Wert in der Benutzertabelle. Wenn in der Benutzertabelle ein übereinstimmender Wert vorhanden ist, betrachtet die Instanz den Benutzer als vorauthentifiziert und meldet ihn an.

Die Digest-Token-Authentifizierung ist sicherer als einfache unverschlüsselte HTTP-Kopfzeilen, da jede versehentliche oder beabsichtigte Änderung der unverschlüsselten HTTP-Kopfzeile einen anderen Hash-Wert erzeugt. Wenn der Hash-Wert nicht übereinstimmt, verweigert die Instanz dem Benutzer den Zugriff auf die angeforderte Instanz. Dadurch wird verhindert, dass Benutzer versuchen, sich mit den Anmeldeinformationen eines anderen Benutzers anzumelden.

Weitere Informationen zum Ablauf von Digest-Links finden Sie in diesem KB-Artikel .

Hinweis:
Verwenden Sie die zeitlich begrenzte Authentifizierung (TLA), um zeitbasierte Ablauf-Links zu konfigurieren. Weitere Informationen finden Sie unter Zeitlich begrenzte Authentifizierung.

Integrationsanforderungen

Eine Integration der Digest-Token-Authentifizierung erfordert:

- Ein Webserver
- SiteMinder oder eine andere Single Sign-on-Anwendung, um den Benutzer im lokalen Netzwerk vorab zu authentifizieren
- Eine Webseite oder ein Portal, die Benutzeranmeldeinformationen in einem der folgenden Formate an die Zielinstanz übergibt
  - HTTP-Header
  - URL-Parameter
  - Cookie
- Eine Webseite oder ein Portal, die bzw. das ein Digest-Token erstellt und mithilfe einer der folgenden Codierungstechniken an die Zielinstanz übergibt
  - SHA1
  - MD5
  - SHA 256 (empfohlen)

Digest-Eigenschaften für Single Sign-on (SSO) für mehrere Anbieter konfigurieren

Nachdem Sie ein Digest-Installations-Exist-Skript aktiviert haben, konfigurieren Sie Eigenschaften für Multi-Provider-SSO.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie Single Sign-on mit mehreren Anbietern nicht verwenden, konfigurieren Sie Single Sign-on-Standardeigenschaften.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**.
2. Füllen Sie die Felder im Formular „Digest-Eigenschaften“ aus.

Option	Bezeichnung
Name	Geben Sie den Namen des Digest-Tokens ein.
Benutzer	Geben Sie das Feld sys_user ein, das die übereinstimmenden Daten für den eingehenden Header enthält.
HTTP-Digest-Headername	Geben Sie den generierten HTTP-Header ein. Beispiel: DE_USER.
HTTP-Headername	Geben Sie den HTTP-Header ein, den Sie für Ihr erstelltes Digest-Token generiert haben. Beispiel: SM_USER.
Geheime Passphrase	Geben Sie den geheimen Schlüssel ein, der zum Codieren von Digest-Schlüsseln verwendet werden soll. Zum Beispiel 32 oder mehr Zeichen.
Feld „SSO-Umleitung fehlgeschlagen“.	Geben Sie die URL ein, um Benutzer nach einer fehlgeschlagenen Authentifizierung umzuleiten.
Weiterleitung für externe Abmeldung	Geben Sie die URL ein, um Benutzer nach der Abmeldung umzuleiten.
Single Sign-on-Skript	Wählen **Sie MultiSSO_DigestedToken aus**.

3. Klicken Sie auf **Aktualisieren**.
4. Setzen Sie Ihr verarbeitetes Token standardmäßig auf „true“.
   Wenn Sie den Standardwert auf „true“ festlegen, wird der standardmäßige Digest-Token-Datensatz des Systems, der SSO zugeordnet ist, überschrieben. Sobald der erste mit Multi-Provider-SSO verbundene IdP-Datensatz aktiviert ist, werden nur Datensätze verwendet, die dem Multi-Provider-SSO zugeordnet sind.

   Digest-Token-Datensätze, die in der Digest-Eigenschaftstabelle vorhanden sind, können einzeln aufgerufen werden, indem die Sys_ID des IdP angehängt wird. Zum Beispiel ein Digest-Token-Datensatz in der folgenden Authentifizierungs-URL: https://<instance_name> .service-now.com/login_with_sso.do? glide_sso_id=<sys_id_of_Digest_token_record> &SM_USER=<user_name> &DE_USER=<digested_token>

Beispiel für Digest-Token-Implementierungen

Im Folgenden finden Sie einige Beispiele für die Erstellung eines Digest-Tokens.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielimplementierungen der Digest-Authentifizierung

Mit erstellter Digest	Wert des geheimen Schlüssels	Hash-Methode	Beispiel
Java	32 und mehr Zeichen	SHA256	Beispiel für einen Java Digest-Algorithmus für die Verschlüsselung
C	Wert des Parameters „sharedKey“.	Wert des strEncryptionMethod-Parameters (SHA256 oder MD5)	Beispiel C

Beispiel für einen Java Digest-Algorithmus für die Verschlüsselung

Dieser Java-Algorithmus veranschaulicht die Erstellung eines Digest-Tokens aus einem HTTP-Header.

Dieses Beispiel setzt Folgendes voraus:

- Der Webserver unterstützt Java
- Die Hash-Berechnungsmethode ist SHA1
- Der Wert des geheimen Schlüssels ist abc123
- Der unverschlüsselte HTTP-Header-Name ist user_name

Ändern Sie den Java-Code, um einen anderen Hash-Berechnungsmechanismus (z. B. MD5) zu verwenden, ändern Sie den Wert des geheimen Schlüssels oder den HTTP-Header-Namen.

```
public class DigestTest
{
   private static final String MAC_ALG = "HmacSHA256";
     fKey  = {32 or more characters};
   public byte[] getDigest(String acct) {
      try {
         byte[] bkey = fKey.getBytes();
         byte[] data = acct.getBytes();
         Mac mac = null;
         try {
            mac = Mac.getInstance(MAC_ALG);
            mac.init(new SecretKeySpec(bkey, MAC_ALG));
         } catch (Exception e) {
            e.printStackTrace();
         }
         byte[] sig = mac.doFinal(data);
         String signature = new String(sig);
         System.out.println("value:" + acct);
         System.out.println("digested value:  " + signature);
         return sig;
      } catch (IllegalStateException e) {
         e.printStackTrace();
      }
      return null;
   }
   public static void main(String[] args) {
      BASE64Encoder encoder = new BASE64Encoder();
      DigestTest test = new DigestTest();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        String userName = "user_name";
        System.out.println("base 64 digest username: " +
encoder.encode(test.getDigest(userName)));
    }
}
```

Beispiel C

Diese C-Klasse veranschaulicht die Erstellung eines Digest-Tokens aus drei Eingabeparametern.

- strEncryptionMethod – Listet die Hash-Berechnungsmethode auf (SHA1, SHA256 oder MD5)
- message – Listet den Wert auf, der in ein Digest-Token konvertiert werden soll
- sharedKey – Listet den geheimen Schlüssel auf

Hinweis:
Verwenden Sie einen sichereren Hash-Algorithmus wie SHA256 für die Generierung von Digest-Token.

Dieses Beispiel setzt Folgendes voraus:

- Der Webserver unterstützt C
- Anderer Code ruft diese Klasse auf und übergibt die erwarteten Parameter

Beispielcode

```
private stringdigestData(string strEncryptionMethod , string message , string sharedKey ) {
        UnicodeEncoding myUnicodeEncoding  = new UnicodeEncoding ( ) ;

        byte [ ] messageBytes  = System. Text. Encoding. ASCII. GetBytes (message ) ;
        byte [ ] sharedKeyBytes  = System. Text. Encoding. ASCII. GetBytes (sharedKey ) ;
        byte [ ] hashedMessage ;

        string b64SHA1Message ;

         if (this. DEBUG ) {
           TextBoxMessage. Text = message ;
           TextBoxSecret. Text = sharedKey ; }

         switch ( (strEncryptionMethod ) )

         { case "SHA1" :

              HMACSHA1 hmacsha1  = new HMACSHA1 ( ) ;
              hmacsha1. Key = sharedKeyBytes ;
              hashedMessage  = hmacsha1. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

            case "MD5" :

              HMACMD5 hmacmd5  = new HMACMD5 (sharedKeyBytes ) ;
              hashedMessage  = hmacmd5. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            default :
              b64SHA1Message  = "Unknown Encryption Method" ; break ;
          }

        TextBoxBase64. Text = b64SHA1Message ; return b64SHA1Message ;
      }
```

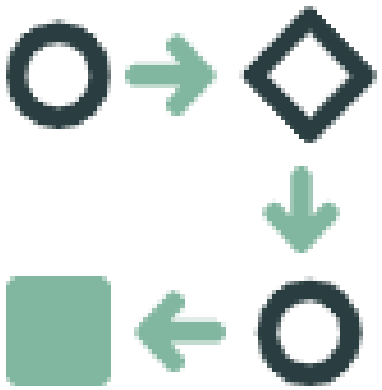
Zero Trust-Zugriff

Zero Trust EinZugriff (ZTA) ist ein Sicherheitsmodell, das davon ausgeht, dass standardmäßig keinem Benutzer oder Gerät vertraut wird.

Erkunden	Aktivieren
Lernen Sie die Funktionen und den Geschäftsnutzen von Zero Trust Access kennen.	Machen Sie sich mit der Aktivierung des Zero Trust-Zugriffs vertraut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren



Konfigurieren Sie Zero Trust-Zugriff.

Referenz: Eigenschaften

Informieren Sie sich über die Eigenschaften in Zero Trust Access.

Zero Trust-Zugriff erkunden

Zero Trust Access (ZTA) ist ein Sicherheitsmodell, bei dem davon ausgegangen wird, dass standardmäßig keinem Benutzer oder Gerät vertraut wird.

ZTA stellt sicher, dass jeglicher Zugriff auf Anwendungen und Daten erst nach Identitätsverifizierung und Risikobewertung des Benutzers auf der Grundlage der geringsten Berechtigung gewährt wird.

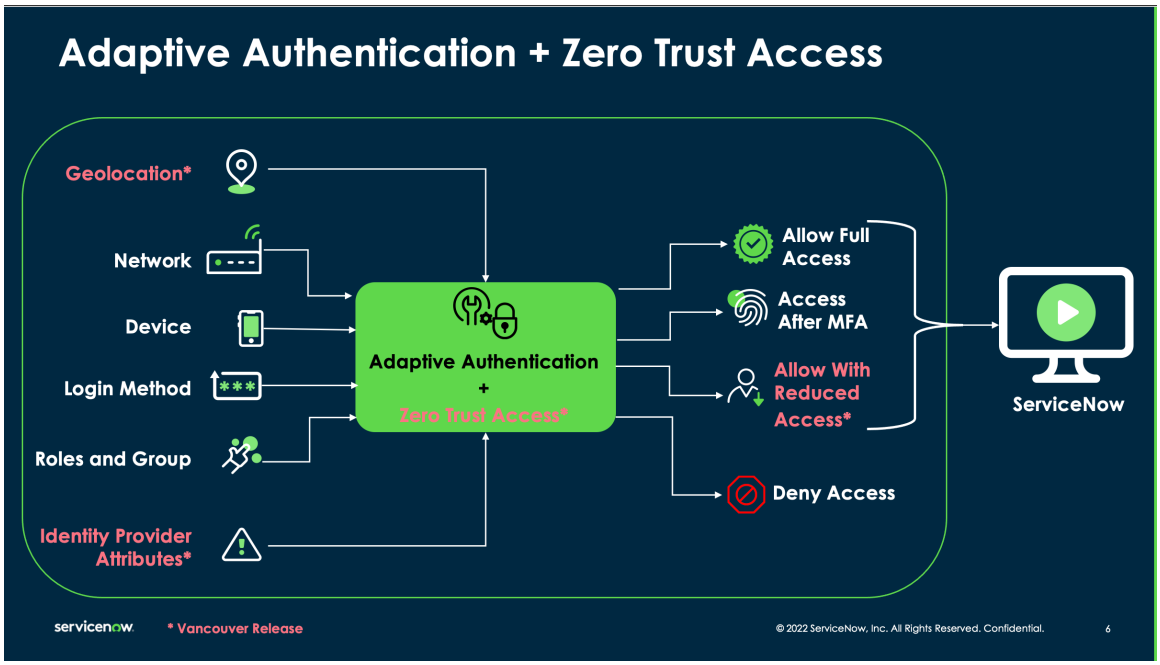
Zero Trust: Richtlinienbasierter Sitzungszugriff

ServiceNow® Mit Zero Trust – richtlinienbasierter Sitzungszugriff (Sitzungszugriff) können Organisationen die Benutzerberechtigungen in einer Websitzung basierend auf einer Vielzahl von Faktoren dynamisch reduzieren, darunter IP-Adresse, Standort, Authentifizierungsmethode, Rolle des Benutzers, Gruppe, Benutzer mit MFA und von gemeinsam genutzten Attributen Identitätsanbieter (IDP). Dies kann dazu beitragen, Organisationen vor nicht autorisiertem Zugriff und Datenschutzverletzungen zu schützen, selbst wenn Benutzer mit hohen Berechtigungen von nicht vertrauenswürdigen Geräten oder Standorten auf Anwendungen zugreifen.

Zero Trust: Richtlinienbasierter Sitzungszugriff

Es ermöglicht Sicherheitsadministratoren, den Benutzerzugriff in einer Sitzung basierend auf IP-Adresse, Standort, Identitätsanbieterattributen und Benutzerattributen mithilfe von adaptiven Authentifizierungsrichtlinien zu reduzieren oder zu beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- Sitzungszugriffskonfigurationen können nur mit der Rolle „ security_admin “ durchgeführt werden. Sie müssen Ihre Rolle auf security_adminerhöhen.
- Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Benutzer zugewiesen ist. In diesem Fall werden keine Änderungen an der angemeldeten Sitzung vorgenommen. Der Benutzer greift weiterhin mit den zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, solange der Benutzer bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Benutzer muss sich von der Sitzung abmelden, damit die Richtlinie wirksam wird.
- Der Sitzungszugriff hat keine Auswirkungen, wenn sich der Benutzer in einem vertrauenswürdigen Netzwerk befindet und später innerhalb einer Sitzung zu einem VPN wechselt (Änderung des Standorts oder Netzwerks).
- Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu einer Einschränkung des Zugriffs. Wenn beispielsweise ein Benutzer nach dem Einrichten der Sitzung vom Unternehmensnetzwerk in ein nicht vertrauenswürdiges Netzwerk wechselt, wird der Zugriff nur eingeschränkt, wenn sich der Benutzer abmeldet und erneut anmeldet.

Anwendungsfall

Im Folgenden sind einige der Anwendungsfälle von Zero Trust-Zugriff aufgeführt:

- Reduzieren Sie die Berechtigungen basierend auf dem mit der Sitzung verbundenen Risiko. Beispielsweise kann ein Benutzer mit Erfüllerrolle, der sich von außerhalb des vertrauenswürdigen Netzwerks anmeldet, so konfiguriert werden, dass er nur die Rolle „Anfordernde Person“ für die Sitzung hat.
- Reduzieren Sie den Zugriff basierend auf der IdP-Antwort für eine Benutzersitzung, wenn der Benutzer ein nicht vertrauenswürdiges Gerät verwendet. Weitere Informationen finden Sie unter Konfigurieren Sie das IdP-Attribut für den Sitzungszugriff.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Rollenzuordnung stellt sicher, dass der Benutzer keine anderen Berechtigungen in einer Sitzung hat. Wenn sich der Benutzer aus einem vertrauenswürdigen Netzwerk anmeldet, werden alle vorhandenen Berechtigungen für eine Sitzung zugewiesen.

Mehrere IP-Bedingungen und mehrere Rollen- oder Gruppenzuweisungen können als Teil der Richtlinie definiert werden.

Zero Trust-Zugriff – Mobile

Sie können die Richtlinie „Zero Trust Access – Session Access“ (Zero Trust-Zugriff – Sitzungszugriff) innerhalb der Richtlinie „Adaptive Authentifizierung“ verwenden, um die Rollen oder Berechtigungen der jeweiligen Sitzung in Mobile zu reduzieren.

Zero Trust-Zugriff – Sitzungszugriff für Mobilgeräte kann aktiviert werden, indem **glide.authenticate.session_access.mobile.enabled** in der Tabelle „Systemeigenschaften“ aktiviert wird.

Um Zero Trust-Zugriff – Sitzungszugriff für Mobilgeräte mit den IdP-Attributen zu verwenden, können Sie das Feld **glide.authenticate.session_access.mobile.refresh_token_interval** konfigurieren. Dadurch können Administratoren den Sitzungszugriff basierend auf dem Aktualisierungstoken effektiv steuern.

Weitere Informationen finden Sie unter Configure Zero Trust Access for mobile .

Zero Trust-Zugriff wird aktiviert

Aktivieren Sie die **Richtlinie Zero Trust - Policy Based Session Access** com.snc.zero_trust_session_access, um Sicherheitsadministratoren das Reduzieren oder Beschränken des Benutzerzugriffs in einer Sitzung basierend auf IP-Adresse, Standort, Identitätsanbieterattributen und Benutzerattributen mithilfe von adaptiven Authentifizierungsrichtlinien zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin **„Zero Trust - Policy Based Session Access** “ (com.snc.zero_trust_session_access).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

Hinweis:
Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle „Sitzungszugriff“ konfigurieren

Konfigurieren Sie den Sitzungszugriff, um den Benutzerzugriff in einer Sitzung basierend auf IP, Standort, Identitätsanbieterattributen und Benutzerattributen mithilfe von adaptiven Authentifizierungsrichtlinien zu reduzieren.

Vorbereitungen

Erforderliche Rolle: security_admin

Hinweis:

- Sitzungszugriffskonfigurationen können nur mit der Rolle „ security_admin “ durchgeführt werden. Sie müssen Ihre Rolle auf security_adminerhöhen.
- Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Benutzer zugewiesen ist. In diesem Fall werden keine Änderungen an der angemeldeten Sitzung vorgenommen. Der Anwender greift weiterhin mit seinen zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, solange der Benutzer bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Benutzer muss sich von der Sitzung abmelden, damit die Richtlinie wirksam wird.
- Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu einer Einschränkung des Zugriffs. Wenn beispielsweise ein Benutzer nach dem Einrichten der Sitzung vom Unternehmensnetzwerk in ein nicht vertrauenswürdiges Netzwerk wechselt, wird der Zugriff nur eingeschränkt, wenn sich der Benutzer abmeldet und erneut anmeldet.

Prozedur

1. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**.
2. Um eine Rollenkonfiguration für den Sitzungszugriff zu erstellen, wählen Sie **Neu**.
3. Füllen Sie im Formular die folgenden Felder aus:

Konfiguration der Sitzungszugriffsrolle

Feld	Beschreibung
Name	Name der Konfiguration
Beschreibung	Kurzbeschreibung der Konfiguration.
Richtlinie	Wählen Sie die Richtlinie für die adaptive Authentifizierung aus. Verwenden Sie das Suchsymbol, um die Liste der Richtlinien anzuzeigen.
Aktion	**Rollen entfernen** oder **auf Rollen beschränken**. ○ **Rollen entfernen**: Wenn sich der konfigurierte Benutzer anmeldet, wird die Liste der in der Rollen- oder Gruppenliste angegebenen Rollen für die Sitzung entfernt. ○ **Auf Rollen beschränken**: Wenn sich der konfigurierte Benutzer anmeldet, werden

Automatische Übersetzung

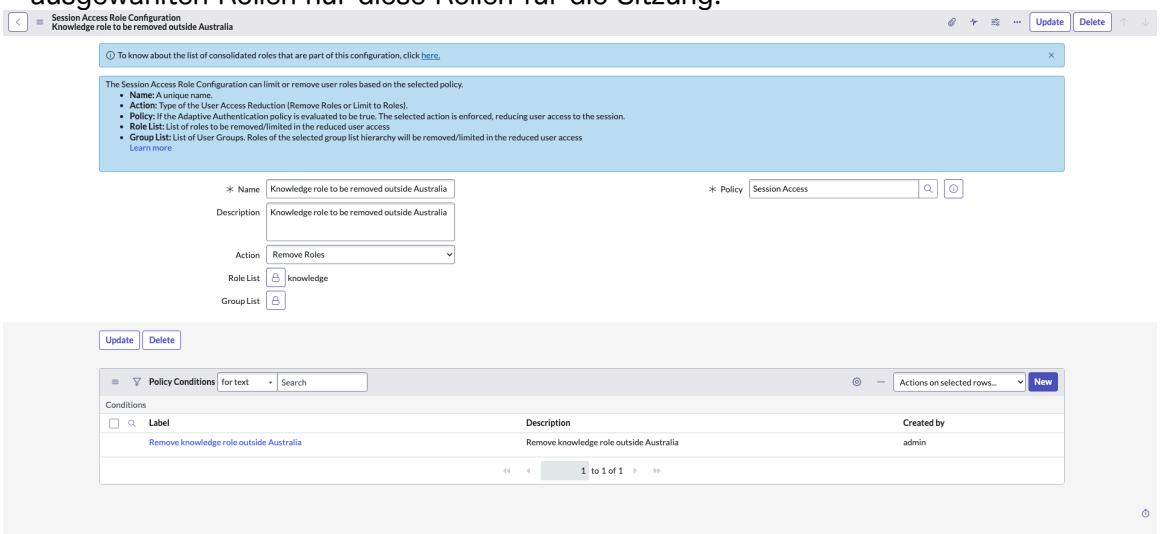
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	dem Benutzer nur die ausgewählten Rollen bereitgestellt, und alle anderen Rollen werden für die Sitzung entfernt.
Rollenliste	Wählen Sie Rollen aus der Rollenliste aus.
Gruppenliste	Wählen Sie die Rollen aus der Gruppenliste aus, die Sie entfernen oder auf den Benutzer beschränken möchten.

4. Wählen Sie, **Absenden**.

   Die Anmeldung für Benutzer basierend auf den konfigurierten Ländern lautet wie folgt:

   - In **Rollen entfernen**haben die Benutzer aus den konfigurierten Ländern mit den ausgewählten Rollen diese Rollen für die Sitzung nicht mehr.
   - In **Auf Rollen beschränken**haben die Benutzer aus den konfigurierten Ländern mit den ausgewählten Rollen nur diese Rollen für die Sitzung.



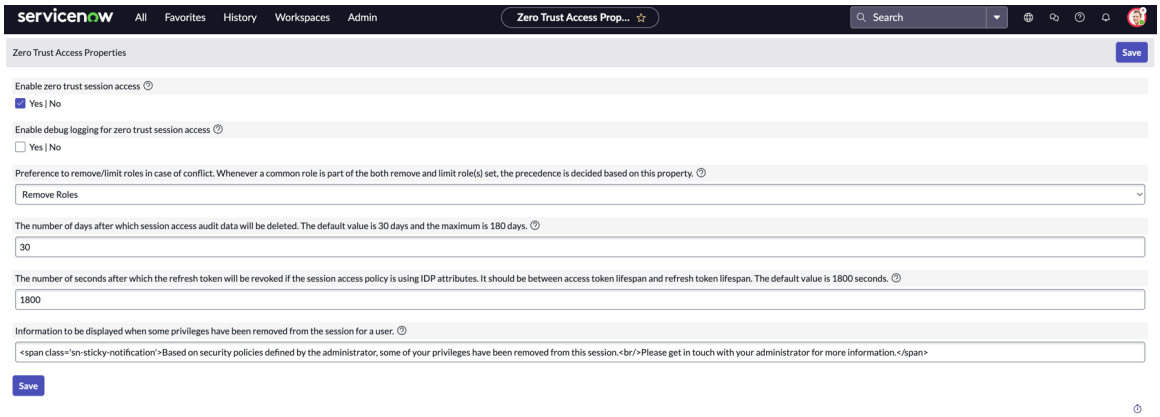
   Weitere Informationen zum Entfernen oder Einschränken von Rollen für eine Sitzung, die anhand eines Beispielanwendungsfalls erläutert wird, finden Sie unter Verwenden Sie Zero Trust-Zugriff.

Systemeigenschaften für Zero Trust-Zugriff

Verwenden Sie Systemeigenschaften, um den Zero Trust-Zugriff zu aktivieren und an Ihre Sicherheitsanforderungen anzupassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften



Systemeigenschaften für Zero Trust-Zugriff

Eigenschaft	Beschreibung
Aktivieren Sie Zero Trust-Sitzungszugriff	Option, mit der Administratoren die Funktion „Zero Trust-Sitzungszugriff“ verwenden können. Standardmäßig ist der Wert `false`.
Aktivieren Sie die Debug-Protokollierung für Zero Trust-Sitzungszugriff	Option zum Aktivieren der Debug-Protokollierung für Zero Trust-Sitzungszugriff.
Einstellung zum Entfernen/Einschränken von Rollen im Konfliktfall. Immer wenn eine allgemeine Rolle Teil der festgelegten Rolle(n) zum Entfernen und Begrenzen ist, wird die Rangfolge basierend auf dieser Eigenschaft festgelegt.	**Entfernen Sie Rollen,** oder **beschränken Sie Rollen**
Die Anzahl der Tage, nach denen Audit-Daten zum Sitzungszugriff gelöscht werden. Der Standardwert beträgt 30 Tage, der Höchstwert 180 Tage.	Standardmäßig sind es 30 Tage.
Die Anzahl der Sekunden, nach denen das Aktualisierungstoken widerrufen wird, wenn die Sitzungszugriffsrichtlinie IdP-Attribute verwendet. Sie muss zwischen der Lebensdauer des Zugriffstokens und der Lebensdauer des Aktualisierungstokens liegen. Der Standardwert beträgt 1800 Sekunden.	Standardmäßig sind es 1800 Sekunden.
Informationen, die angezeigt werden sollen, wenn für einen Benutzer einige Berechtigungen aus der Sitzung entfernt wurden.	Beschreibung, die Sie Ihren Benutzern in Bezug auf die Einschränkung oder den Entzug von Berechtigungen anzeigen möchten. Beispielbeschreibung: `Basierend auf den vom Administrator definierten Sicherheitsrichtlinien wurden einige Ihrer Rollen aus dieser Sitzung entfernt. Wenden Sie sich an Ihren Administrator, um weitere Informationen zu erhalten.`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

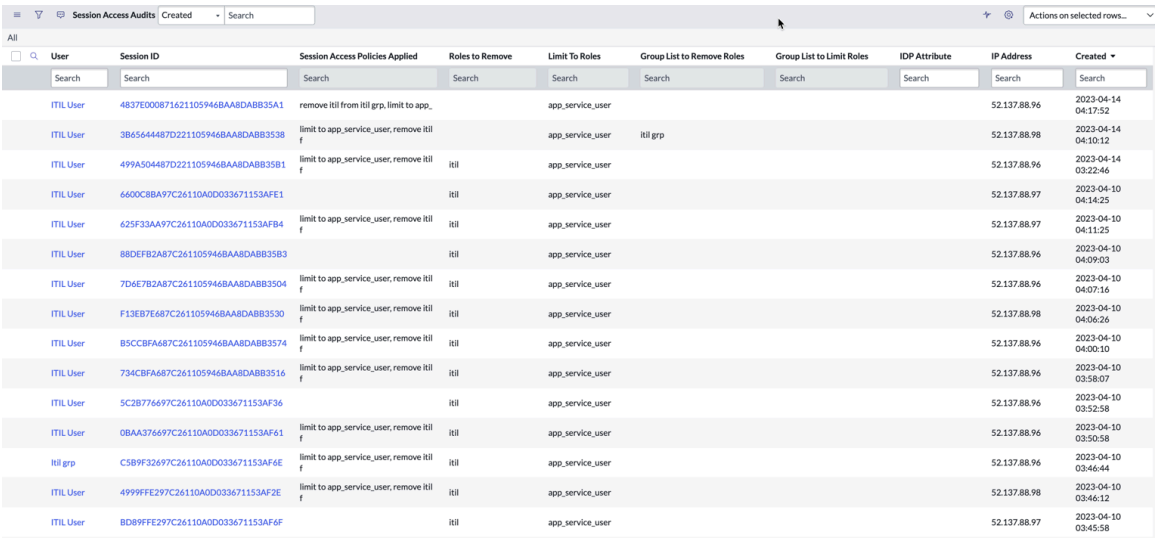
Audits des Sitzungszugriffs

Die Sitzungszugriffsaudits zeigen die Sitzungszugriffsprotokolle und Informationen zur Sitzung eines Benutzers an.

Audits

Das Audit „Sitzungszugriff“ zeigt Audit-Informationen wie folgt an:

Hinweis:
Verwenden Sie die Eigenschaft glide.authenticate.session_access.log_audit_event, um die Audit-Informationen auszufüllen.



Audits des Sitzungszugriffs

Feld	Beschreibung
Benutzer	Details des Benutzers.
Sitzungs-ID	Details zur Sitzung, die als eindeutige ID angezeigt werden.
Mobile-Client	Die Mobile-Client-Details. **ServiceNow Agent** (Now Agent) und **ServiceNow Request** (Now Mobile).
Sitzungszugriffsrichtlinien angewendet	Die angewendete Sitzungszugriffsrichtlinie.
Zu entfernende Rollen	Rollen, die dem Benutzer während der Protokollierung entzogen wurden.
Auf Rollen beschränken	Rollen, die bei der Protokollierung auf den Benutzer beschränkt waren.
Gruppenliste zur Entfernung von Rollen	Informationen über die Gruppe, die Rollen für den Benutzer entfernt hat.
Gruppenliste zur Beschränkung von Rollen	Informationen über die Gruppe, die über eingeschränkte Rollen für den Benutzer verfügt.
Mobile-Client	Details des über ein Mobilgerät angemeldeten Benutzers mit eingeschränktem oder entferntem Zugriff.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audits des Sitzungszugriffs (Fortsetzung)

Feld	Beschreibung
IDP-Attribut	Der IDP, der für diese Sitzung verwendet wurde
IP-Adresse	Details der IP-Adresse, die vom Benutzer für die Anmeldung verwendet wird.
Erstellt	Details zu Datum und Uhrzeit des erstellten Benutzerdatensatzes.

Verwenden Sie Zero Trust-Zugriff

Verwenden Sie die Zero Trust-Zugriffsfunktion mit einem End-to-End-Anwendungsfall.

Vorbereitungen
Erforderliche Rolle: security_admin

Aktivieren Sie die **Eigenschaft Sitzungszugriff aktivieren**.

Hinweis:

- Sitzungszugriffskonfigurationen können nur mit der Rolle „ security_admin “ durchgeführt werden. Sie müssen Ihre Rolle auf security_adminerhöhen.
- Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Benutzer zugewiesen ist. In diesem Fall werden keine Änderungen an der angemeldeten Sitzung vorgenommen. Der Anwender greift weiterhin mit seinen zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, solange der Benutzer bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Benutzer muss sich von der Sitzung abmelden, damit die Richtlinie wirksam wird.
- Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu einer Einschränkung des Zugriffs. Wenn beispielsweise ein Benutzer nach dem Einrichten der Sitzung vom Unternehmensnetzwerk in ein nicht vertrauenswürdiges Netzwerk wechselt, wird der Zugriff nur eingeschränkt, wenn sich der Benutzer abmeldet und erneut anmeldet.

Sitzungszugriff ist eine Funktion, mit der Administratoren dynamisch einen Satz von Rollen für den Benutzer reduzieren oder beschränken können, wenn der Benutzer versucht, sich aus verschiedenen Umgebungen bei der Instanz anzumelden, z. B. aus einem nicht vertrauenswürdigen Netzwerk oder von einem anderen -Gerät usw.

Der Sitzungszugriff kann durch die erstellte Richtlinie und die ausgewählte Aktion bei der Konfiguration gesteuert werden. Einige der Szenarien sind:

- Wenn die Richtlinie auf true festgelegt ist und die **Rollenaktion auf Rollen entfernen**festgelegt ist, werden die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Benutzer entfernt, wenn er versucht, sich bei der Instanz anzumelden.
- Wenn die Richtlinie auf true festgelegt ist und die **Rollenaktion auf Auf Rollen beschränken**festgelegt ist, werden dem Benutzer nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen zugewiesen, wenn er versucht, sich bei der Instanz anzumelden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im folgenden Verfahren wird eine End-to-End-Konfiguration der Sitzungszugriffskonfiguration erläutert, in der die Rolle auf den Benutzer beschränkt ist, der sich bei der Instanz anmeldet. Ebenso können Sie Rollen entfernen, indem Sie während der Konfiguration die Option **Rollen** entfernen auswählen.

Prozedur

1. Navigieren zu **Alle** > **Sitzungszugriff** > **Konfigurationen der Sitzungszugriffsrolle**.
2. Wählen Sie auf der Seite „Konfigurationen der Sitzungszugriffsrolle“ die Option **Neu**aus.
3. Um eine Rolle für den Benutzer einzuschränken, füllen Sie im Formular die folgenden Felder aus:
   - Name
   - Beschreibung
   - Richtlinie
   - Aktion
   - Rollenliste
   - Gruppenliste

   a. Wählen Sie **Auf Rollen** beschränken aus, um die Rollen für den Benutzer zu beschränken. Beispiel: **itil**.

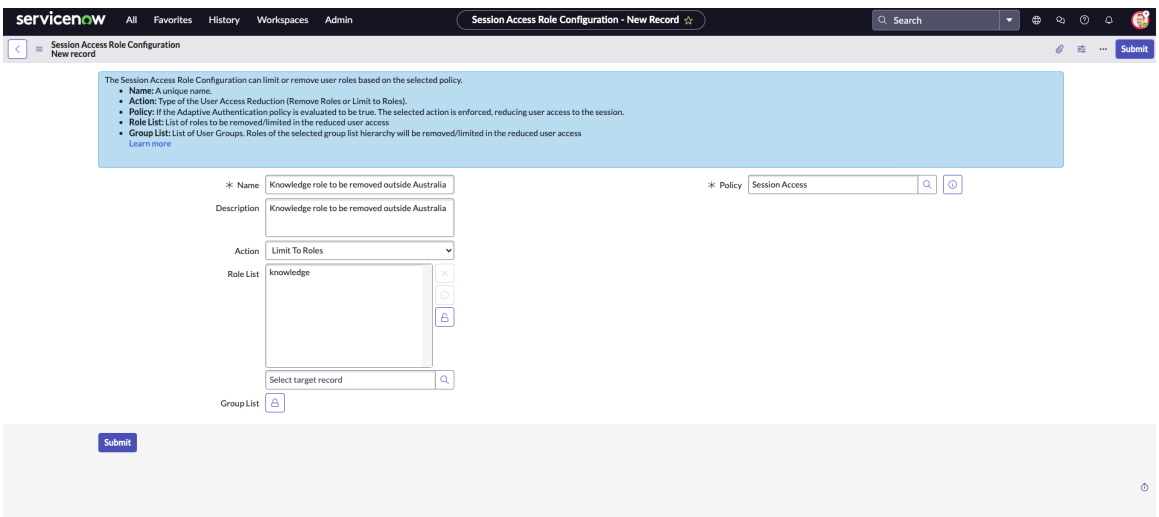
   b. Wählen Sie die **Wissensrolle** aus der Rollenliste aus.

   c. Wählen Sie die **Richtlinie**aus.

   Sie können die Sitzungszugriffsrichtlinie mithilfe von Authentifizierungsrichtlinien und Filterkriterien (Rolle, Gruppe, IP, Standort) mit Richtlinieneingaben und Bedingungen erstellen.

   Verwenden Sie die Richtlinie in der Konfiguration des Sitzungszugriffs. Beispiel: Sie möchten die Rolle (Wissen) auf den Benutzer beschränken, der sich außerhalb des Standorts (Australien) anmeldet.

   d. Wählen Sie Aktion als **Auf Rollen beschränken**.
   Wenn die Richtlinie auf true festgelegt ist, sind nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Benutzer verfügbar, wenn er versucht, sich bei der Instanz anzumelden.



Automatische Übersetzung

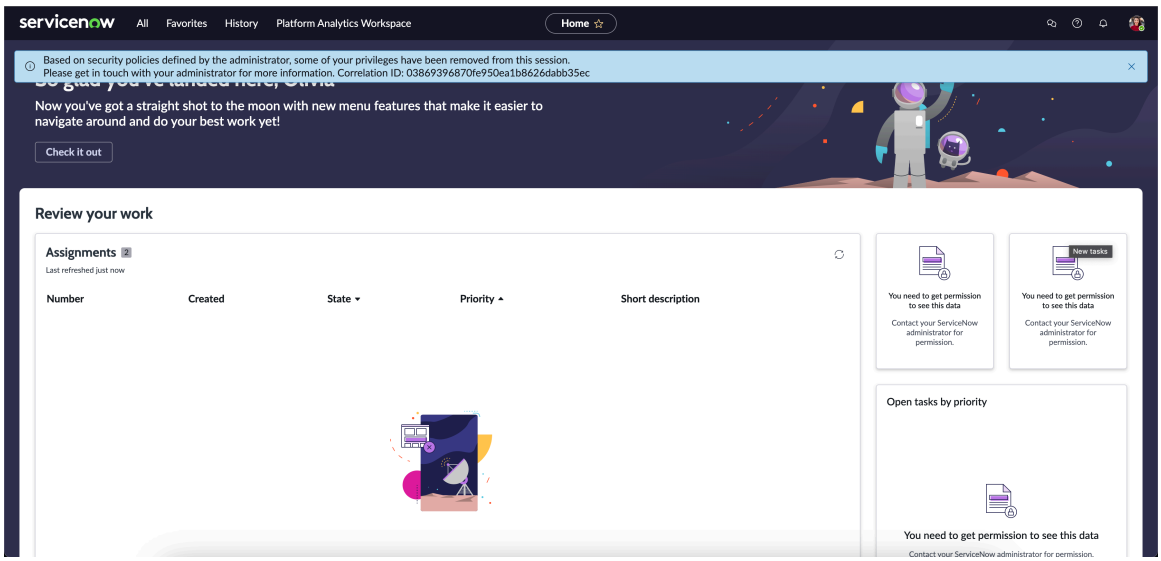
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Wählen Sie **Absenden**.

Ebenso können Sie die Gruppe aus der Gruppenliste auswählen, um Rollen für die Benutzer innerhalb der Gruppe einzuschränken oder zu entfernen.

Wenn sich der Benutzer bei der Instanz außerhalb von Australien anmeldet, werden nur die **Wissensrolle** und die zugehörigen untergeordneten Rollen für die protokollierte Sitzung zugewiesen, und andere Rollen für den Benutzer sind eingeschränkt.

Nach der Anmeldung wird dem Benutzer in seinem Profilabschnitt die folgende Fehlermeldung auf der Plattform angezeigt:



Der Benutzer kann sich an die Administratoren wenden und die Korrelations-ID zur Untersuchung angeben.

Hinweis:
Die Korrelations-ID ist die sys_id des entsprechenden Audit-Datensatzes in der Audit-Tabelle des Sitzungszugriffs.

Konfigurieren Sie das IdP-Attribut für den Sitzungszugriff

Verwenden Sie das IDP-Attribut (Identitätsanbieter), das aus der SAML-Antwort (Security Assertion Markup Language) erstellt wurde, um den Benutzersitzungszugriff auf die Instanz zu entfernen oder einzuschränken.

Vorbereitungen
Erforderliche Rolle: security_admin

Aktivieren Sie die **Eigenschaft Sitzungszugriff aktivieren**.

Hinweis:
Um die Rollenkonfiguration „Sitzungszugriff“ zu verwenden, müssen Sie Ihre Rolle auf `security_admin`erhöhen.

Der Sitzungszugriff kann durch die erstellte Richtlinie und die ausgewählte Aktion bei der Konfiguration gesteuert werden. Einige der Szenarien sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Richtlinie auf „Wahr“ festgelegt ist und die **Rollenaktion** zusammen mit der IDP-Attributeingabe und -bedingung auf Rollen entfernen festgelegt ist, werden die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Benutzer entfernt, wenn er versucht, sich bei der Instanz anzumelden.
- Wenn die Richtlinie auf „wahr“ festgelegt ist und die **Rollenaktion** zusammen mit der IDP-Attributeingabe und -bedingung auf Auf Rollen beschränken festgelegt ist, werden dem Benutzer beim Versuch, sich bei der Instanz anzumelden, nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen zugewiesen.

Das folgende Verfahren zeigt Schritte zum Konfigurieren des IDP-Attributs aus der SAML-Antwort für eine Richtlinieneingabe zur Steuerung des Sitzungszugriffs.

Prozedur

1. Navigieren zu **Alle** > **Sitzungszugriff** > **Konfigurationen der Sitzungszugriffsrolle**.
2. Wählen Sie auf der Seite „Konfigurationen der Sitzungszugriffsrolle“ die Option **Neu**aus.
3. Um eine Rolle für den Benutzer zu entfernen, füllen Sie im Formular die folgenden Felder aus:
   - Name
   - Beschreibung
   - Richtlinie
   - Aktion
   - Rollenliste
   - Gruppenliste

   a. Wählen **Sie Rollen** entfernen aus, um Rollen für den Benutzer zu entfernen.
   Beispiel: **itil**.

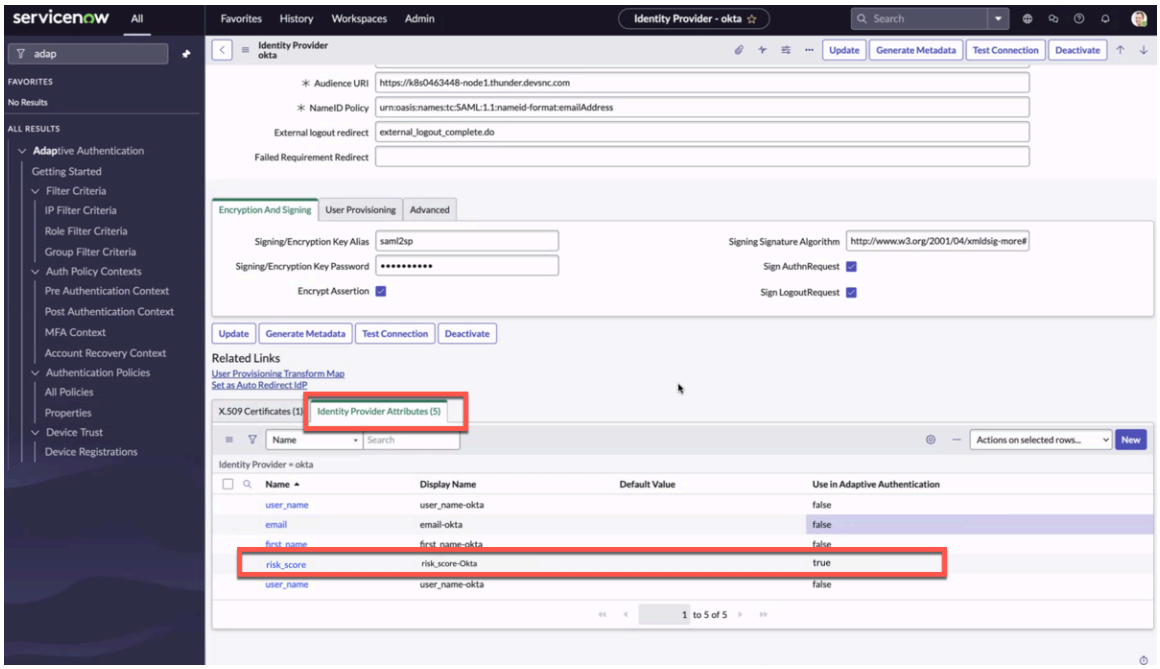
   b. Wählen Sie die **itil-** Rolle aus der Rollenliste aus.

   c. Wählen Sie die **Richtlinie**aus.
   Weitere Informationen zum Erstellen von Richtlinien mit verschiedenen Filterkriterien mithilfe der Richtlinienerstellung für die adaptive Authentifizierung finden Sie unter Filterkriterien.

   d. Wählen Sie Aktion als Rollen entfernen aus.
   Wenn die Richtlinie auf true festgelegt ist und die **Rollenaktion auf Rollen entfernen**festgelegt ist, werden die ausgewählten Rollen für den Benutzer entfernt, wenn er versucht, sich bei der Instanz anzumelden.

   e. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.
   Beispiel:
   - **Richtlinieneingabe**: Risikopunktzahlattribut von Okta (IDP).
   - **Policenbedingungen**: Risikopunktzahl von 60 bis 80 als Bedingung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn basierend auf dieser Konfiguration der Risikopunktzahl-Attributwert von Okta (IDP) 80 überschreitet, wird der Benutzer nicht mit den Rollen (**employee**) und den untergeordneten Rollen authentifiziert, die aus der Instanz entfernt wurden, sondern nur mit anderen Rollen zugewiesen. Wenn die Risikopunktzahl zwischen 60 und 80 liegt, wird der Benutzer bei der Instanz mit allen Rollen authentifiziert.

Weitere Informationen zum Erstellen der Richtlinie des Kontexts nach der Authentifizierung mit Richtlinieneingaben und Bedingung finden Sie unter Kontext nach der Authentifizierung.

Hinweis:
Wenn die Eigenschaft **Sitzungszugriff aktivieren** inaktiv ist, werden die Rollen des Benutzers durch die Konfiguration für Sitzungszugriff nicht eingeschränkt oder entfernt.

f. Wählen Sie **Absenden**.

Zero Trust-Zugriff für Mobilgeräte

Zero Trust Access (ZTA) ist ein Sicherheitsmodell, bei dem davon ausgegangen wird, dass standardmäßig keinem Benutzer oder Gerät vertraut wird.

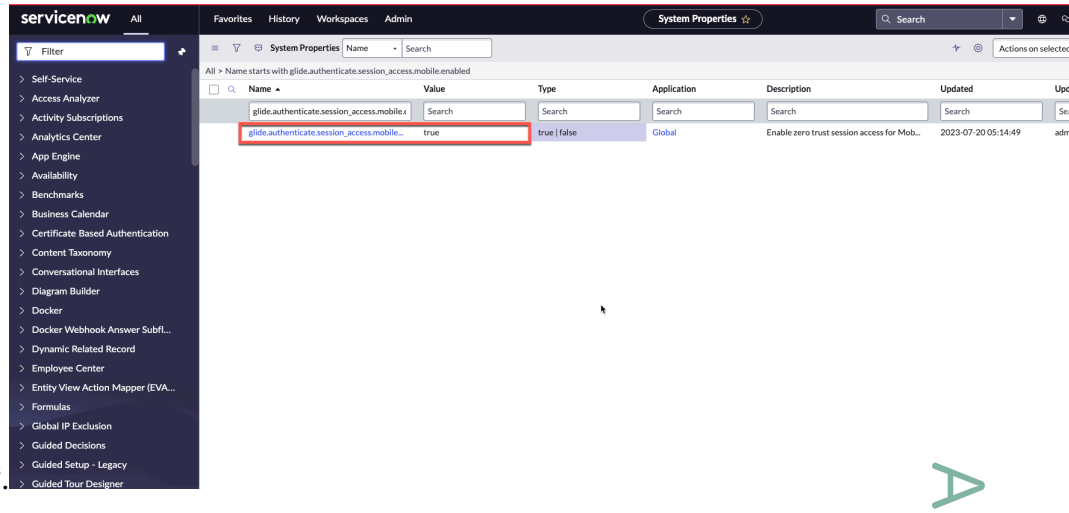
Sie können die Richtlinie „Zero Trust Access – Session Access“ (Zero Trust-Zugriff – Sitzungszugriff) innerhalb der Richtlinie „Adaptive Authentifizierung“ verwenden, um die Rollen oder Berechtigungen der jeweiligen Sitzung in Mobile für -Benutzer zu reduzieren.

Um Zero Trust-Zugriff auf Mobilgeräten zu aktivieren, müssen Sie die folgenden Aufgaben ausführen:

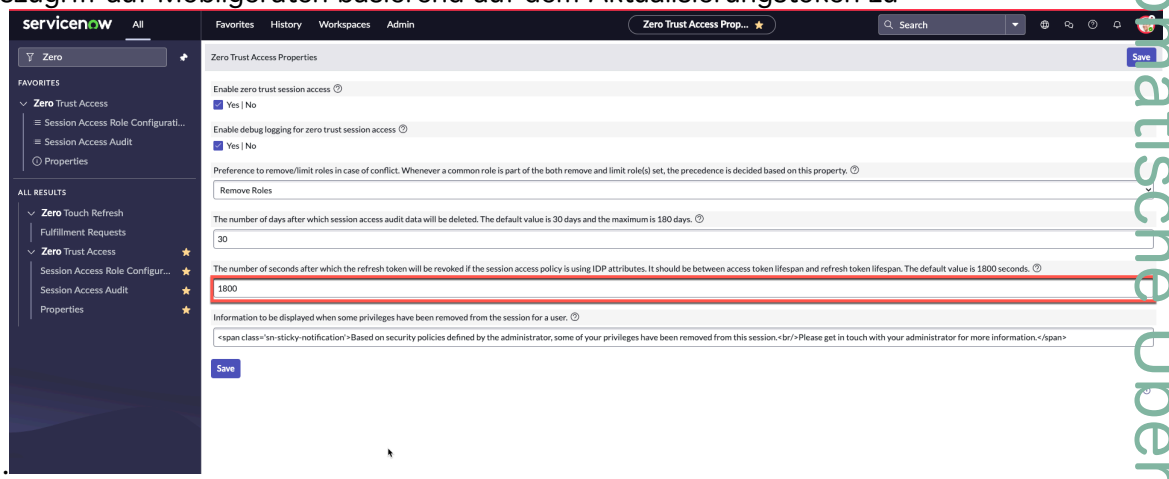
- Sitzungszugriffskonfigurationen können nur mit der Rolle „ `security_admin` “ durchgeführt werden. Sie müssen Ihre Rolle auf `security_admin`erhöhen.
- Aktivieren Sie die **Richtlinie Zero Trust - Policy Based Session Access** `com.snc.zero_trust_session_access`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Aktivieren Sie glide.authenticate.session_access.mobile.enabled** aus der Tabelle „Systemeigenschaften“.



- Konfigurieren Sie das Feld **glide.authenticate.session_access.mobile.refresh_token_interval**, um den Sitzungszugriff auf Mobilgeräten basierend auf dem Aktualisierungstoken zu steuern.



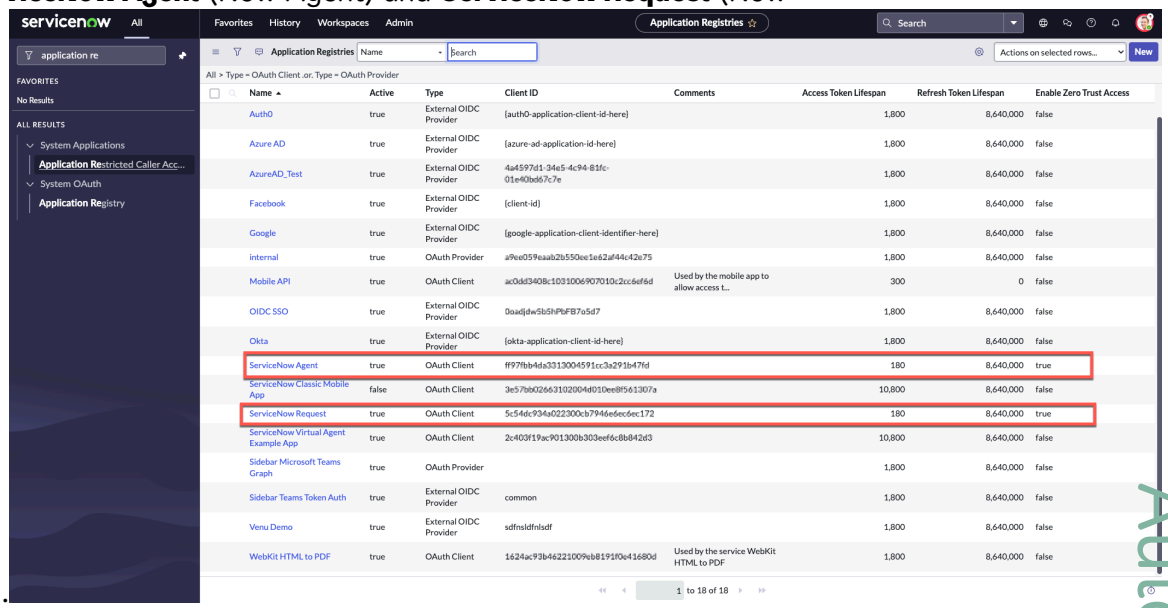
> **Hinweis:**
> Sie müssen die Sekunden des Aktualisierungstokens konfigurieren, wenn Sie einen IDP für Mobile-App-Anmeldungen verwenden. Standardmäßig werden Benutzer nach 1800 Sekunden (30 Minuten) von den Mobile-Apps abgemeldet.

- Zero Trust-Zugriff aktivieren ist unter **Anwendungsregistrierungen** für die Mobile-Client-Anwendung (OAuth-Client) aktiviert. In diesem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall **ServiceNow Agent** (Now Agent) und **ServiceNow Request** (Now Mobile).



- Konfigurieren Sie die Rolle „Sitzungszugriff“, um Rollen für die Benutzer, die sich basierend auf den Richtlinieneingaben und -bedingungen protokollieren, zu reduzieren oder zu entfernen. Weitere Informationen zur Konfiguration finden Sie unter Rolle „Sitzungszugriff“ konfigurieren.

Die Konfiguration wertet die Anmeldung aus, um die Rollen der Benutzer, die auf Ihre ServiceNow® -Instanz zugreifen, basierend auf den Richtlinienfiltern und -bedingungen zu reduzieren oder zu entfernen. Weitere Informationen finden Sie unter Configure Zero Trust Access for mobile .

Verbindung und Anmeldeinformationen

Anmelde- und Verbindungsinformationen sind erforderlich, um auf einen Computer oder ein Netzwerkgerät für Discovery, Service-Mapping und Cloud-Management zuzugreifen oder um mit Orchestration zu arbeiten. Beim Hinzufügen von Inhalten zu Share oder App-Store können Sie für Ihre Umgebung relevante Verbindungen und Anmeldeinformationen konfigurieren, ohne den integrierten Inhalt zu ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden

Erfahren Sie mehr über -Anmeldeinformationen.

Konfigurieren

Konfigurieren Sie Anmeldeinformationen.

Referenz

Ruft Details zu -Anmeldeinformationen ab.

Problembehandlung

Erfahren Sie, wie Sie Probleme mit Verbindungen und Anmeldeinformationen beheben können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durchsuchen von Anmeldeinformationen, Verbindungen und Aliassen

Alle Anwendungsintegrationen in Now Platform verwenden Verbindungen, Anmeldeinformationen und Aliasse von , um Anwendungen den Zugriff auf -Ressourcen zu ermöglichen.

Bevor Sie eine Anwendungsintegration in Now Platformausführen können, müssen Sie Verbindungsinformationen und entsprechende Anmeldeinformationen erstellen und konfigurieren und einen Alias hinzufügen. Um zu verstehen, wie ServiceNow diese Begriffe definiert:

Verbindung

Eine *Verbindung* ist eine Integration mit einem System, z. B. eine IP-Adresse oder ein Endpunkt mit Protokollen. Bei der Integration in eine Datenbank enthalten sie bestimmte Daten, z. B. Angaben zur Datenbank.

Anmeldeinformationen

Anmeldeinformationen sind die Authentifizierungsdaten, die zum Herstellen der Verbindung erforderlich sind, z. B. eine ID und ein Passwort.

Alias

Ein *Alias* ist eine Namenskonvention oder ein Tag, das an eine Reihe von Verbindungen oder Anmeldeinformationen in Ihrer Instanz gebunden ist. Ein Alias enthält die erforderlichen Verbindungs- und Anmeldeinformationen für eine Anwendungsintegration. Anstatt diese Informationen bei jeder Integration einzugeben, können Sie einen Alias verwenden. Sie können beispielsweise einen Alias festlegen, um Ihre QA-, Entwicklungs- und Produktions-Anmeldeinformationen für dieselbe Anwendungsintegration zu speichern. Der Alias löst die Anwendungsintegration für jede Umgebung auf.

Now Platform unterscheidet verschiedene Arten von Aliassen:

Anmeldeinformationsalias

Dieser Alias wird nur Anmeldeinformationsdaten zugeordnet und zur Laufzeit aufgelöst.

Ungültiger Alias für Verbindungen und Anmeldeinformationen

Dieser Alias wird den Verbindungsinformationen und den Anmeldeinformationen zugeordnet, die zum Abschließen der Integration erforderlich sind, und zur Laufzeit aufgelöst.

Innerhalb von Aliassen für Verbindungen und Anmeldeinformationen können Sie auch zusätzliche Aliasse erstellen, die als *untergeordnete Aliasse*bezeichnet werden. Mit untergeordneten Aliassen können Sie mehrere Verbindungen innerhalb derselben Anwendungsintegration erstellen. Wenn Sie einen untergeordneten Alias erstellen, wird der Alias, unter dem Sie ihn erstellt haben, zum *übergeordneten Alias*. Während untergeordnete Aliasse Eigenschaften von ihrem übergeordneten Alias erben, enthalten untergeordnete Aliasse ihre eigenen Verbindungs- und Anmeldeinformationen.

Vorteile der Verwendung von Verbindungen, Anmeldeinformationen und Aliassen

- Zentraler Ort zum Speichern und Verwalten von Anmeldeinformationen für einen externen Service
- Einmal definieren und für mehrere Plattformfunktionen wiederverwenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Minimieren Sie die Konfiguration anderer Plattformfunktionen
- Ermöglichen Sie Nicht-Administratoren die Verwendung vordefinierter Verbindungen und Anmeldeinformationen
- Erhöhte Sicherheit

Funktionen mit Verbindungen, Anmeldeinformationen und Aliassen

Die folgenden -Funktionen verwenden Verbindungen, Anmeldeinformationen und Aliasse:

- Flow Designer
- IntegrationHub
- Cloud-Management
- Discovery
- Orchestration
- Service-Mapping

Sie können Aliasse für Now Platform auf eine von zwei Arten einrichten:

- Verwenden des Moduls Verbindungen und Anmeldeinformationen Weitere Informationen finden Sie unter Verbindungs- und Anmeldealias erstellen.
- Im Dashboard „Verbindungen“ von IntegrationHub. Weitere Informationen finden Sie unter Verbindungen hinzufügen .

Hinweis:
IntegrationHub erfordert ein separates Abonnement. Weitere Informationen finden Sie unter Anforderung IntegrationHub .

Synchronisierung der Anmeldeinformationen auf MID Servern

Jeder *MID Server*in Ihrem Netzwerk, der mit der -Instanz synchronisiert wird, speichert eine Kopie aller von Ihnen erstellten Anmeldeinformationen. Der MID Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die die Kommunikation und die Bewegung von Daten zwischen einer ServiceNow-Instanz und externen Anwendungen, Datenquellen und Services ermöglicht. Diese Synchronisierung beschleunigt das Lesen von Anmeldeinformationen, wenn Anwendungen wie Discovery oder Service-Mapping im Netzwerk auf mehrere Geräte zugreifen müssen. Die MID Server führen eine Synchronisierung durch, wenn sie einen `credentials_reload`-Auftrag in der ECC-Warteschlange finden. Der Auftrag zum Neuladen weist den MID Server an, einen SOAP-Aufruf an die Instanz auszuführen, um die gesamte Liste der Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [discovery_credentials] einschließlich aller Feldwerte abzurufen. Weitere Informationen finden Sie unter MID Server .

Die SOAP-Antwort, die Ihre Instanz an die einzelnen MID Server sendet, enthält auch benutzerdefinierte Felder, die Sie von Ihnen angepassten Formularen für Anmeldeinformationen hinzugefügt haben. Wenn Sie Referenzfelder hinzugefügt haben, werden die Daten in der referenzierten Tabelle ebenfalls als Teil der SOAP-Antwort gesendet. Dies kann zu Leistungsproblemen führen, wenn die Anmeldeinformationen mit mehreren MID Servern synchronisiert werden. Dieses Problem können Sie am besten in den Griff bekommen, wenn Sie der Tabelle „Systemeigenschaften“ [sys_properties] folgende Eigenschaften manuell hinzufügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Um die Werte in diesen Eigenschaften zu ändern, fügen Sie sie der Tabelle „Systemeigenschaften“ [sys_properties] hinzu. Wenn Sie sie nicht hinzufügen, verwendet das System den Standardwert.

Eigenschaft	Beschreibung
com.snc.credentials_user_fields	Schließt alle benutzerdefinierten Felder in die Synchronisierung der Anmeldeinformationen ein. Legen Sie diese Eigenschaft auf „false“ fest, wenn Sie die Felder, die Sie den Anmeldeinformationsformularen hinzugefügt haben, nicht einbeziehen möchten. • **Typ**: true | false • **Standardwert**: true
com.snc.credentials_recursion_depth	Definiert die Anzahl der Tabellen, die durchlaufen werden sollen, wenn der Anmeldeinformationssynchronisierungsmechanismus Felder aus Referenztabellen erfasst. Verringern Sie diese Anzahl, wenn Leistungsprobleme auftreten und Sie über angepasste Formulare für Anmeldeinformationen verfügen, die Referenzfelder für Tabellen enthalten, die ebenfalls Referenzfelder enthalten. • **Typ**: Ganzzahl • **Standardwert**: 3

Bereichsschutz für Anmeldeinformationen und Verbindungen

Sie können bestimmte Typen von Verbindungs- und Anmeldeinformationsdatensätzen als zu einem Bereich gehörend klassifizieren und den Schutz des Bereichs darauf erweitern. Diese Bereichsrichtlinien dienen dem Schutz von Datensätzen, die Sie in einer Tabelle erstellen, und verhindern Interaktionen mit Datensätzen, die für einen anderen Bereich privat sind.

Ein **Anwendungsfeld** ist in den Tabellen „Verbindung“ [sys_connection] und „Discovery-Anmeldeinformationen“ [discovery_credentials] verfügbar, um diese Datensatztypen bestimmten Bereichen zuzuordnen. Sie ist in UI-Formularen in Washington DCnicht sichtbar, Sie können sie jedoch problemlos hinzufügen. Weitere Informationen zu diesen Datensatztypen und zum Hinzufügen des Felds zu ihren UI-Formularen finden Sie unter:

- Erste Schritte mit Verbindungen
- Erste Schritte mit Anmeldeinformationen
- Anmeldeinformationsaliasse für Discovery
- Formularlayout konfigurieren

Die Beschränkung der Verwendung eines Verbindungs- und Anmeldeinformationsdatensatzes auf einen bestimmten Bereich ist wichtig für die Verwaltung von Anwendungen, die erzwungene Sicherheit erfordern. Zu diesen Anwendungen gehören HR Service Delivery oder Security Operations Verbindungs- und Anmeldeinformationsdatensätze, die in bereichsbezogenen verwalteten Anwendungen erstellt werden, sind für Administratoren nicht sichtbar. Die Zuordnung eines Verbindungs- und Anmeldeinformationsdatensatzes zu einem bestimmten Anwendungsbereich bietet den folgenden Schutz:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wendet Zugriffskontrolllistenregeln (ACLs) auf eingeschränkte Bereiche an. Weitere Informationen zu bereichsbezogenen ACLs finden Sie unter Zugriffskontrolllistenregeln.

Hinweis:
Einige Anwendungen mit Bereichsverwaltung und erzwungener Sicherheit erfordern möglicherweise ein zusätzliches Setup. Weitere Informationen finden Sie unter HR-Rollen verwalten

- Schützt Datensätze, wenn sie mit einem Skript abgefragt werden. Wenn Sie eine Abfrage aus dem globalen Bereich ausführen und sich der Verbindungs- und Anmeldeinformationsdatensatz in einem geschützten Bereich befindet, wird er nicht in der Abfrage angezeigt, es sei denn, Sie erhalten Zugriff darauf.

Sie können abfragebeschränkte Datensätze anpassen und Zugriff gewähren, indem Sie den eingeschränkten Aufruferzugriff verwenden. Weitere Informationen finden Sie unter Einstellungen für eingeschränkte Anruferzugriffsberechtigungen . Umfangsbeschränkungen gelten auch für alle untergeordneten Tabellen der Tabellen „Verbindung“ [sys_connection] und „Discovery-Anmeldeinformationen“ [discovery_credentials]. Leere Felder und andere Bereiche sind nicht eingeschränkt.

Hinweis:
Bereichsschutz ist nur für bestimmte gesicherte Bereiche aktiviert, um Verwirrung beim Einrichten neuer Datensätze zu vermeiden. Wenn jemand eine Verbindung in seinem bereichsbezogenen Anwendungsbereich herstellt, erfolgt keine automatische Bereichsbeschränkung.

Domänentrennung und Anmeldeinformationen und Verbindungen

Domänentrennung wird in Anmeldeinformationen und Verbindungen unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

Übersicht

Die Anmeldeinformationen sind an verschiedene ServiceNow-Funktionen gebunden, die auf Systeme außerhalb der Instanz zugreifen. Die Anmeldeinformationen folgen der Domain Separation, die an diejenige Funktion gebunden ist, welche die Anmeldeinformationen verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindungen sind protokollspezifische Informationen, die auf einen Zielhost außerhalb der Instanz verweisen. Eine Verbindung kann die Domäne angeben, um eine Aktivität auszuführen.

Funktionsweise der Domain Separation für Anmeldeinformationen und Verbindungen

Anmeldeinformationen greifen auf Ressourcen außerhalb der Instanz zu und werden von Discovery, Orchestration, verwendet. Service-Mapping, und Cloud Provisioning and Governance -Anwendungen. Diese Anmeldeinformationen sind nicht an eine bestimmte Domäne gebunden, sondern können an eine Anwendung gebunden sein und folgen dann der von der Anwendung verwendeten Domain Separation. Anmeldeinformationen können auch einem MID Server zugewiesen werden und dann der in der Konfiguration MID-Server angegebenen Domänentrennung folgen.

Verbindungen greifen auf einen Zielhost zu, der eine *JMS*-, *JDBC*-oder *HTTP(s)*-Verbindung verwendet. Sie können eine globale oder eine bestimmte Domäne angeben, zu der die Verbindung gehört.

Zugehörige Informationen

Domänentrennung für Service Provider

Konfigurationsvorlagen für Verbindungen und Anmeldeinformationen

Ermöglichen Sie Benutzern mit der Rolle „admin“ und „flow_designer“, Spoke-Integrationen mit Drittanbietersystemen über ein einzelnes, anpassbares Formular einzurichten.

Sie können beispielsweise eine OAuth-Integration einrichten, die einen OAuth-Provider registriert, ein Token generiert und Verbindungs- und Anmeldeinformationsdatensätze erstellt. Ein Aktionsdesigner oder -entwickler kann eine Konfigurationsvorlage verwenden, um die Spoke an einem Ort einzurichten, und das System erstellt die zugehörigen Datensätze.

Vorteile

Konfigurationsvorlagen ermöglichen Folgendes:

- Administratoren oder Flow Designer, um komplexe Integrationen mit einem einzigen Formular einzurichten.
- Entwickler können statische Werte in einer Integration festlegen, was den Setup-Prozess für Administratoren und Flow Designer vereinfacht.

Unterstützte Anmeldeinformationstypen

Sie können Konfigurationsvorlagen für Integrationen mit diesen Anmeldeinformationstypen erstellen:

- Standardauthentifizierung
- API Key
- OAuth JWT Bearer-Gewährungstyp
- Gewährungstyp des OAuth-Autorisierungscodes
- Benutzerdefinierte Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten der Konfigurationsvorlage

Standarddatenvorlage

Damit werden statische Informationen festgelegt, die für jede Integration gelten. Beispielsweise können Sie die API und die Token-URL festlegen, wenn der Wert für jede Integration gilt.

Dynamische Datenvorlage

Damit werden Informationen festgelegt, die der Benutzer zum Einrichten der Integration eingeben muss. Beispielsweise können Sie Schlüssel-Wert-Paare aus Benutzername und Passwort hinzufügen, um benutzerdefinierte Werte zu erfassen.

Nachbearbeitungsskript

Damit werden zusätzliche Datensätze erstellt, die für die Integration erforderlich sind. Wenn Ihre Spoke beispielsweise benutzerdefinierte Tabellen enthält, können Sie Datensätze in diesen Tabellen auf der Grundlage von Benutzereingaben in der Konfigurationsvorlage erstellen. Dieses Skript wird ausgeführt, nachdem die Verbindungs- und Anmeldeinformationsdatensätze erstellt wurden.

Skript vorab bearbeiten

Füllt die benutzerdefinierten Felder im Abschnitt „ **Zusätzliche Informationen** “ vorab aus, wenn Sie eine vorhandene Verbindung bearbeiten. Wenn Sie die benutzerdefinierten Felder vorab ausfüllen, können Sie den aktuellen Wert anzeigen, der dem benutzerdefinierten Feld zugeordnet ist.

Demodaten

Die Tabelle „Verbindungs- und Anmeldeinformationsvorlagen“ [sys_alias_templates] enthält Beispielvorlagen, die zeigen, wie Vorlagen für gängige Authentifizierungstypen eingerichtet werden. Verwenden Sie diese Beispiele als Leitfaden, wenn Sie eigene erstellen.

Konfigurieren Sie eine Vorlage für den Gewährungstyp OAuth JWT Bearer

Diese Beispielkonfigurationsvorlage richtet Anmeldeinformations- und Verbindungsdatensätze mit dem Gewährungstyp JWT Bearer ein, um Anforderungen bei DocuSign zu authentifizieren.

Standarddatenvorlage

Jedes Element der obersten Ebene in der Standarddatenvorlage erstellt einen zugeordneten Datensatz. Die Vorlage enthält die folgenden Abschnitte:

- `Anmeldeinformationen`: Erstellt einen Datensatz in der Tabelle „Anmeldeinformationen“.
- `Verbindung`: Erstellt einen Datensatz in der Tabelle „Verbindungen“ [sys_connection] und alle zugehörigen Verbindungsdatensätze.
- `Zusätzlich`: Erstellt optional Datensätze in einer benutzerdefinierten Tabelle. Das Nachverarbeitungsskript teilt dem System mit, was mit diesen Datensätzen geschehen soll.

Im folgenden Beispiel werden die für die OAuth JWT Bearer-Gewährungstypauthentifizierung erforderlichen Datensätze erstellt.

```
{
 "credential": {
  "oauth_entity": {
   "oauth_entity_profile": [
    {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
      "name": "Docusign Profile",
      "default": true,
      "oauth_entity_profile_scope": [
       "users:read.email"
      ]
     }
    ],
    "code_challenge_method": "S256",
    "type": "consumer",
    "oauth_entity_scope": [
     {
      "oauth_entity_scope": "users:read.email",
      "name": "email"
     }
    ],
    "client_id": "<provider-client-id>",
    "use_mutual_auth": false,
    "revoke_token_url": "https://<provider-domain-name>.com/oauth2/revoke",
    "default_grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
    "public_client": false,
    "oauth_api_script": "3e3a3a11c333210016194ffe5bba8f70",
    "name": "Docusign Spoke OAuth",
    "client_secret": "<provider-client-secret>",
    "auth_url": "https://<provider-domain-name>.com/oauth2/auth",
    "token_url": "https://<provider-domain-name>.com/oauth2/token",
    "redirect_url": "https://<instance-name>.service-now.com/oauth_redirect.do"
   },
   "jwt_provider": {
    "jwt_keystore_aliases": {
     "kid": "<provider-key-id>",
     "name": "Docusign Spoke JWT Key",
     "signing_keystore": "<signing-keystore-sys-id>",
     "signing_algorithm": "rsa_256",
     "signing_key_password": "password"
    },
    "jwt_claim_validation" : [ {
     "name" : "iss",
     "is_standard" : true,
     "data_type" : "string",
     "value":"<docusign-iss-claim>"
    }, {
     "name" : "sub",
     "is_standard" : true,
     "data_type" : "string",
     "value":"<docusign-sub-claim>"
    }, {
     "name" : "aud",
     "is_standard" : true,
     "data_type" : "string",
     "value":"<docusign-aud-claim>"
    }, {
     "name" : "scope",
     "is_standard" : false,
     "data_type" : "string",
     "value" : "signature impersonation"
    } ],
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    "name": "Docusign Spoke JWT Provider",
    "jwt_api_script": "9ef6af86ff10330001d3cd6bd53bf144"
   },
   "name": "Docusign Spoke Credential",
   "table": "oauth_2_0_credentials"
  },
  "connection": {
   "use_mid": false,
   "connection_url": "https://<provider-domain-name>.com",
   "name": "Docusign Spoke Connection",
   "table": "http_connection"
  },
"additional":{
   "docusign_account_name": "<docusign-account-name>",
   "docusign_account_email": "<docusign-account-email>"
}
}
```

Dynamisches Datenschema

Das dynamische Datenschema definiert, was der Benutzer sieht, wenn er einen Alias für Verbindungen und Anmeldeinformationen erstellt und seine Eingaben erfasst. Verwenden Sie die Dot-Walking-Syntax, um Benutzereingaben Feldern zuzuordnen, die in der Standarddatenvorlage erstellt wurden. Zum Beispiel ordnet `connection_fields` die Benutzereingabe dem Feld `connection_url` im `Verbindungsobjekt` zu, das von der Standarddatenvorlage erstellt wird.

```
{
  "connection_fields": [
    {
      "name": "connection.connection_url",
      "label": "Connection URL",
      "type": "text",
      "defaultValue": "https://demo.docusign.net",
      "hint": "Connection URL for Docusign"
    }],
"additional_fields":[
    {
      "name": "additional.docusign_account_id",
      "label": "Docusign Account Number",
      "type": "text",
      "hint": "Docusign Account Number"
    },
    {
      "name": "additional.docusign_account_name",
      "label": "Docusign Account Name",
      "type": "text",
      "hint": "Name to identify the Docusign account"
    },
    {
      "name": "additional.docusign_account_email",
      "label": "Docusign Account Email",
      "type": "text",
      "hint": "Docusign Account Email"
    }
  ],
  "credential_fields": [
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  {
    "name": "credential.oauth_entity.client_id",
    "label": "OAuth Client ID",
    "type": "text",
    "hint": "Client ID for Docusign"
  },
  {
    "name": "credential.oauth_entity.redirect_url",
    "label": "OAuth Redirect URL",
    "type": "text",
    "defaultValue": "https://<instance-name>.service-now.com/oauth_redirect.do",
    "hint": "Callback URL for Docusign"
  },
{
    "name": "credential.jwt_provider.jwt_claim_validation[0].value",
    "label": "Issuer (iss) Claim value",
    "type": "text",
    "hint": "The integrator key (also known as client ID) of the application"
  },
{
    "name": "credential.jwt_provider.jwt_claim_validation[1].value",
    "label": "Subject (sub) Claim value",
    "type": "text",
    "hint": "The user ID of the user to be impersonated"
  },
{
    "name": "credential.jwt_provider.jwt_claim_validation[2].value",
    "label": "Audience (aud) Claim value",
    "type": "text",
    "defaultValue": "account-d.docusign.com",
    "hint": "The URI of the authentication service instance to be used e.g.
account.docusign.com"
  },
  {
    "name": "credential.jwt_provider.jwt_keystore_aliases.kid",
    "label": "Key ID (kid)",
    "type": "text",
    "hint": "Indicates which key was used to secure the JWS"
  },
  {
    "name": "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
    "label": "Key Store",
    "type": "file"
  }
 ]
}
```

Nachbearbeitungsskript

Das folgende Nachverarbeitungsskript ordnet Benutzereingaben Feldern in der Tabelle sn_docusign_spoke_accounts zu.

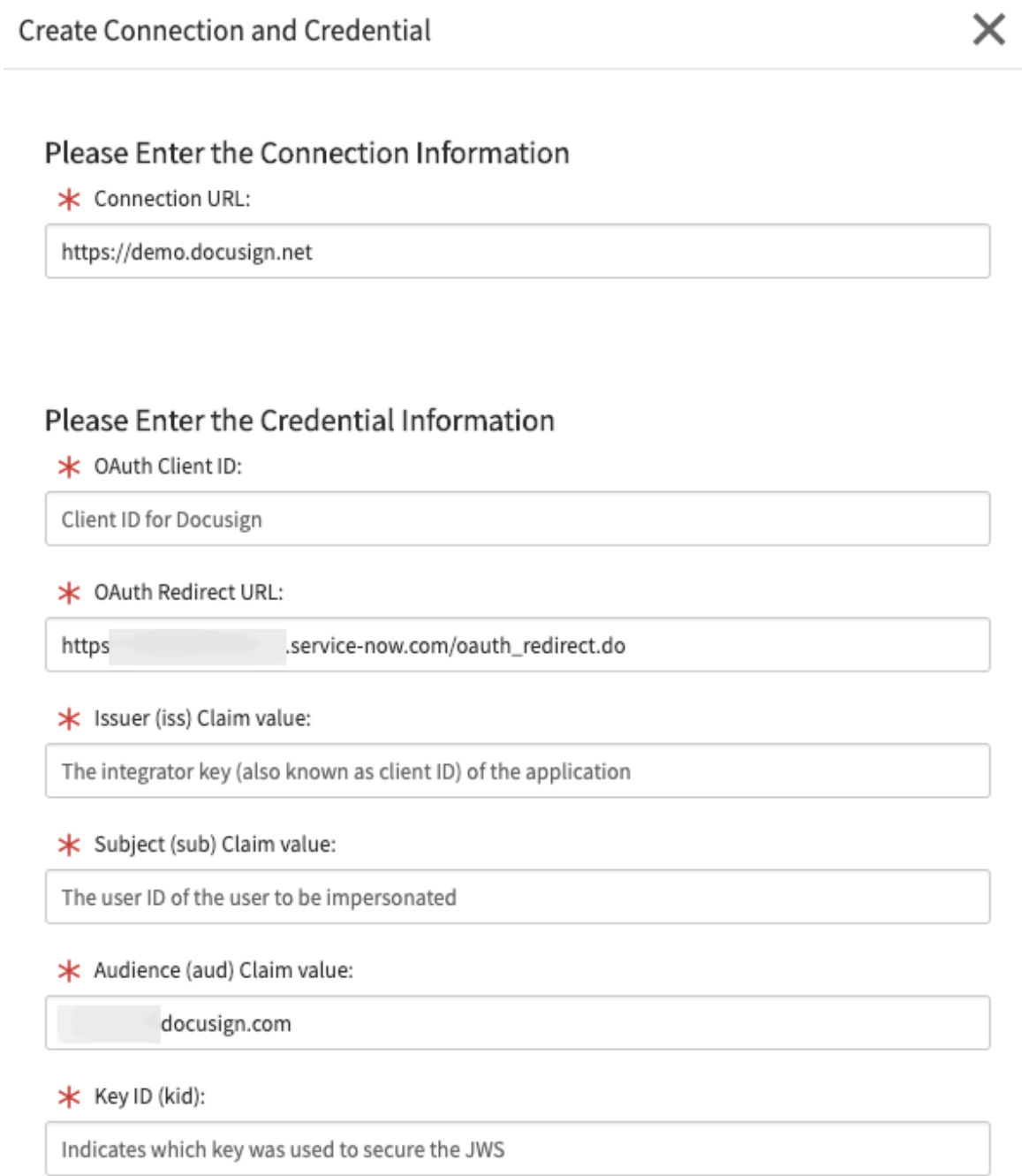
```
(function execute(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData) {
 var jsonDynamicDataP = JSON.parse(jsonDynamicData);
 var accountGR = new GlideRecord("sn_docusign_spoke_accounts");
   accountGR.setValue("account_name",
 jsonDynamicDataP["additional.docusign_account_name"]);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    accountGR.setValue("alias", aliasId);
    accountGR.setValue("email", jsonDynamicDataP["additional.docusign_account_email"]);
    accountGR.setValue("id", jsonDynamicDataP["additional.docusign_account_id"]);
    accountGR.insert();
})(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData);
```

Daraus resultierendes Konfigurationsformular für DocuSign-Verbindungen und -Anmeldeinformationen

Wenn der Benutzer zum zugeordneten DocuSign-Alias für Verbindungen und Anmeldeinformationen navigiert und **Neue Verbindung und Anmeldeinformationen erstellen**auswählt, wird das folgende Dialogfeld angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Konfigurationsvorlage

Erstellen Sie eine Vorlage, die die zum Einrichten einer Spoke erforderlichen Eingaben definiert. Legen Sie statische Schlüssel-Wert-Paare fest, um Datensätze zu erstellen und Werte festzulegen, die für jede Integration gelten. Legen Sie dynamische Schlüssel-Wert-Paare fest, um Benutzereingaben zu erfassen und Feldwerte festzulegen, die variieren können. Mit dieser Vorlage können Administratoren und Flow-Designer die Spoke über ein einziges Formular einrichten.

Vorbereitungen

Erforderliche Rolle: Aktionsdesigner oder Administrator

Prozedur

1. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Konfigurationsvorlagen**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie den Typ der Konfigurationsvorlage aus, die Sie erstellen möchten.
   Wenn Sie einen Typ auswählen, erhalten Sie Startdaten, die Sie beim Konfigurieren der Vorlage unterstützen.
4. Fügen Sie im Feld **Name** einen Namen hinzu, um die Vorlage zu identifizieren.
5. **Nehmen Sie im Feld Standarddatenvorlage** die erforderlichen Änderungen vor.
   In diesem Feld werden statische Informationen festgelegt, die für jede Integration gelten. Beispielsweise können Sie die API und die Token-URL festlegen, wenn der Wert für jede Integration gilt.

   Diese Objekte in der Standarddatenvorlage sind erforderlich:

   - `credential`: Erstellt einen Anmeldeinformationsdatensatz mit den erforderlichen Feldern.
   - `connection`: Erstellt einen Verbindungsdatensatz mit den erforderlichen Feldern. Greifen Sie mit dem untergeordneten Objekt „ `extended_attributes` “ auf Verbindungsattribute zu. Beispiel:

```
"connection": {
        "extended_attributes": {
           "api_version": "v1"

        },
     "connection_url": "https://<provider-domain-name>.com",
     "name": "Spoke Connection",
     "table": "http_connection"
  }
```

   Sie können das `zusätzliche` Objekt verwenden, um Daten für eine benutzerdefinierte Tabelle einzurichten, und das Nachverarbeitungsskript verwenden, um die Daten in die Tabelle einzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In der Standarddatenvorlage für den Gewährungstyp OAuth-Autorisierungscode müssen die Werte für die Schlüssel oauth_entity_profile_scope und oauth_entity_scope übereinstimmen. Im folgenden Beispiel haben beide Schlüssel den Wert E-Mail des Benutzers lesen.

```
"oauth_entity_profile": [
      {
        "grant_type": "authorization_code",
        "name": "<provider-name> Profile",
        "default": true,
        "oauth_entity_profile_scope": [
          "Read user's email"
        ]
      }
    ],
    "code_challenge_method": "S256",
    "type": "consumer",
    "oauth_entity_scope": [
      {
        "oauth_entity_scope": "Read user's email",
        "name": "email"
      }
    ],
```

6. **Nehmen Sie im Feld Dynamisches Datenschema** die erforderlichen Änderungen vor.
   Dieses Feld Damit werden Informationen festgelegt, die der Benutzer zum Einrichten der Integration eingeben muss. Beispielsweise können Sie Schlüssel-Wert-Paare aus Benutzername und Passwort hinzufügen, um benutzerdefinierte Werte zu erfassen.

   Felder im dynamischen Datenschema umfassen die folgenden Eigenschaften:

   - name: Das Feld, dem die Eingabe des Benutzers zugeordnet ist. Geben Sie beispielsweise connection.connection_url ein, um die Benutzereingabe dem Feld Verbindungs-URL im Verbindungsdatensatzzuzuordnen.
   - Bezeichnung: Die Feldbezeichnung, die dem Benutzer beim Ausfüllen der Vorlage angezeigt wird.
   - Typ: Der Feldtyp Stellen Sie sicher, dass dieser Datentyp mit dem Datentyp des Felds übereinstimmt, dem Sie den Wert zuordnen.
   - defaultValue: Optional. Der Standardwert des Felds. Wenn kein Standard angegeben ist, wird der Hinweis angezeigt.
   - Hinweis: Optional. Hinweistext, der angezeigt werden soll, wenn kein Standardwert vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie eine Vorlage für die Authentifizierung des Gewährungstyps OAuth JWT Bearer einrichten, möchten Sie möglicherweise eine Benutzereingabe für ein einzelnes Schlüssel-Wert-Paar im Array `jwt_claim_validation`. Sie können auf ein einzelnes Schlüssel-Wert-Paar im dynamischen Datenschema verweisen, indem Sie auf seinen Index im Array verweisen. Beispielsweise kann Ihre Standarddatenvorlage dieses Fragment enthalten.

```
"jwt_claim_validation" : [ {
      "name" : "iss",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-iss-claim>"
    }, {
      "name" : "sub",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-sub-claim>"
    }, {
      "name" : "aud",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-aud-claim>"
    }, {
      "name" : "scope",
      "is_standard" : false,
      "data_type" : "string",
      "value" : "signature impersonation"
    } ],
```

Verweisen Sie mit dem nullbasierten Index des Elements auf das `iss` -Schlüssel-Wert-Paar: `credential.jwt_provider.jwt_claim_validation[0].value`.

7. **Wahlweise:** **Fügen** Sie im Feld Nachverarbeitungsskript ein Skript hinzu, das Damit werden zusätzliche Datensätze erstellt, die für die Integration erforderlich sind. Wenn Ihre Spoke beispielsweise benutzerdefinierte Tabellen enthält, können Sie Datensätze in diesen Tabellen auf der Grundlage von Benutzereingaben in der Konfigurationsvorlage erstellen. Dieses Skript wird ausgeführt, nachdem die Verbindungs- und Anmeldeinformationsdatensätze erstellt wurden.enthält.
   Das Nachverarbeitungsskript hat Zugriff auf diese globalen Objekte.

Globales Objekt	Beschreibung
aliasId	Sys_id des Alias-Datensatzes aus der Tabelle „Alias für Verbindungen und Anmeldeinformationen“ [sys_alias].
connectionSysId	Sys_id des von der Vorlage erstellten Verbindungsdatensatzes.
jsonDefaultData	JSON-Inhalt aus dem Feld **Standarddatenvorlage** im Zeichenfolgenformat.
jsonDynamicData	JSON-Inhalt aus dem Feld **„Dynamische Datenvorlage“** im Zeichenfolgenformat.

8. **Fügen** Sie im Feld Vorbearbeitungsskript ein Skript hinzu, um die zusätzlichen Felder vorab auszufüllen, wenn Sie eine Verbindung bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Skript gibt ein Array von Objekten zurück. Jedes Objekt verfügt über ein Name-Wert-Paar zum Ausfüllen der zusätzlichen Felder. Wenn die Verbindung beispielsweise Felder erfordert, die sich in einer benutzerdefinierten Tabelle befinden, können Sie diese Felder der benutzerdefinierten Tabelle zuordnen.

Das **Vorbearbeitungsskript** hat Zugriff auf die folgenden globalen Objekte:

Globales Objekt	Beschreibung
aliasId	Sys_id des Alias-Datensatzes aus der Tabelle „Alias für Verbindungen und Anmeldeinformationen“ [sys_alias].
connectionSysId	Sys_id des von der Vorlage erstellten Verbindungsdatensatzes.
jsonDefaultData	JSON-Inhalt aus dem Feld **Standarddatenvorlage** im Zeichenfolgenformat.
jsonDynamicData	JSON-Inhalt aus dem Feld **„Dynamische Datenvorlage“** im Zeichenfolgenformat.

Jedes Objekt im Skript hat die folgenden Eigenschaften:

- `name`: Name des benutzerdefinierten Felds zur Angabe des Werts in der Verbindung.
- `value`: Wert, den Sie zuordnen möchten, um das benutzerdefinierte Feld auszufüllen. Sie können das Feld entweder mithilfe einer Funktion oder Variablen zuordnen oder es hartcodieren.

Die folgenden Datentypen werden für die Felder unterstützt:

Unterstützte Datentypen für die Felder

Typ	Beschreibung
Text	Zeichenfolgenwert.
Boolean	Auswahlfeld. Die Auswahl gibt den Wert „Wahr“ an, die Aufhebung der Auswahl den Wert „Falsch“.
Nummer	Numerischer Wert.
Datum	Datumswert im Format jjjj-mm-tt. Sie können auch das GlideDate-Objekt verwenden.
Auswahl	Liste der gültigen Auswahlmöglichkeiten, die im Feld **„Dynamisches Datenschema“ definiert**sind.
Referenz	Gültiger GlideRecord.
Auswahlgruppe	Gruppen, die einen anderen Satz von Feldern enthalten. Diese Gruppen sind als Auswahl in einer Dropdown-Liste verfügbar, wenn Sie eine Verbindung bearbeiten. Die Felder in jeder Gruppe werden angezeigt, wenn Sie die erforderliche Gruppe aus der Dropdown-Liste auswählen. Betrachten Sie beispielsweise die folgende Struktur der Auswahlgruppe, die im Feld **Dynamisches Datenschema definiert** ist: `{ "name": "radio_groups", "label": "Radio Groups", "type": "radio", "groups": [{`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung

	<pre>"name": "radio_group1",
	"label": "Radio Group 1",
	"fields": [{
	"name": "radio_field1",
	"label": "Radio Field 1",
	"type": "text",
	"defaultValue": "efgh",
	"mandatory": true
	}]
	}, {
	"name": "radio_group2",
	"label": "Radio Group 2",
	"fields": [{
	"name": "radio_field2",
	"label": "Radio Field 2",
	"type": "text",
	"defaultValue": "abcd",
	"mandatory": true
	}],
	"default_group": true
	}</pre>
	In diesem Beispiel können Sie das folgende Code-Fragment verwenden, um zu verstehen, wie Auswahlgruppen im Skript mithilfe von Dot-Walking verwendet werden:
	<pre>{
	name: "radio_field.first_radio_group.radio_field1",
	value: "radio field 1"
	}, {
	name:
	"radio_field.second_radio_group.radio_field2",
	value: "radio field 2"
	}, {
	name: “radio_groups”,
	value: gr.getValue(‘radio_groups’)
	}</pre>
	Weitere Informationen zur Verwendung von Dot-Walking finden Sie unter Dot-Walking .

Tipp:
Wenn die vorab ausgefüllten Werte beim Bearbeiten einer Verbindung nicht in den Feldern angezeigt werden, navigieren Sie zu **Systemdiagnostik** > **Sitzung debuggen** > **Protokoll debuggen** , um das Problem zu diagnostizieren.

9. Fügen Sie die Vorlage einem Alias für Verbindungen und Anmeldeinformationen hinzu.

a. Navigieren zu **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.

b. Öffnen Sie den Aliasdatensatz für die Spoke.

c. Klicken Sie im Feld **Konfigurationsvorlage** auf das Suchsymbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie die von Ihnen erstellte Vorlage aus der Liste aus.

e. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Wenn der Benutzer zum zugeordneten Alias für Verbindungen und Anmeldeinformationen navigiert und **Neue Verbindung und Anmeldeinformationen erstellen**auswählt, wird ein Dialogfeld angezeigt, um die Eingabe zu erfassen. Wenn Sie eine Vorlage für den Gewährungstyp OAuth-Autorisierungscode erstellt haben, können Sie in diesem Dialogfeld auch ein OAuth-Token abrufen.

Nächste Maßnahme

Testen Sie die Vorlage, indem Sie zum zugehörigen Alias für Verbindungen und Anmeldeinformationen navigieren und **Neue Verbindung und Anmeldeinformationen erstellen**auswählen. Stellen Sie sicher, dass der Dialog die erwarteten Daten erfasst und die erforderlichen Datensätze im System erstellt.

Erste Schritte mit Verbindungen

Verwenden Sie die Verbindungstabelle, um eine Basic-, JMS-, JDBC- oder HTTP(s)-Verbindung zu einem Zielhost einzurichten.

Verbindungstabelle

Die Tabelle „Verbindung“ (sys_connection) ist die Basistabelle für alle Verbindungstabellen. Sie können Verbindungen für die folgenden Protokolle einrichten:

- Basisverbindung für PowerShell und SSH
- JDBC
- JMS
- HTTP(s)

Die Verbindungstabelle verweist auf die Verbindungsalias-Tabelle, die den Verbindungsalias mit Verbindungsinformationen koppelt. Jede Verbindung zeichnet die folgenden Informationen auf:

Basisverbindungseigenschaften

Feld	Beschreibung
Name	Name der Verbindung Dieses Feld muss in der Tabelle eindeutig sein.
Anmeldeinformationen	Geben Sie die Anmeldeinformationen an, die für diese Verbindung verwendet werden sollen. Dies ist optional.
Verbindungsalias	Der Verbindungsalias löst die Verbindung und die Anmeldeinformationen zur Laufzeit auf. Pro Verbindungsalias ist jeweils nur eine Verbindung aktiv.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die aktuelle Verbindung zu aktivieren.
Domäne	Domäne, zu der die Verbindung gehört.

Die Anmeldeinformationen sind für alle aktiven Verbindungen eindeutig, sofern sie nicht leer sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade der Verbindungsinformationen

- Die Tabellen „JDBC-Verbindung“ [jdbc_connection] und „JMS-Verbindung“ [orch_jms_ds] sind vorhandene Orchestration-Verbindungstabellen, die jetzt von der Tabelle „Verbindung“ [sys_connection] erweitert werden. Die Tabellen wurden ursprünglich von „sys_metadata“ erweitert. Die auf „sys_metadata“ bezogenen Daten wurden entfernt.
- Die Tabellen werden aus dem Laufzeit-Plugin „Orchestration“ [com.snc.runbook_automation.runtime] zum Plugin „Anmeldeinformationen und Verbindungen“ verschoben.
- Der Upgrade-Prozess ruft JDBC- und JMS-Verbindungsinformationen ab, erstellt entsprechende Verbindungsaliasnamen und weist den Alias der zugehörigen Verbindung zu.
- JDBC-Feldnamenänderungen:
  - Der JDBC-Server wird in Host umbenannt
  - Der Datenbankport wird in Port umbenannt
  - Daten des JDBC-Servers und der Datenbank werden während des Upgrades zu Host und Port migriert

Basisverbindungen für PowerShell und SSH erstellen

Konfigurieren Sie die Verbindungsinformationen für die Verwendung mit einer benutzerdefinierten Aktivität oder Aktion, die das PowerShell- oder Secure Shell-Protokoll (SSH) verwendet.

Vorbereitungen

Erforderliche Rolle: admin oder connection_admin

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Basisverbindung für PowerShell und SSH** aus.
4. Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Eindeutiger Name des Verbindungsdatensatzes
Anmeldeinformationen	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Host	Vollständig qualifizierter Domänenname des Zielhosts, auf dem das System die Aktivität oder Aktion ausführt. Zum Beispiel: host.domain.com.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legt die Domäne fest, in der die Aktivität ausgeführt wird. Flow Designer unterstützt keine Domänentrennung und dieses Feld ignoriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Standardport überschreiben	Von der Verbindung verwendeter Zielport. Wenn Sie dieses Feld leer lassen, verwendet das System den Wert für den Standardport.
MID-Server verwenden	Aktivieren Sie das Kontrollkästchen, um eine Verbindung mit dem Zielhost über einen MID-Server herzustellen. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“. **Hinweis:** PowerShell erfordert einen MID-Server.
MID Auswahl	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters. ◦ MID Server automatisch**auswählen**: Wählt den MID Server automatisch aus. ◦ **Spezifischer MID Server**: Verwendet den von Ihnen ausgewählten MID Server. ◦ **Spezifischer MID-Cluster**: Verwendet den von Ihnen ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist. **Hinweis:** Stellen Sie sicher, dass auf den Verbindungsdatensatz IntegrationHub verwiesen wird, nicht auf einen Verbindungsdatensatz Orchestration.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Weitere Informationen dazu, wie MID-Server während der Laufzeit ausgewählt wird, finden Sie unter MID Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID Server automatisch auswählen in der Liste MID-** Auswahl ausgewählt ist.
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID Server selection .
MID-Server	Spezifischer MID-Server, auf dem der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Spezifischer MID Server** aus der MID-Auswahlliste ausgewählt wird.
MID-Cluster	Spezifischer MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist und **Spezifischer MID-Cluster** in der MID-Auswahlliste ausgewählt ist.

5. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTP(s)-Verbindung erstellen

Die HTTP(s)-Verbindung stellt die Informationen bereit, mit der benutzerdefinierte HTTP(s)-Aktionen oder -Aktivitäten eine Verbindung herstellen.

Vorbereitungen

Erforderliche Rolle: connection_admin

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**, klicken Sie auf **Neu**und wählen Sie **HTTP(s)-Verbindung**aus.
2. Fügen Sie die folgenden Verbindungsinformationen hinzu, und klicken Sie auf **Absenden**:

Feld	Beschreibung
Name	Eindeutiger Name dieser HTTP(s)-Verbindung.
Anmeldeinformationen	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
URL-Builder	Geben Sie entweder die Verbindungs-URL manuell ein, oder verwenden Sie das System, um die URL basierend auf den Eingaben zu erstellen. Standardmäßig ist dieses Kontrollkästchen deaktiviert. Wenn diese Option aktiviert ist, wird die Verbindungs-URL aus den folgenden Feldern berechnet: ○ Gegenseitige Authentifizierung – Aktivieren Sie das Kontrollkästchen, wenn die gegenseitige Authentifizierung verwendet wird. ○ Protokoll – Wenn keine gegenseitige Authentifizierung verwendet wird, geben Sie das Protokoll ein. Der Standardwert ist HTTPs. ○ Protokollprofil – Wenn die gegenseitige Authentifizierung verwendet wird, geben Sie das Protokollprofil aus „sys_protocol_profile“ ein. ○ Host ○ Port ○ Basispfad – Pfad der Verbindungszeichenfolge. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Verbindungs-URL	Wenn der URL-Builder deaktiviert ist, geben Sie die Verbindungs-URL in dieses Feld ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legen Sie die Domäne, fest in der die Aktion oder Aktivität ausgeführt wird.
MID-Server verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID-Auswahl	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters. ○ MID Server automatisch**auswählen**: Wählt den MID Server automatisch aus. ○ **Spezifischer MID Server**: Verwendet den von Ihnen ausgewählten MID Server. ○ **Spezifischer MID-Cluster**: Verwendet den von Ihnen ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist. **Hinweis:** Stellen Sie sicher, dass auf den Verbindungsdatensatz IntegrationHub verwiesen wird, nicht auf einen Verbindungsdatensatz Orchestration.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Weitere Informationen dazu, wie MID-Server während der Laufzeit ausgewählt wird, finden Sie unter MID Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID Server automatisch auswählen in der Liste MID-** Auswahl ausgewählt ist.
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID Server selection .
MID-Server	Spezifischer MID-Server, auf dem der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Spezifischer MID Server** aus der MID-Auswahlliste ausgewählt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Cluster	Spezifischer MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist und **Spezifischer MID-Cluster** in der MID-Auswahlliste ausgewählt ist.
Verbindungszeitüberschreitung	Anzahl der Millisekunden, die das System auf eine erfolgreiche Hostverbindung wartet. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Lassen Sie dieses Feld leer, um den Standard-Zeitüberschreitungswert für Verbindungen zu verwenden.

3. Klicken Sie auf **Absenden**.
   Sie können jetzt eine benutzerdefinierte HTTP(s)-Aktion oder -Aktivität erstellen.

JDBC-Verbindung erstellen

Die JDBC-Verbindung enthält die Informationen, mit der benutzerdefinierte JDBC-Aktionen oder -Aktivitäten eine Verbindung zu verschiedenen Zieldatenbanken herstellen.

Vorbereitungen

Sie müssen über eine geeignete JAR-Datei verfügen, unabhängig davon, ob sie mit der Instanz oder mit einer benutzerdefinierten JAR-Datei bereitgestellt wird.

Hinweis:
Die ServiceNow-Instanz stellt die Dateien mysql-connector-java-5.1.21.jar, sql-server-jdbc-4.0.jar und ojdbc6.jar als Teil des aktuellen Release bereit, das MySQL-, SQLServer- und Oracle-Datenbanken unterstützt. Andere Datenbanken wie Sybase oder DB2 Universal müssen eine benutzerdefinierte JAR-Datei verwenden, die in die Instanz hochgeladen werden muss, bevor die JDBC-Verbindung festgelegt wird.

Erforderliche Rolle: connection_admin

Warum und wann dieser Vorgang ausgeführt wird

JDBC-Anmeldeinformationen werden von der Aktivitätendesignervorlage separat abgerufen und unterstützen externe Anmeldeinformationsspeicher wie CyberArk.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**, klicken Sie auf **Neu**, und wählen Sie **JDBC-Verbindung**aus.
2. Füllen Sie das Formular anhand der Felder in der Tabelle aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

JDBC-Verbindungsfelder

Feld	Datenbankformat	Beschreibung
Name	Alle	Eindeutiger Name dieser JDBC-Verbindung. Zum Beispiel könnten Sie **JDBC MySQLProd** eingeben.
Berechtigung	Alle	Fügen Sie Anmeldeinformationen für den JDBC-Provider hinzu.
Verbindungsalias	Alle	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
Abfragezeitüberschreitung	Alle	Maximale Dauer, die die JDBC-Abfrage ohne Antwort ausgeführt werden darf.
Verbindungstimeout	Alle	Anzahl der Millisekunden, die das System auf eine erfolgreiche JDBC-Verbindung wartet. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Lassen Sie dieses Feld leer, um den Standard-Zeitüberschreitungswert für Verbindungen zu verwenden.
Aktiv	Alle	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Alle	Domäne für diese Tabelle. Standardmäßig wird die Tabelle „JDBC-Verbindung“ [jdbc_connection] in der Domäne **global** ausgeführt.
Format	Alle	Datenbanktyp für diese Verbindung. Die Standardoptionen sind: ○ **MySQL** ○ **Oracle** ○ **SQL Server** ○ **Keine** Sie können **Sybase** oder **DB2 Universal** der Auswahlliste hinzufügen, indem Sie die entsprechende JAR-Datei des JDBC-Treibers in die Instanz hochladen. Orchestration erkennt diese Treiber automatisch, wenn sie in das System geladen werden, und fügt sie dieser Liste hinzu.
Host	Oracle, MySQL, SQLServer	Hostname oder IP-Adresse des Datenbankservers.
Oracle-SID	Oracle	Der Site-Identifier der Oracle-Datenbank. Der Standardwert ist **orcl**.
Oracle-Anschluss	Oracle	Port, den die Oracle-Datenbank verwendet. Der Standardwert ist **1521**.
Datenbankname	MySQL, SQLServer	Name der Datenbank.
Port	MySQL, SQLServer	Port, den die ausgewählte Datenbank verwendet.
Instanzname	SQLServer	Instanzname für den ausgewählten SQLServer.
Verbindungs-URL	Alle	URL, mit der der MID Server eine Verbindung zu der angegebenen Datenbank herstellt. Die URL wird beim Speichern des Formulars automatisch erstellt und ist für die Standarddatenbanken schreibgeschützt. **Hinweis:** Wenn das ausgewählte Format keine der Standarddatenbanken ist, müssen Sie die Verbindungs-URL manuell erstellen, damit der MID Server darüber informiert ist, wie die Verbindung erstellt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
JDBC-Laufwerk	Keiner, DB2 Universal, Sybase	Der für diese Verbindung zu verwendende JDBC-Treiber, wenn es sich nicht um eine Standarddatenbank handelt. **Hinweis:** Wenn Sie eine Sybase- oder DB2 Universal-Datenbank hinzufügen, müssen Sie den Treibernamen in dieses Feld eingeben und die Treiber-JAR-Datei in die Instanz hochladen.
MID Server verwenden	Alle	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID Auswahl	Alle	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters. ○ MID Server automatisch**auswählen**: Wählt den MID Server automatisch aus. ○ **Spezifischer MID Server**: Verwendet den von Ihnen ausgewählten MID Server. ○ **Spezifischer MID-Cluster**: Verwendet den von Ihnen ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist. **Hinweis:** Stellen Sie sicher, dass auf den Verbindungsdatensatz IntegrationHub verwiesen wird, nicht auf einen Verbindungsdatensatz Orchestration.
Fähigkeiten	Alle	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Weitere Informationen dazu, wie MID-Server während der Laufzeit ausgewählt wird, finden Sie unter MID Server-Auswahl. Dieses Feld ist nur sichtbar, wenn **MID Server automatisch auswählen in der Liste MID-**Auswahl ausgewählt ist.
MID-Anwendung	Alle	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
		Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID Server selection .
MID-Server	Alle	Spezifischer MID-Server, auf dem der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Spezifischer MID Server** aus der MID-Auswahlliste ausgewählt wird.
MID-Cluster	Alle	Spezifischer MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist und **Spezifischer MID-Cluster** in der MID-Auswahlliste ausgewählt ist.

3. Klicken Sie auf **Absenden**.

Zugehörige Informationen

JDBC-Anmeldeinformationen

JMS-Verbindung erstellen

Konfigurieren Sie Ihr System für die Verwendung von Java Messaging Service (JMS) mit einer benutzerdefinierten JMS-Aktivität oder -Aktion.

Vorbereitungen

Erforderliche Rolle: connection_admin

Warum und wann dieser Vorgang ausgeführt wird

Der MID Server muss über die richtigen JMS Connection Factorys für Ihre Organisation verfügen. Konfigurieren Sie diese Werte in der Eigenschaft `mid.property.jms.command.allowed_factory_names` in **MID-Server** > **Eigenschaften**. Die Standardwerte für diese Eigenschaft können in einen beliebigen Wert oder eine durch Kommas getrennte Liste von Werten geändert werden, die der JMS-Provider eines Drittanbieters bekanntgibt.

Prozedur

1. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**.
2. Klicken Sie auf **Neu**, wählen Sie **JMS-Verbindung**aus, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Option	Bezeichnung
Name	Eindeutiger Name dieser Connection Factory.
Anmeldeinformationen	Fügen Sie Anmeldeinformationen für den JMS-Provider hinzu.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Ursprüngliche Kontext-Werkseinstellung	Name der JNDI-Klasse, die zum Erstellen des Initial-Context verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Hinweis: Um beispielsweise eine Verbindung zu ActiveMQ V5.10 (JMS-Provider) herzustellen, lautet der Wert org.apache.activemq.jndi.ActiveMQInitialContextFactory.
Provider-URL	Speicherort der laufenden JMS-Provider-Installation. **Hinweis:** So stellen Sie beispielsweise eine Verbindung zu ActiveMQ V5.1 her: tcp://ipAdresseOderHostname: 61616.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legen Sie die Domäne, fest in der die Aktion oder Aktivität ausgeführt wird.
MID Server verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID-Auswahl	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters. ○ MID Server automatisch**auswählen**: Wählt den MID Server automatisch aus. ○ **Spezifischer MID Server**: Verwendet den von Ihnen ausgewählten MID Server. ○ **Spezifischer MID-Cluster**: Verwendet den von Ihnen ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist.
MID-Cluster	Spezifischer MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID Server verwenden aktiviert** ist und **Spezifischer MID-Cluster** in der MID-Auswahlliste ausgewählt ist.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID Server selection .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID Server selection .

3. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Berechtigungen**.
4. Klicken Sie auf **Neu**, wählen Sie **JMS-Anmeldeinformationen** aus, und geben Sie dann den Benutzernamen und das Passwort ein, die der MID für die Kommunikation mit dem JMS-Provider verwenden soll.
   Weitere Informationen finden Sie unter JMS-Anmeldeinformationen.
5. Klicken Sie auf **Absenden**.
   Sie können jetzt eine benutzerdefinierte JMS-Aktion oder -Aktivität erstellen.

Verbindungsattribute für IntegrationHub erstellen

Definieren Sie verbindungsspezifische Variablen, die Sie in IntegrationHub-Integrationsschritten verwenden können.

Vorbereitungen

Erforderliche Rolle:

- Um Verbindungsattribute zu erstellen, ist die Administratorrolle erforderlich.
- Um Attributwerte zuzuweisen, ist die Rolle „connection_admin“ oder die Administratorrolle erforderlich.
- Die Rolle „action_designer“ oder die Administratorrolle ist erforderlich, Im Attribute in einer benutzerdefinierten Aktion zu verwenden, ist die Rolle „action_designer“ oder die Administratorrolle erforderlich.

Verbindungsattribute werden nur von Integrationsschritten verwendet, für die IntegrationHub abonniert werden muss. Weitere Informationen zum Aktivieren von IntegrationHubfinden Sie unter Fordern Sie eine an IntegrationHub Plugin .

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Integrationsschritt verwenden, müssen Sie eine Verbindung mit einem externen System herstellen. Verwenden Sie einen Alias für Verbindungen und Berechtigungen, anstatt die Verbindung inline zu definieren. Mit einem Alias können Sie die Verbindungsdetails einmal aktualisieren, ohne jede Aktion neu konfigurieren zu müssen. Jeder Aktionsschritt, bei dem ein Alias verwendet wird, erbt die ihm zugeordneten Attribute. Vom Flow Designer werden Attribute als Datenpillen angezeigt, die Sie in Ihren Aktionsschritt ziehen können. Sie können beispielsweise ein Seitengrößenattribut erstellen, das zu einem Abfrageparameter für den REST-Schritt wird.

Weitere Informationen zum Erstellen benutzerdefinierter Flow Designer -Aktionen finden Sie unter Aktionsdesigner .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Erstellen Sie einen Aliasdatensatz, oder wählen Sie einen aus.
3. Klicken Sie in der zugehörigen Liste „Verbindungsattribute“ auf **Neu**.
4. Legen Sie die Attributbezeichnung und den Feldtyp fest.
   Eine Liste der Feldtypen finden Sie unter Feldtypen .
5. Klicken Sie auf den zugehörigen Link „Erweiterte Ansicht“, um erweiterte Dictionary-Voreinstellungen für das Attribut festzulegen.
   Auf diese Weise lässt sich beispielsweise ein Attribut mit einem dynamisch berechneten Wert erstellen. Weitere Informationen finden Sie unter Wörterbucheintragsformular .
6. Klicken Sie auf **Absenden**.
7. Definieren Sie die Attributwerte im Verbindungsdatensatz.
   a. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**.
   b. Erstellen Sie einen Verbindungsdatensatz mit demselben Verbindungstyp wie der Alias, oder wählen Sie einen aus.
   c. Wählen Sie unter **Verbindungsalias** den Alias mit Verbindungsattributen aus.
   d. Speichern Sie den Datensatz.
      Die Registerkarte „Attribute“ wird mit den im Aliasdatensatz definierten Verbindungsattributen gefüllt.
   e. Legen Sie Werte für die Attribute fest.
      Wenn für den Alias **Unterstützt mehrere aktive Verbindungen** aktiviert ist, können Sie einem Alias mehrere Verbindungsdatensätze zuordnen und in jedem Verbindungsdatensatz Attributwerte definieren. Wenn mehrere Verbindungsdatensätze mit Attributwerten für denselben Alias vorhanden sind, Die bei der Ausführung des Ablaufs verwendete Verbindung bestimmt die Attributwerte. Angenommen, Sie haben eine Aktion, die einen Alias mit zwei aktiven Verbindungsendpunkten verwendet: Produktion und Test. Das Attribut wird nach dem Wert aufgelöst, der von der zur Laufzeit verwendeten Verbindung festgelegt wird.
8. Fügen Sie den Alias einem Integrationsschritt im Aktionsdesigner hinzu.
   a. Navigieren Sie zu Flow Designer, und erstellen oder wählen Sie eine Aktion.
   b. Fügen Sie der Aktion einen Integrationsschritt hinzu.
   c. Fügen Sie unter „Verbindungsdetails“ den Alias hinzu, für den Sie Attribute erstellt haben.

Die mit dem Alias verknüpften Verbindungsattribute werden als Datenpillen im Datenbereich angezeigt.

Hinweis:
Das System verfolgt keinen Change an Bezeichnungen und Datentypen von Verbindungsattributen, nachdem Sie den Alias einem Schritt zugeordnet haben. Um die Bezeichnung oder den Datentyp eines Verbindungsattributs zu aktualisieren, löschen Sie den Alias aus dem Schritt, und fügen Sie ihn erneut hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit Anmeldeinformationen

Der MID Server verwendet die Anmeldeinformationen, die Sie in der Tabelle „Anmeldeinformationen“ [discovery_credentials] erstellen, um auf Ressourcen für Discovery, Orchestration, Service Mapping und Cloud Management zuzugreifen.

Verwendung von Anmeldeinformationen durch MID Server

Standardmäßig verwenden Windows-MID Server die Anmeldeinformationen des MID Server-Service auf dem Hostcomputer, um Windows-Geräte im Netzwerk zu ermitteln. Sie sollten die Anmeldeinformationen für den Windows MID Server-Service so konfigurieren , dass sie mindestens über lokale Administratorrechte verfügen. Für Linux - und UNIX -Computer und -Netzwerkgeräte verwendet der MID Server die SSH- und SNMP-Anmeldeinformationen, die in der Instanz in konfiguriert sind **Discovery** > **Berechtigungen**.

MID Server, die von Orchestration verwendet werden, müssen Zugriff auf die erforderlichen Anmeldeinformationen haben, um Befehle auf Computern im Netzwerk auszuführen, wie in den Workflow-Aktivitäten angegeben. Orchestration kann dieselben SSH- und SNMP-Anmeldeinformationen wie Discoveryverwenden, verfügt jedoch über zwei zusätzliche Anmeldeinformationen, die für bestimmte Workflow-Aktivitäten entwickelt wurden: Windows (für PowerShell-Aktivitäten) und VMware.

Verschlüsselung und Entschlüsselung

Die Plattform speichert die Anmeldeinformationen in einem verschlüsselten Feld in der Tabelle „Anmeldeinformationen“ [discovery_credentials]. Einmal eingegeben, können sie nicht angezeigt werden.

Wenn der MID Server Anmeldeinformationen anfordert, entschlüsselt Now Platform die Anmeldeinformationen mit dem folgenden Prozess:

1. Die Anmeldeinformationen werden in der Instanz mit dem festen Schlüssel „password2“ entschlüsselt.
2. Die Anmeldeinformationen werden in der Instanz mit dem öffentlichen Schlüssel des MID Servers erneut verschlüsselt.
3. Die Anmeldeinformationen werden im Lastenausgleichsmodul mit SSL verschlüsselt.
4. Die Anmeldeinformationen werden auf dem MID Server mit SSL entschlüsselt.
5. Die Anmeldeinformationen werden auf dem MID Server mit dem privaten Schlüssel des MID Servers entschlüsselt.

Hinweis:
Die Plattform verfügt nicht über separate Verschlüsselungsschlüssel für Instanzen mit mehreren Mandanten.

Reihenfolge der Anmeldeinformationen

Anmeldeinformationen kann ein Wert für die Reihenfolge im Anmeldeinformationsformular zugewiesen werden. Die Anwendung wird so gezwungen, alle verfügbaren Anmeldeinformationen in einer bestimmten Reihenfolge durchzugehen. Wenn Sie keinen Wert für die Reihenfolge angeben, versucht die Anwendung die Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [discovery_credential] nach dem Zufallsprinzip, bis ein funktionierender gefunden wird. Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Orchestration versucht, einen Befehl auf einem SSH-Server auszuführen, z. B. auf einem Linux- oder UNIX-Computer.
- Discovery versucht, ein SNMP-Gerät abzufragen, z. B. einen Drucker, Router oder eine UPS.

Nach der Ermittlung der Anmeldeinformationen für ein Gerät erstellen Discovery und Orchestration anhand der Tabelle „Anmeldeinformationsaffinität“ [dscy_credentials_affinity] eine Affinität zwischen den Anmeldeinformationen und dem Gerät. Bei allen nachfolgenden Ermittlungen oder Orchestration-Aktivitäten wird versucht, die Anmeldeinformationen in dieser Tabelle einem Gerät zuzuordnen, für das eine Affinität besteht. Wenn sich die Anmeldeinformationen für ein Gerät ändern, testen Discovery und Orchestration alle verfügbaren Anmeldeinformationen erneut, bis sie eine neue Affinität herstellen.

Hinweis:
Wenn Orchestration und Discovery installiert sind und der Anmeldeinformationsalias aktiviert ist, können mehrere Affinitäten vorhanden sein. In diesem Fall sucht die Plattform nach Anmeldeinformationen für jede Affinität und fügt die Anmeldeinformation für die Affinität mit der niedrigsten Reihenfolgenummer in die Probe ein.

Das Angeben einer Reihenfolge für die Anmeldeinformationen ist in den folgenden Situationen hilfreich:

- Die Tabelle „Anmeldeinformationen“ enthält viele Anmeldeinformationen, von denen einige häufiger als andere verwendet werden. Beispiel: Die Tabelle enthält 150 SSH-Anmeldeinformationen, und fünf dieser Anmeldeinformationen werden für die Anmeldung bei 90 % der Geräte verwendet. Es wird empfohlen, diese fünf Anmeldeinformationen mit niedrigen Reihenfolgenummern zu konfigurieren, wodurch sie oben in der Ausführungsliste platziert werden. Discovery und Orchestration arbeiten schneller, wenn sie zuerst diese allgemeinen Anmeldeinformationen ausprobieren. Nach der ersten erfolgreichen Verbindung weiß Now Platform, welche Anmeldeinformationen beim nächsten Mal für jedes Gerät verwendet werden sollen.
- Now Platform verfügt über eine aggressive Anmeldesicherheit. Konfigurieren Sie Datenbankanmeldeinformationen beispielsweise mit einem niedrigen Wert für die Reihenfolge, wenn Solaris-Datenbankserver im Netzwerk nur drei fehlgeschlagene Anmeldeversuche bereitstellen, bevor der MID Server gesperrt wird.

Anmeldeinformationsaliasse

Aliasse für Anmeldeinformationen sind für Discovery und Orchestrationverfügbar.

Mit Aliassen für Discovery kann ein Administrator:

- ein Filterverhalten für Anmeldeinformationen mit konfigurierbaren Compliance-Stufen einsetzen.
- mehrere Anmeldeinformationsaliase einem Discovery-Zeitplan zuweisen.
- Verhindern Sie die Erstellung von Anmeldeinformationsaffinitäten, die unangemessene oder vertrauliche Anmeldeinformationen verwenden. Weitere Informationen finden Sie unter Affinitäten von Anmeldeinformationen.

Aliasse für Orchestration ermöglichen Workflow-Erstellern Folgendes:

- jeder Aktivität in einem Orchestration-Workflow individuelle Anmeldeinformationen zuweisen
- jeder Aktion in Flow Designer individuelle Anmeldeinformationen zuweisen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zuweisen.
- jedem Vorkommen derselben Aktion im Designer-Flow unterschiedliche Anmeldeinformationen zuweisen

Externe Anmeldeinformationsspeicher

Wenn Sie nicht möchten, dass Anmeldeinformationen in Ihrer Instanz gespeichert werden, können Sie externe Repositorien für Anmeldeinformationen verwenden. Externe Anmeldeinformationsspeicher speichern die Anmeldeinformationen an einem externen Standort, auf den Ihre Instanz zugreifen kann. CyberArk ist der einzige externe Anmeldeinformationsspeicher, der unterstützt wird. Andere externe Speicher können jedoch mithilfe der ServiceNow-API konfiguriert werden.

Verbindungs- und Anmeldealias erstellen

Definieren Sie einen Alias, um einen Anmelde- oder einen Verbindungsdatensatz zu kennzeichnen.

Vorbereitungen

Erforderliche Rolle:

- Die Administratorrolle ist erforderlich, um einen Alias zu erstellen.
- Die Rollen „credential_admin“ und „connection_admin“ haben Lesezugriff auf den Aliasdatensatz.

Warum und wann dieser Vorgang ausgeführt wird

Der Verbindungs- und Anmeldealias definiert einen Alias, der einen Anmelde- oder einen Verbindungsdatensatz kennzeichnet. Der Alias enthält diese Felder.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Aliasse für Verbindungen und Anmeldeinformationen

Feld	Beschreibung
Name	Name des Alias. Ein Alias darf nur Buchstaben, Ziffern und Unterstriche enthalten. Während eines Upgrades wird das Tag im Anmeldedatensatz zu einem Verbindungs- und Anmeldealias migriert. Wenn das Anmeldeinformations-Tag andere Sonderzeichen als Buchstaben, Ziffern und Unterstriche enthält, wird der Tag-Name nach dem Upgrade beibehalten. Sie können diesen migrierten Alias weiterhin verwenden, Sie können ihn allerdings erst aktualisieren, wenn Sie den Namen den Namensbeschränkungen entsprechend ändern.
ID	Eindeutiger Bezeichner für den Alias für Verbindungen und Anmeldeinformationen, basierend auf dem Format `scope_name.alias_name`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wenn der Bereich Global ist, ist die ID der Aliasname. Wenn Sie beispielsweise einen Workday-Alias im globalen Bereich erstellen, wird die ID auf workday festgelegt. ○ Wenn Sie einen Workday-Alias im Bereich der HR-App erstellen, wird die ID auf x_hr_app.workday festgelegt.
Typ	Wählen Sie entweder **Anmeldeinformationen** oder **Verbindung und Anmeldeinformationen aus**. Der Standardwert ist „Verbindung und Anmeldeinformationen“.
Anwendung	Anwendungsbereich, für den der Alias für Verbindungen und Anmeldeinformationen zugewiesen wird. Der aktuelle Sitzungsumfang, den Sie zuletzt in der Anwendungsauswahl ausgewählt haben, wird angezeigt. ○ Zum Beispiel wird **Global** angezeigt, wenn dies der aktuelle Bereich für diese Sitzung ist. ○ Sie können den Bereich in der Anwendungsauswahl ändern, bevor Sie einen Alias erstellen. Weitere Informationen zu Anwendungsbereichen und ihrer Auswahl finden Sie unter: ▪ Anwendungsbereich ▪ Anwendungen aus der Anwendungsauswahl auswählen
Verbindungstyp	Name des Verbindungstyps, entweder Basic, HTTP, JDBC, JMS oder Kafka. Der Standardwert ist HTTP.
Unterstützt mehrere aktive Verbindungen	Bezeichner, der angibt, ob der Alias mehrere aktive Verbindungen unterstützt. Fügen Sie mithilfe der Tabelle „Verbindungen“ Verbindungen hinzu, und verknüpfen Sie sie mithilfe der zugehörigen Liste „Verbindungen“ mit dem Alias.
Standard-Wiederholungsrichtlinie	Wiederholungsrichtlinie für den Alias. Weitere Informationen finden Sie unter Wiederholungsrichtlinie .
Konfigurationsvorlage	Konfigurationsvorlage, die zum Erstellen eines Verbindungs- und Anmeldeinformationsdatensatzes verwendet werden soll.

4. Klicken Sie auf **Speichern**.
Die zugehörige Liste Verbindungen und Verbindungsattribute wird angezeigt.

Zugehörige Liste	Beschreibung
Verbindungen	Zugehörige Verbindungsdatensätze, die diesem Alias zugeordnet sind. Nachdem Sie den Alias erstellt haben, können Sie Verbindungsdatensätze definieren und diese mit dem Alias verknüpfen. Wenn **Unterstützt mehrere aktive Verbindungen** ausgewählt ist, können Sie einem Alias mehrere Verbindungen zuordnen.
Verbindungsattribute	Attribute für die Verbindung. Definieren Sie für eine Verbindung spezifische Daten, und verwenden Sie sie in einem IntegrationHub-Integrationsschritt. Weitere Informationen finden Sie unter Verbindungsattribute für IntegrationHub erstellen.
Untergeordnete Aliasse	Untergeordnete Aliasse, die dem übergeordneten Alias zugeordnet sind. Nach dem Erstellen eines Alias für Verbindungen und Anmeldeinformationen können Sie einen untergeordneten *Alias* erstellen, um mehrere Verbindungen für dieselbe Anwendungsintegration zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Verbindungen	Zugehörige Verbindungsdatensätze, die diesem Alias zugeordnet sind. Nachdem Sie den Alias erstellt haben, können Sie Verbindungsdatensätze definieren und diese mit dem Alias verknüpfen. Wenn **Unterstützt mehrere aktive Verbindungen** ausgewählt ist, können Sie einem Alias mehrere Verbindungen zuordnen.
Verbindungsattribute	Attribute für die Verbindung. Definieren Sie für eine Verbindung spezifische Daten, und verwenden Sie sie in einem IntegrationHub-Integrationsschritt. Weitere Informationen finden Sie unter Verbindungsattribute für IntegrationHub erstellen.

5. **Wahlweise:** Wenn Sie neue Anmeldeinformationen und Verbindungen erstellen möchten, die Ihrem Anmeldeinformationsalias zugeordnet sind, klicken Sie unter *Related Links*auf **Neue Verbindung und Anmeldeinformationen erstellen**.
   Die resultierenden Verbindungs- und Anmeldeinformationsdatensätze basieren auf einer vordefinierten Konfigurationsvorlage. Weitere Informationen finden Sie unter Konfigurationsvorlagen für Verbindungen und Anmeldeinformationen.
6. **Wahlweise:** Wenn Sie einen untergeordneten Alias für Ihre Verbindung und Ihren Anmeldeinformationsalias erstellen möchten, wählen Sie in der zugehörigen Liste „ **Untergeordnete Aliasse** “ die Option **Neu**aus.

   a. Geben Sie einen Namen für den untergeordneten Alias ein, und wählen Sie **Absenden**.
      Der untergeordnete Alias erbt Eigenschaften vom übergeordneten Alias. Sie können dann einen untergeordneten Alias so konfigurieren, dass er seinen eigenen Satz von Verbindungs- und Anmeldeinformationen enthält.

Nächste Maßnahme

Erstellen Sie einen oder mehrere Verbindungsdatensätze, die dem Alias oder den untergeordneten Aliassen zugeordnet werden sollen. Weitere Informationen zum Erstellen von Verbindungen finden Sie unter Erste Schritte mit Verbindungen. Fügen Sie dem Alias Verbindungsattribute hinzu, um Verbindungsmetadaten für Abläufe im Flow Designer verfügbar zu machen.

Anmeldeinformationsaliasse für Discovery

Mit Aliassen für Anmeldeinformationen für Discovery kann ein Administrator bestimmte Anmeldeinformationen für Erkennungszeitpläne verwenden. Sie können Verhaltensweisen für Ihre Aliasse konfigurieren, die bestimmen, wie strikt das System ihre Nutzung durchsetzt.

Ohne Anmeldeinformationsaliasse können Discovery-Zeitpläne auf alle Anmeldeinformationen zugreifen, die in der Instanz definiert sind. Dieses Verhalten ist unter bestimmten Umständen möglicherweise nicht wünschenswert, insbesondere für Anmeldeinformationen mit erhöhten Berechtigungen. Anmeldeinformationsaliasse bieten mehr Kontrolle darüber, welche Anmeldeinformationen ein Discovery-Zeitplan verwenden darf, und verhindern, dass Anmeldeinformationen mit erhöhten Rechten unnötigerweise offengelegt werden.

Funktionsweise von Anmeldeinformationsaliassen

Eine Geschäftsregel namens „ *Discovery-Affinität und Cred* -Alias einfügen“ (zuvor „ *Discovery-Affinität*einfügen“) wird ausgeführt, wenn ein Datensatz in die ECC-Warteschlange eingefügt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird. Die Geschäftsregel hängt die Anmeldeinformationsaliasse, die im Discovery-Zeitplan definiert werden, an die Probe an, damit der MID Server Anmeldeinformationen filtern kann. Die erste Aufgabe des MID Servers besteht darin, die Liste der Anmeldeinformationen für die Suche zu erstellen. Sie filtert die Anmeldeinformationen nach Affinität und dann nach Tags, falls vorhanden. Die Affinitäten werden an das obere Ende der Liste und die entsprechenden Tags an das untere Ende der Liste gesetzt. Der MID Server geht immer wieder die Liste durch, bis er funktionierende Anmeldeinformationen findet. Dann erstellt der MID Server eine Affinität für diese Anmeldeinformationen.

Hinweis:
Die Anmeldeinformationen müssen mit allen Anmeldeinformations-Tags übereinstimmen.

Wenn mit der Geschäftsregel festgestellt wird, dass eine Affinität für das Gerät vorhanden ist, wird anhand der Regel die richtige *credential_id* identifiziert, die zu verwenden ist. Dies ist die *sys_id* des Datensatzes in der Tabelle „Anmeldeinformationen“ [discovery_credentials]. Wenn die Plattform auf eine Affinität mit einem Aliaswert für Anmeldeinformationen stößt, der in der Geschäftsregel als *credential_alias* definiert ist, ermittelt die Geschäftsregel, ob die von der Affinität referenzierten Anmeldeinformationen den angegebenen Alias aufweisen. Wenn dies der Fall ist, wählt die Geschäftsregel die *credential_id* des Alias aus und übergibt diesen Wert an den MID Server. Wenn die Anmeldeinformationen nicht über den angegebenen Anmeldeinformationsalias verfügen, werden alle anderen für das Zielsystem vorhandenen Affinitäten geprüft.

Discovery-Anmeldeinformationsalias erstellen

Erstellen Sie den Alias, und fügen Sie diesen Alias dann den Anmeldeinformationen im Anmeldeinformationsdatensatz hinzu. Sie können Anmeldeinformationen mehreren Aliassen und mehrere Anmeldeinformationen einem einzelnen Alias hinzufügen.

Vorbereitungen
Erforderliche Rolle: admin, credential_admin (nur Lesezugriff), connection_admin (nur Lesezugriff)

Warum und wann dieser Vorgang ausgeführt wird
Ein Discovery-Zeitplan verwendet nur Anmeldeinformationen, die in den für den betreffenden Zeitplan definierten Aliassen enthalten sind.

Hinweis:
Wenn ein Anmeldeinformationsalias für einen Zeitplan definiert ist, ignoriert er alle zuvor vorhandenen Anmeldeinformationsaffinitäten zwischen den Anmeldeinformationen und dem Ziel, das in einem Zeitplan erkannt wird, der für die Verwendung dieses Anmeldeinformationsalias eingerichtet ist.

Prozedur

1. Erstellen Sie einen Alias.

a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.

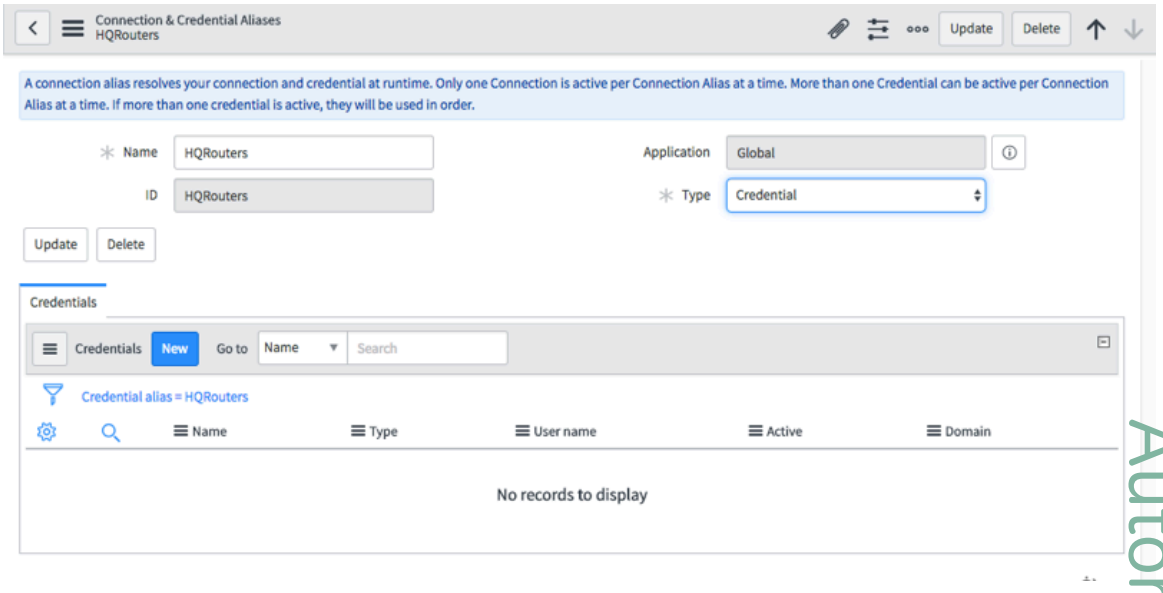
b. Klicken Sie auf **Neu**.

c. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie **Anmeldeinformationen** für den **Typ**des Alias aus.

d. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die zugehörige Liste „ **Anmeldeinformationen** “ wird angezeigt. Sie können für diesen Alias in dieser Liste neue Anmeldeinformationen hinzufügen, nicht jedoch bestehende Anmeldeinformationen.

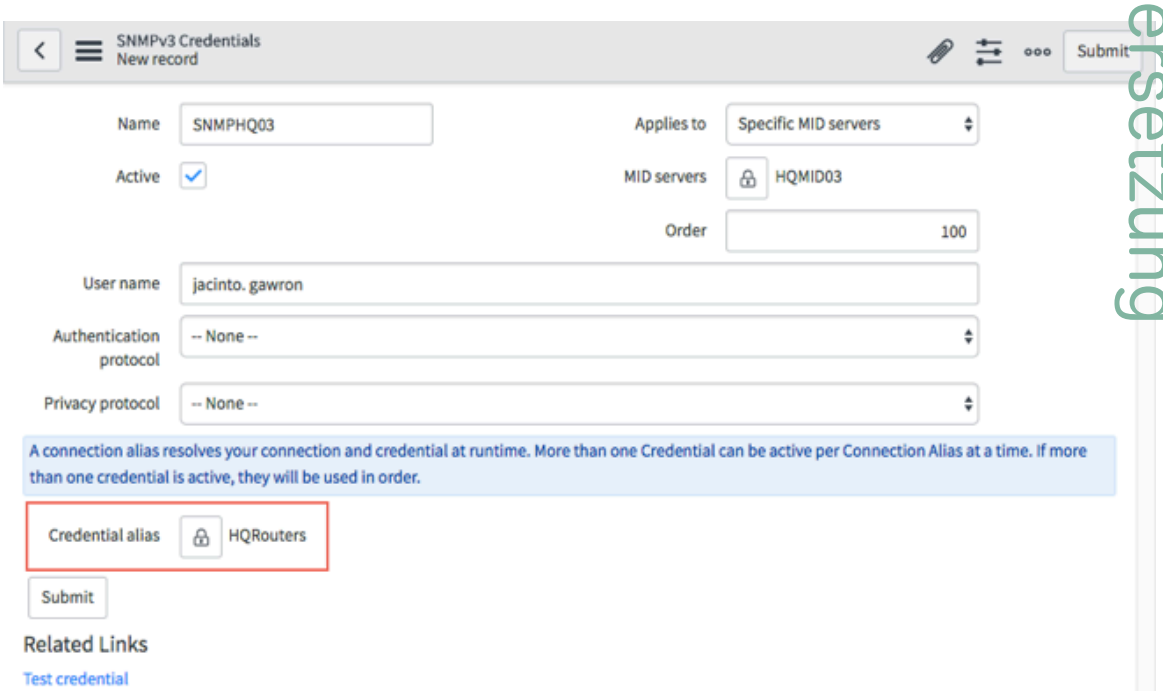


2. Konfigurieren Sie Anmeldeinformationen für den neuen Alias.

a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Berechtigungen**.

b. Wählen Sie vorhandene Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu**, um neue Anmeldeinformationen zu erstellen.

c. Entsperren Sie im **Anmeldeinformationsdatensatz** das Feld Anmeldeinformationsalias, und wählen Sie den von Ihnen erstellten Alias aus.

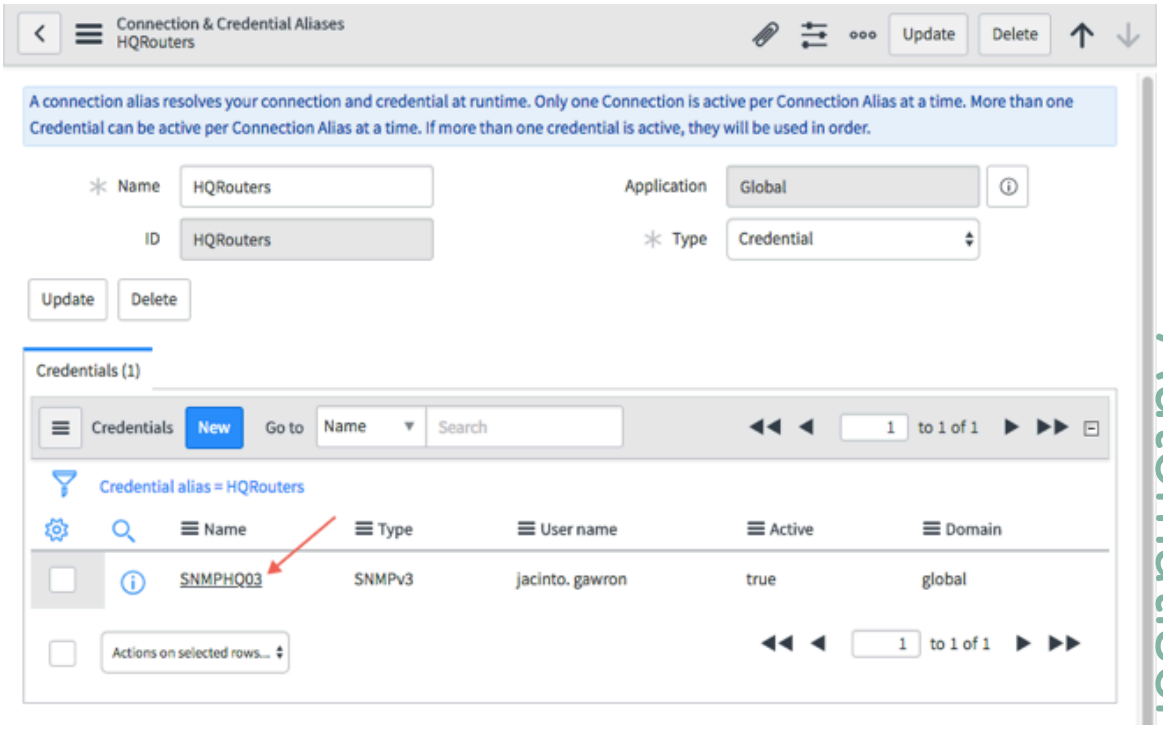


d. Speichern Sie den Datensatz, oder senden Sie ihn ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Zurück zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen** und öffnen Sie Ihren neuen Alias.
   Die Anmeldeinformationen, die Sie an den Alias angehängt haben, werden jetzt in der zugehörigen Liste angezeigt.



4. Um zusätzliche Anmeldeinformationen für diesen Alias zu erstellen, klicken Sie in der zugehörigen Liste auf **Neu**, und wählen Sie einen Anmeldeinformationstyp aus.
   Der Aliasname ist im Feld Anmeldeinformationsalias des Anmeldeinformationsdatensatzes vorab **ausgefüllt**.
5. Füllen Sie die Felder im Formular aus, und senden Sie den Datensatz.

Anmeldeinformationsaliasse für Orchestration-Aktivitäten

Der Anmeldeinformationsalias ermöglicht einem Administrator mehr Kontrolle über die in Orchestration-Aktivitäten verwendeten Anmeldeinformationen.

Dies ist nützlich, wenn eine Aktivität zur Ausführung einer Aufgabe bestimmte Anmeldeinformationen benötigt. Sie können ein Anmeldeinformations-Tag verwenden, um bestimmten Aktivitäten in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zuzuweisen.

Der Anmeldeinformationsalias interagiert mit der Anmeldeinformationsaffinität, um zu bestimmen, welche Anmeldeinformationen für eine Orchestration-Aktivität verwendet werden sollen.

Funktionsweise des Anmeldeinformationsalias

Eine Geschäftsregel namens „ *Discovery-Affinität* einfügen“ (im Geneva-Release umbenannt von „Berechtigungsnachweis-Affinität einfügen“) wird ausgeführt, wenn ein Datensatz in die ECC-Warteschlange eingefügt wird. Diese Regel bestimmt, ob eine Berechtigungsaffinität für das Gerät besteht, und identifiziert die richtige, zu verwendende *credential_id* (die *sys_id* des Datensatzes in der Tabelle „Anmeldeinformationen“ [discovery_credentials]). Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

die Plattform auf eine Affinität mit einem definierten Aliaswert für Anmeldeinformationen (*credential_alias* in der Geschäftsregel) stößt, ermittelt die Geschäftsregel, ob die von der Affinität referenzierten Anmeldeinformationen den angegebenen Alias haben. Wenn dies der Fall ist, wählt die Geschäftsregel die *credential_id* des Anmeldeinformationsalias aus und übergibt diesen Wert an den MID Server. Wenn der Anmeldeinformationen nicht über den angegebenen Anmeldeinformationsalias verfügen, werden alle anderen für das Zielsystem vorhandenen Affinitäten geprüft. Wenn keine Affinität auf entsprechend gekennzeichnete Anmeldeinformationen verweist, durchläuft der MID Server die Tabelle „Anmeldeinformationen“ *[discovery_credentials]* und wählt die Anmeldeinformationen mit dem entsprechenden Tag aus. Der MID Server erstellt dann eine neue Affinität für diese Anmeldeinformationen.

Anmeldeinformationen erstellen und testen

Erstellen und testen Sie die Anmeldeinformationen, die Discovery, Service Mapping, Cloud Management und Orchestration für den Zugriff auf Hardware und Software in Ihrem Netzwerk benötigen.

Vorbereitungen

Erforderliche Rolle: admin

Überprüfen Sie Ihre Sicherheitsrichtlinie und -optionen mit dem Sicherheitsteam Ihrer Organisation.

Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe enthält allgemeine Verfahren zum Erstellen von Anmeldeinformationen. Weitere Informationen zu bestimmten Feldern und Anforderungen finden Sie in der Dokumentation zu Ihrem Anmeldeinformationstyp.

Unterstützte Anmeldeinformationstypen

Applicative-Anmeldeinformationen	Virtual Server Interface	Chef-Server-Anmeldeinformationen
CIM-Anmeldeinformationen	Cloud-Anmeldeinformationen	Infoblox-Anmeldeinformationen
JDBC-Anmeldeinformationen	JMS-Anmeldeinformationen	OAuth 2.0-Anmeldeinformationen
SAP-Anmeldeinformationen	SNMP-Anmeldeinformationen	SSH-Anmeldeinformationen
VMware-Anmeldeinformationen	Windows-Anmeldeinformationen	

Hinweis:
Um die Sicherheit zu verbessern, beschränken Sie den Umfang der Anmeldeinformationen auf einen bestimmten MID Server oder Zeitplan, um unnötige Anmeldeinformationen zu vermeiden.

Prozedur

1. Navigieren Sie zu einem dieser Module:
   - **Discovery** > **Berechtigungen**
   - **Service Mapping** > **Berechtigungen**
   - **Orchestration** > **Berechtigungen**
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf der Seite „Berechtigungen“ auf einen Link für den Anmeldeinformationstyp, und füllen Sie das Formular aus.

   Weitere Informationen finden Sie in der Dokumentation zum ausgewählten Anmeldeinformationstyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können einen Anmeldeinformationsdatensatz zuerst absenden und dann später testen oder die Anmeldeinformationen unmittelbar vor dem Speichern testen.

Das Testen der Anmeldeinformationen wird für folgende Anmeldeinformationstypen unterstützt:

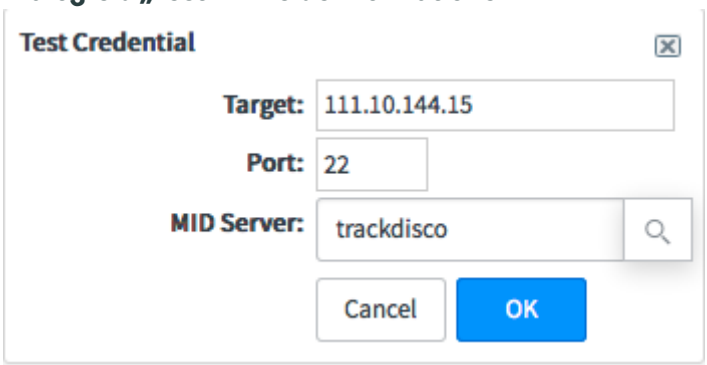
- Private SSH-Schlüssel
- Windows
- SNMP v3
- VMware
- JDBC
- JMS

4. Klicken Sie unter **Zugehörige Links** auf **Test-Anmeldedaten**.

> **Hinweis:**
> Die Anmeldeinformationen sind während des Tests stets verschlüsselt.

5. Füllen Sie die Felder im Dialogfeld „Test-Anmeldeinformationen“ aus.

Dialogfeld „Test-Anmeldeinformationen“



Felder im Dialogfeld „Test-Anmeldeinformationen“

Feld	Beschreibung	Anmeldeinformationstyp
Ziel	Zielhost, auf dem diese Anmeldeinformationen ausgeführt werden. Dieser Wert muss für alle Anmeldeinformationstypen eine IP-Adresse sein, mit Ausnahme von VMware, für das die Host-URL angegeben werden kann. Sie können keine MID-Server als Ziel verwenden.	Alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung	Anmeldeinformationstyp
	Hinweis: Bei JMS ist dies die Provider-URL. Die Informationen in dieser URL teilen JNDI mit, wie der JMS-Provider gefunden und darauf zugegriffen werden kann. Ein Beispielwert für die Verbindung zu ActiveMQ V5.1 ist tcp://ipAdresseOderHostname:61616.	
Port	Port des Ziels, der für diesen Test verwendet werden soll. Das System füllt dieses Feld vorab mit dem Standardport für den ausgewählten Anmeldeinformationstyp aus.	Alle
MID Server	Für diesen Test zu verwendender MID Server. Sie müssen einen Windows-MID-Server verwenden, um die Windows-Anmeldeinformationen zu testen. Nur MID-Server, die **In Betrieb** und **Überprüft** sind, stehen zur Verfügung.	Alle
DB-Typ	Typ der Datenbank, für die diese Anmeldeinformationen getestet werden sollen.	JDBC
DB-Name	Name der Datenbank, für die diese Anmeldeinformationen getestet werden sollen.	JDBC
Ursprüngliche Kontext-Werkseinstellung	Name der JNDI-Klasse, die zum Erstellen des InitialContext verwendet wird. Bei Verwendung dieser **Ursprünglichen Kontext-Werkeinstellung** werden verschiedene JMS-Objekte, z. B. JMS-Verbindung, erstellt. Wenn Sie beispielsweise eine Verbindung zu ActiveMQ V5.10 (JMS-Provider) herstellen möchten, lautet der Wert in diesem Feld org.apache.activemq.jndi.ActiveMQInitialContextFactory	JMS

6. Klicken Sie auf **OK**, um den Test zu beginnen.
   Ein Indikator zeigt an, dass das System versucht, das Ziel mit den von Ihnen angegebenen Anmeldeinformationen zu kontaktieren. Wenn die Instanz eine Verbindung zum Ziel herstellt, wird eine Erfolgsmeldung angezeigt. Wenn die Instanz bei den von Ihnen angegebenen Testeingaben auf ein

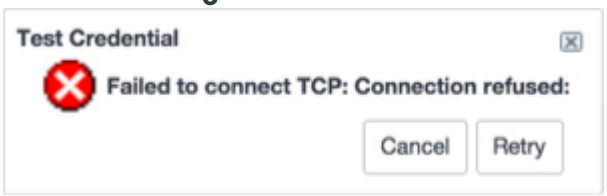
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem stößt, wird die entsprechende Fehlermeldung angezeigt. Nachfolgend finden Sie einige häufige Fehlermeldungen.

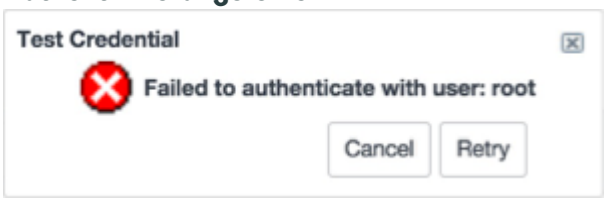
- Falsches Ziel oder falsche Portnummer:

  TCP-Verbindungsfehler

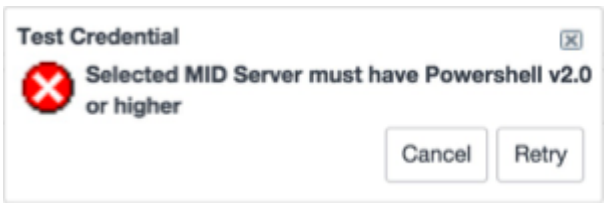
- Falscher Benutzername oder falsches Passwort:

  Authentifizierungsfehler

- Falscher MID Server für Windows-Anmeldeinformationen:

  MID Server-Fehler

7. Klicken Sie auf **Neuversuch**, um das Dialogfeld „Test-Anmeldedaten“ zu öffnen und den Eingabefehler zu korrigieren.
8. Wenn der Test der Anmeldeinformationen erfolgreich ist, klicken Sie auf **Absenden**, um den Datensatz zu speichern.

> **Wichtig:**
> Durch das Testen der Anmeldeinformationen kann nicht sichergestellt werden, dass die Anmeldeinformationen über die erforderlichen Berechtigungen für die beabsichtigten Discovery- oder Orchestration-Workflow-Aufgaben verfügen.

Ansible Tower-Anmeldeinformationen

Ansible Tower-Anmeldeinformationen werden für den Zugriff auf den Account zur Ansible-Konfigurationsverwaltung benötigt. Verwenden Sie diese Anmeldeinformationen zum Verwalten von Ansible-Ressourcen über die Cloud-Management-Anwendung.

Zur Integration von Cloud Provisioning and Governance mit dem Ansible-Konfigurationsverwaltungskonto müssen Benutzername und Passwort für das Administratorkonto in Ansible konfiguriert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Ansible Tower-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Benutzername/ Passwort	Geben Sie die Authentifizierungsinformationen für den Ansible Tower-Benutzer mit Administratorrechten ein.

Hinweis:
Sie müssen keine anderen Felder konfigurieren

Anmeldeinformationen für API-Keys

Ein API-Key ist ein eindeutiger Code, der an eine API übergeben wird, um die aufrufende Anwendung oder den aufrufenden Benutzer zu identifizieren.

Anmeldeinformationen für API-Keys

Formularfelder für Anmeldeinformationen für API-Keys

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
API Key	Geben Sie den API Key ein.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Flows und Workflows, jeder Aktivität in einem Flow oder Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Flow oder Workflow unterschiedliche Anmeldeinformationen zu.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Applicative-Anmeldeinformationen

Einige Anwendungen erfordern zusätzlich zu den vom Host-Computer benötigten weitere Anmeldeinformationen. Anmeldeinformationen, die für den Zugriff auf diese Anwendungen erforderlich sind, werden als Applicative-Anmeldeinformationen bezeichnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typische Anmeldeinformationen enthalten einen Benutzernamen und ein Passwort für die Anmeldung bei einem Gerät oder einer Anwendung. Während die meisten Anwendungen nur einen Berechtigungsnachweis für den Zugriff auf sie benötigen, verfügen Hosts und Anwendungen manchmal über separate Anmeldeinformationen für zusätzliche Sicherheit. Beispielsweise benötigen ABAP SAP Central Services (ASCS) zusätzlich zu den SSH- oder Windows-Host-Anmeldeinformationen für den Server, auf dem ASCS gehostet wird, Applicative-Anmeldeinformationen.

Hinweis:
ServiceNow-Anwendungen beziehen sich auf Geräte und Anwendungen, die Anwendungsservices als Konfigurationselemente (Configuration Items, CIs) umfassen.

Wie bei Hostanmeldeinformationen weisen Sie MID ServersApplicative-Anmeldeinformationen zu.

Sie erstellen Applicative-Anmeldeinformationen pro CI-Typ. Der CI-Typ für ASCS ist beispielsweise SAP ASCS-Anwendung [cmdb_ci_appl_sap_ascs]. Das vorkonfigurierte Muster zum Erkennen von CIs, die zu diesem CI-Typ gehören, enthält Befehle, für die von MID-Server die Verwendung des anwendbaren Berechtigungsnachweises für diesen CI-Typ erfordern. Wenn für diesen CI-Typ mehrere Anmeldeinformationen konfiguriert sind, versucht MID-Server, diese Anmeldeinformationen in der von Ihnen definierten Reihenfolge zu verwenden, bis die passenden Anmeldeinformationen gefunden werden.

Überprüfen Sie die Informationen zu den Discovery-Anforderungen in der ServiceNow-Dokumentation, um festzustellen, ob Sie Applicative-Anmeldeinformationen für bestimmte Anwendungs-CIs konfigurieren müssen. Es ist nicht erforderlich, Applicative-Anmeldeinformationen zu konfigurieren, wenn dies in den Voraussetzungen von Discovery nicht erwähnt wird.

Felder für Applicative-Anmeldeinformationen

Feld	Beschreibung
Name	Name des Berechtigungsnachweises Verwenden Sie einen beschreibenden Namen wie Oracle DB oder London Oracle DB (für eine Oracle-Datenbank). Verwenden Sie keine Leerzeichen oder Sonderzeichen für den Anmeldeinformationsnamen.
Aktiv	Aktivieren Sie das Kontrollkästchen, um den Berechtigungsnachweis zu verwenden.
Benutzername	Geben Sie den tatsächlichen Benutzernamen des Antragsnachweises ein.
Passwort	Geben Sie das tatsächliche Passwort des Antragsnachweises ein. Verwenden Sie keine Leerzeichen oder Sonderzeichen für den Anmeldeinformationsnamen.
CI-Typ	Wählen Sie einen CI-Typ aus, zu dem das CI gehört.
Anmeldeinformationsalias	Erstellen Sie einen Alias, um bestimmten Discovery-Zeitplänen bestimmte Anmeldeinformationen zuzuweisen. Bei der Zuweisung eines Alias müssen Sie den Tabellennamen für den CI-Typ identifizieren, dessen Applicative-Anmeldeinformationen von der Anwendung verwendet werden. Von Anwendungen können Applicative-Anmeldeinformationen eines CI-Typs verwendet werden, der sich von ihrem eigenen unterscheidet. Informationen zu einer bestimmten Anwendung finden Sie in der entsprechenden Tabelle aus der Liste: • ABAP SAP Central Services (ASCS): cmdb_ci_appl_sap_ascs • IBM Security Access Manager-Appliance: cmdb_ci_app_server_webseal

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Applicative-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
	• SAP Central-Instanz: cmdb_ci_appl_sap_ascs • SAP Central Services (SCS): cmdb_ci_appl_sap_ascs • SAP Evaluated Receipt Settlement (ERS): cmdb_ci_appl_sap_ascs • SAP Java-Cluster: cmdb_ci_appl_sap_ascs • SAP NetWeaver Dialog Instance: cmdb_ci_appl_sap_ascs • Microsoft Exchange Mailbox (für Microsoft Exchange): cmdb_ci_exchange_mailbox • Microsoft SQL-Datenbank: cmdb_ci_db_mssql_instance • MySQL Server: cmdb_ci_db_mysql_instance • Oracle Advanced Queue-Warteschlange: cmdb_ci_db_ora_instance • Oracle-Datenbank: cmdb_ci_db_ora_instance • Oracle E-Business Suite: cmdb_ci_db_ora_instance • Oracle WebLogic-Modul: cmdb_ci_app_server_weblogic • Tibco Enterprise Message Service (EMS): cmdb_ci_appl_tibco_message
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Virtual Server Interface

Der Anmeldeinformationstyp für die Standardauthentifizierung verwaltet den Zugriff zum Speichern von Anmeldeinformationen für die Standardauthentifizierung.

Diese Felder stehen im Formular „Anmeldeinformationen“ für die Standardauthentifizierung zur Verfügung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **Standardauthentifizierung** nennen.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den eindeutigen Schlüssel ein, der für diese Anmeldeinformationen im externen CyberArk-Anmeldeinformationsspeichersystem konfiguriert wurde. Die Nachweis-ID kann als Safe-Überschreibung verwendet werden, wenn mehrere Safes verwendet werden. Standardmäßig lautet die Syntax im Feld „ **Anmeldeinformations-ID** “: `<safe name>:<Credential ID>`. Wenn der Safe-Name weggelassen wird, muss ein Safe-Name in der Datei config.xml definiert sein. Um das Trennzeichen vom Standard-Doppelpunkt in ein anderes Zeichen zu ändern, überschreiben Sie den Wert mit dem optionalen Parameter `ext.cred.safe_name`. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Chef-Server-Anmeldeinformationen

Chef-Server-Anmeldeinformationen greifen auf Chef-Integrationen mit der Instanz zu.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „Chef-Server“ verfügbar. Diese Informationen stammen aus den Einstellungen, die Sie bei der Durchführung der Chef-Server-Installation konfiguriert haben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Administratorname	Geben Sie den Administratornamen an, den Sie während der Chef-Server-Installation erstellt haben.
Administratorschlüssel	Geben Sie den privaten RSA-Schlüssel ein, den der Chef-Server beim Erstellen des Administrators generiert hat.
Validierungsname	Geben Sie den Namen des Prüfers ein.
Bestätigungsschlüssel	Geben Sie den privaten RSA-Schlüssel ein, den der Chef-Server beim Erstellen einer Organisation generiert hat.
Zertifikatname	Geben Sie den Zertifizierungsnamen ein.
Zertifikatschlüssel	Geben Sie den Zertifizierungsschlüssel ein.

CIM-Anmeldeinformationen

Der CIM-Berechtigungstyp verwaltet den Zugriff auf einen CIM-Server (auch als CIMOM - Common Information Model Object Manager bezeichnet), um Informationen zu VMware ESX-Servern zu erhalten. Dieser Anmeldeinformationstyp ist für Discovery verfügbar.

Diese Felder sind im Anmeldeinformationsformular für CIM verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen. Weitere Informationen finden Sie unter Ändern der Anmeldeinformationen auf Nicht-Standard.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifisch **Spezifische MID-Server** wirkt sich nicht auf die MID-Server-Auswahl aus. Sie wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

NetApp-Speichergeräte für CIM-Anmeldeinformationen konfigurieren

NetApp-Speichergeräte erfordern eine zusätzliche Konfiguration, damit Discovery sie untersuchen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Installieren Sie den SMI-S-Agenten auf dem Speichergerät-Host.

   Beachten Sie hinsichtlich Anweisungen und Anforderungen den Data ONTAP SMI-S Agent 5.2 Installation and Configuration Guide.

   Hinweis:

   ServiceNow verwaltet die Dokumentation auf dieser Website nicht. Dieses Dokument kann ohne vorherige Ankündigung geändert werden.

2. Erstellen Sie einen Benutzer-Account und ein Passwort für den SMI-S-Agenten.
3. Erstellen Sie einen Anmeldeinformationsdatensatz für die SMI-S-Agentenanmeldeinformationen. Legen Sie den Anmeldeinformationstyp auf **CIM** fest.

Cloud-Anmeldeinformationen

Cloud-Anmeldeinformationstypen verwalten den Zugriff auf cloudbasierte Anwendungen, einschließlich Amazon Web Services und der Microsoft Azure Cloud.

AWS IAM-Rollen (Identity and Access Management).

Wenn Sie einen MID Server auf Amazon EC2 in einer AWS-Cloud installiert haben und dieser MID Server für die Erkennung von Ressourcen in der Cloud konfiguriert ist, können Sie Sicherheitsanmeldeinformationen verwenden, die von AWS Identity and Access Management (IAM)-Rollen bereitgestellt werden, anstatt Anmeldeinformationen, die auf verwaltet werden Ihre Instanz. Diese AWS-Anmeldeinformationen gewähren Berechtigungen in der Cloud über ein *Instanzprofil*basierend auf Rollen. Diese Anmeldeinformationen sind temporär und rotieren automatisch in einem konfigurierbaren Intervall. Wenn eine IAM-Rolle auf dem MID-Server definiert ist. Weitere Informationen finden Sie unter MID Server für AWS IAM-Rollen konfigurieren.

Discovery ignoriert alle in der Instanz gespeicherten Anmeldeinformationen und verwendet stattdessen die von der Rolle im Instanzprofil gewährten Anmeldeinformationen. Weitere Informationen zu AWS-Instanzprofilen finden Sie unter IAM-Rollen für Amazon EC2.

AWS-Anmeldeinformationen

Formularfelder mit AWS-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen.
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die **Zugriffsschlüssel-ID**, die Sie in der AWS-Verwaltungskonsole generiert haben, z. B: APIAIOSFODNN7BEISPIEL.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder mit AWS-Anmeldeinformationen (Fortsetzung)

Feld	Eingabewert
Geheimer Zugangsschlüssel	Der **geheime Zugriffsschlüssel**, den Sie in der AWS-Verwaltungskonsole generiert haben, z. B.: wPalrXUtnFEMI/K7MDENG/bPxRfiCYBEISPIELSCHLÜSSEL.

Felder des Azure-Dienstprinzipal-Anmeldeinformationsformulars

Feld	Wert
Name	Geben Sie den Namen des Service Principals ein, der bei der Instanz registriert werden soll.
Tenant-ID und	Fügen Sie den Wert der Azure-**Verzeichnis-ID** aus dem Azure-Portal in das Feld Cloud-Management **Tenant-ID** ein.
Client-ID	Fügen Sie die Azure-**Anwendungs-ID** der Anwendung, die Sie in Azure registriert haben, im Feld Cloud-Management **Client-ID** ein.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis**. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.
Geheimschlüssel	Fügen Sie den geheimen Schlüssel ein, der beim Erstellen des Azure Service Principal generiert wurde. Dieses Feld erscheint, wenn die **Authentifizierungsmethode Client-Geheimnis** ist.

Azure Enterprise Agreement-Anmeldeinformationen

Azure Enterprise Agreement-Anmeldeinformationen sind für die Abrechnungsfunktionen der Cloud Management-Anwendung erforderlich.

Formularfelder für Azure Enterprise Agreement-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen ein.
Registrierungsnummer	Geben Sie die Registrierungsnummer von Azure ein.
Zugriffsschlüssel	Fügen Sie den von Azure bereitgestellten Zugriffsschlüssel ein.

Cloud Management-Anmeldeinformationen

Dieser Anmeldeinformationstyp ist für Orchestration verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Cloud Management-Anmeldeinformationen

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **Cloud Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Typ	Geben Sie **AWS** an.
Benutzername	Geben Sie den CIM-Benutzernamen ein, um die Tabelle „Anmeldeinformationen“ zu erstellen. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt.
Passwort	Geben Sie das CIM-Passwort ein.
SSH-Passwortsatz	Geben Sie eine einprägsame Phrase für die Schlüsselgenerierung ein. Zum Beispiel könnten Sie **Freitag ist ein guter Tag** eingeben.
Privater SSH-Schlüssel	Geben Sie den privaten SSH-Schlüssel ein.
Authentifizierungsprotokoll	Wählen Sie das **MD5**- oder **SHA**-Authentifizierungsprotokoll aus, mit dem der **Authentifizierungsschlüssel** erstellt wurde.
Authentifizierungsschlüssel	Geben Sie einen von SSH generierten Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Geben Sie eines der folgenden Datenschutzprotokolle ein, das die Verschlüsselung für die **Datenschutzschlüssel** beschreibt: • **3DES** für Triple Data Encryption Standard (DES) • **AES128** für Advanced Encryption Standard (AES) mit 128-Bit-Verschlüsselung • **AES192** für AES mit 192-Bit-Verschlüsselung • **AES256** für AES mit 256-Bit-Verschlüsselung • **DES** für die alte DES-Verschlüsselung
Geben Sie einen zusätzlichen Datenschutzschlüssel ein.	
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Cloud Management-Anmeldeinformationen (Fortsetzung)

Feld	Eingabewert
Klassifizierung	Geben Sie die Anwendungsklassifizierung für die CI-Ermittlung ein.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Anmeldeinformationen für CMP-Knoten (Cloud Management)

Anmeldeinformationen für CMP-Knoten (Cloud Management) verknüpfen Anmeldeinformationen für einen virtuellen Server, die von Cloud Management bereitgestellt werden. Die Cloud Management-Anwendung erstellt diese Anmeldeinformationen automatisch.

Hinweis:
Möglicherweise müssen Sie diese Anmeldeinformationen deaktivieren, wenn Sie sie nicht mehr verwenden möchten, die Prioritätsreihenfolge ändern oder einen MID Server auswählen, der darauf zugreifen darf. Andernfalls müssen Sie diesen Anmeldeinformationstyp nicht manuell erstellen oder ändern.

Formularfelder für Anmeldeinformationen für CMP-Knoten

Feld	Beschreibung
Name	Der automatisch generierte Name basiert auf dem Rechenzentrum, in dem sich der virtuelle Computer befindet.
Aktiv	Ob die Anmeldeinformationen aktiv sind.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für einen bestimmten MID Server oder für alle MID Server verfügbar sind.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Anmeldeinformationen für CMP-Knoten (Fortsetzung)

Feld	Beschreibung
Benutzername und Passwort	Der Benutzername und das Passwort des virtuellen Servers.
SSH-Passwortsatz und Privater SSH-Schlüssel	Der private Schlüssel und der Passwortsatz, der den Schlüssel schützt, falls der virtuelle Server dies erfordert.
Authentifizierungsprotokoll und Authentifizierungsschlüssel	Der private Schlüssel und der Passwortsatz, der den Schlüssel schützt, falls der virtuelle Server dies erfordert.
Datenschutzprotokoll und Datenschutzschlüssel	Wählen Sie das mit dem virtuellen Server verwendete Verschlüsselungsprotokoll aus, und geben Sie den Datenschutzschlüssel ein.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.

Anmeldeinformationen für Cloud Management (CMP)-SSH-Schlüsselpaar

Cloud Management (CMP)-SSH-Schlüsselpaare speichern die Schlüssel, die die Cloud Management-Anwendung automatisch generiert, wenn Benutzer Stapelressourcen bereitstellen.

Hinweis:
Möglicherweise müssen Sie diese Anmeldeinformationen deaktivieren, wenn Sie sie nicht mehr verwenden möchten. Andernfalls müssen Sie diesen Anmeldeinformationstyp nicht manuell erstellen oder ändern.

Formularfelder für Anmeldeinformationen für CMP-SSH-Schlüsselpaare

Feld	Beschreibung
Name	Der automatisch generierte Name
Aktiv	Ob die Anmeldeinformationen aktiv sind.
Öffentlicher SSH-Schlüssel	Der öffentliche Schlüssel
Privater SSH-Schlüssel	Ein sicherer privater Schlüssel, der anstelle eines Passworts für SSH-Anmeldungen verwendet werden kann.

Infoblox-Anmeldeinformationen

Infoblox-Anmeldeinformationen sind erforderlich, um IP-Pools (IPAM) in der Cloud Management-Anwendung einzurichten.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „Infoblox“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für einen bestimmten MID Server oder für alle MID Server verfügbar sind.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert. Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
wapiversion	Geben Sie die Version von wAPI ein, die Sie verwenden.
Benutzername und Passwort	Geben Sie den InfoBlox-Benutzernamen und das Passwort ein.

JDBC-Anmeldeinformationen

Der JDBC-Anmeldeinformationstyp verwaltet den Zugriff auf eine JDBC-Verbindung (Java Database Connectivity). Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „JDBC“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen. Weitere Informationen finden Sie unter Ändern der Anmeldeinformationen auf Nicht-Standard.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifisch **Spezifische MID-Server** wirkt sich nicht auf die MID-Server-Auswahl aus. Sie wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

JMS-Anmeldeinformationen

Der JMS-Anmeldeinformationstyp verwaltet den Zugriff auf einen Java Message Service (JMS). Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Anmeldeinformationsformular für JMS verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen. Weitere Informationen finden Sie unter Ändern der Anmeldeinformationen auf Nicht-Standard.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifisch **Spezifische MID-Server** wirkt sich nicht auf die MID-Server-Auswahl aus. Sie wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

OAuth 2.0-Anmeldeinformationen

OAuth 2.0-Anmeldeinformationen ermöglichen ServiceNow den Zugriff auf Benutzer-Accounts in einem HTTP-Service.

Diese Felder sind im Anmeldeinformationsformular für OAuth 2.0 verfügbar.

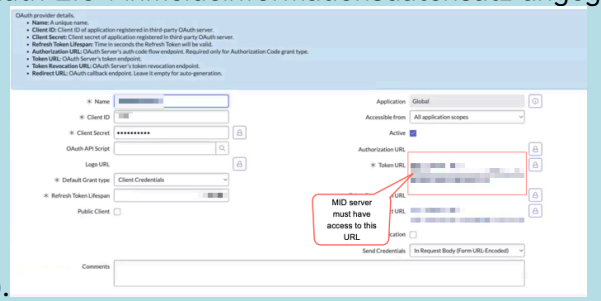
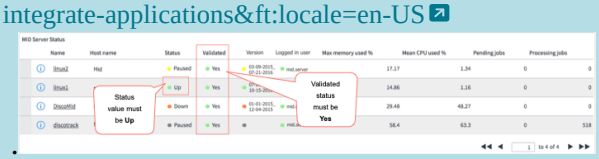
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **OAuth2-Anmeldeinformationen** nennen.
Aktiv	Geben Sie an, ob diese Anmeldeinformationen aktiv sind.
OAuth-Entitätsprofil	Ein OAuth-Profil ist eine Kombination aus einem Gewährungstyp und mindestens einem Bereich.
Verbindung mit Auth-Server über MID-Server herstellen	Verbindet Ihre ServiceNow -Instanz über einen MID-Server] mit einem lokalen OAuth-Server, der sich hinter einer Firewall befindet. Außerdem kann Ihre ServiceNow -Instanz über einen MID-Server mit einem cloud-basierten OAuth-Server verbunden werden. Wenn diese Option aktiviert ist, wird die Anforderung für ein OAuth-Token über MID-Servergesendet. **Wichtig:** • Die Option wird angezeigt, wenn der Wert im Feld **Gewährungstyp** im OAuth-Entitätsprofil auf **Client-Anmeldeinformationen**festgelegt ist. Informationen zum Festlegen eines OAuth-Entitätsprofils für einen OAuth-Drittanbieter finden Sie unter Stellen Sie eine Verbindung zu einem externen OAuth-Provider her. • Wenn Sie das Kontrollkästchen **Verbindung mit Auth-Server über MID Server** herstellen aktivieren, müssen Sie den erforderlichen MID-Server oder MID Servers aus der Liste **Betrifft** Liste identifizieren.
Betrifft	Geben Sie an, ob der Anmeldeinformationsdatensatz für alle MID Server oder einen bestimmten MID Server gilt. Wenn Sie „Spezielle MID Server“ auswählen, fügen Sie die entsprechenden MID Server hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	Wichtig: Stellen Sie sicher, dass Sie diese Überlegungen kennen, wenn Sie das Kontrollkästchen **Verbindung mit Auth-Server über MID-Server** herstellen aktiviert haben. • Stellen Sie sicher, dass alle unter Betrifft ausgewählten MID Servers mit dem Auth-Server kommunizieren können. Dies ist erforderlich, um die Token-Anforderung für die im OAuth-Provider-Datensatz angegebene Token- **URL** auszuführen (die mit dem OAuth-Entitätsprofil verknüpft ist, das im OAuth 2.0-Anmeldeinformationsdatensatz angegeben ist).  • Stellen Sie sicher, dass mindestens ein MID-Server vorhanden ist (im Feld MID Servers, das in **Betrifft**ausgewählt ist) mit den folgenden Konfigurationen: ◦ Der Wert des Felds **Status** ist **In Betrieb**. ◦ Der Wert des Felds **Validiert** lautet **Ja**. ◦ Die Fähigkeit von MID-Server ist auf **REST** oder **ALL**festgelegt. Informationen zum Konfigurieren des MID-Servers finden Sie unter https://www.webstg.servicenow.com/docs/access?context=configure-capabilities&version=washingtondc&pubname=washingtondc-integrate-applications&ft:locale=en-US  . Weitere Informationen zu diesen Status finden Sie unter MID Server dashboard .
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Anmeldeinformationsalias	Geben Sie den Anmeldeinformationsalias an, den Sie an die OAuth 2.0-Anmeldeinformationen binden möchten.
Integrationstyp	Gibt den Integrationstyp für die Anmeldeinformationen an. Rufen Sie eine API einer Drittpartei mit einer OAuth-Anforderung auf, die ein system- oder benutzerspezifisches OAuth-Token generiert. Im Folgenden sind die Integrationstypen aufgeführt: • **System**: Ruft die Token-Informationen basierend auf dem Profil der anfordernden Person ab. • **Persönlich**: Ruft die benutzerspezifischen Tokeninformationen ab. Der Benutzer, der die Sitzung initiiert. Wenn diese **Persönlich** auf der Seite „OAuth-Anfordererprofil“ ausgewählt wird, wird eine zusätzliche Kennzeichnung mit der Bezeichnung „ **Persönlich** “ angezeigt. **Hinweis:** • Auf alle Informationen, die sich auf einen Benutzer beziehen, kann nur mit benutzerspezifischen OAuth-Token mit dem Integrationstyp **Persönlich**zugegriffen werden. • Um das anwenderbezogene Token für die Sitzung zu verwenden, müssen Sie in den Flow-Eigenschaften das Feld **Ausführen als** als **Benutzer, der die Sitzung initiiert**aus.

SAP-Anmeldeinformationen

Der SAP-Anmeldeinformationstyp verwaltet den Zugriff auf SAP JCo-Systeme. Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „SAP“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen. Weitere Informationen finden Sie unter Ändern der Anmeldeinformationen auf Nicht-Standard.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifisch **Spezifische MID-Server** wirkt sich nicht auf die MID-Server-Auswahl aus. Sie wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

SNMP-Anmeldeinformationen

Discovery untersucht viele Arten von Geräten (Switches, Router, Drucker usw.) mithilfe des SNMP-Protokolls. Anmeldeinformationen für SNMP enthalten keinen Benutzernamen, nur ein Passwort, das als *`Community-Zeichenfolge`* bezeichnet wird.

Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und Discovery testet diese automatisch. Geben Sie die entsprechenden SNMP-Anmeldeinformationen ein, falls diese sich von der *`öffentlichen`* Community-Zeichenfolge unterscheiden.

Beim Ermitteln von SNMP werden alle konfigurierten Community-Zeichenfolgen verwendet. Dieses Verhalten gilt nicht für das Ermitteln von SNMPv3.

Die standardmäßige SNMP-Abfrage der Orchestration-Aktivität gibt den Objektbezeichner (OID) eines Geräts zurück und erfordert SNMP-Anmeldeinformationen.

SNMP-Community Anmeldeinformationen

Der Anmeldeinformationstyp der SNMP-Community verwaltet den Zugriff, um viele Arten von Geräten (Switches, Router, Drucker usw.) mithilfe des SNMP-Protokolls zu ermitteln. Dieser Anmeldeinformationstyp ist für Discovery, Service-Mapping und Orchestration verfügbar.

SNMP-Anmeldeinformationen enthalten keinen Benutzernamen, nur ein Passwort (die Community-Zeichenfolge). Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und das System testet diese automatisch. Geben Sie die entsprechenden SNMP-Anmeldeinformationen ein, falls diese sich von der öffentlichen Community-Zeichenfolge unterscheiden.

Diese Felder sind im Anmeldeinformationsformular für SNMP-Community verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen. Weitere Informationen finden Sie unter Ändern der Anmeldeinformationen auf Nicht-Standard.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifisch **Spezifische MID-Server** wirkt sich nicht auf die MID-Server-Auswahl aus. Sie wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

SNMPv3-Anmeldeinformationen

SNMPv3-Anmeldeinformationen akzeptieren ein Datenschutzprotokoll und einen zusätzlichen Datenschutzschlüssel und sind für Discovery und Orchestration verfügbar. Für den externen Speicher in CyberArk können Sie einen Datenschutzkontoschlüssel auswählen.

Diese Felder sind im Anmeldeinformationsformular für SNMPv3 verfügbar.

SNMPv3-Anmeldeinformationsfelder

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SNMP-Community Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder (Fortsetzung)

Feld	Eingabewert
Benutzername	Geben Sie den SNMP-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachfolgende Leerzeichen im Benutzernamen erkennt.
Authentifizierungsprotokoll	Wählen Sie den Authentifizierungstyp aus, der für diese Anmeldeinformationen verwendet werden soll. Die Auswahlmöglichkeiten sind: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Authentifizierungsschlüssel	Geben Sie den mit diesen Anmeldeinformationen zu verwendenden Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Wählen Sie das Verschlüsselungsprotokoll für diese Anmeldeinformationen aus. Die Auswahlmöglichkeiten sind: • 3DES • AES128 • AES192 • AES256 • DES
Datenschutzschlüssel	Geben Sie den Schlüssel ein, der dem ausgewählten Datenschutzprotokoll zugeordnet ist.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für einen externen Anmeldeinformationsanbieter auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Speicher für Berechtigungsnachweise** aktiviert ist.
Datenschutz-Anmeldeinformations-ID	Geben Sie den für SNMPv3-Anmeldeinformationen konfigurierten Datenschutzkonto-Schlüssel in CyberArk ein. Wenn Sie ein Datenschutzprotokoll in CyberArk verwenden, muss dieses Feld denselben Wert aufweisen wie das Feld **Name** für das CyberArk-SNMPv3-Datenschutzkonto. Dieses Feld ist für SNMPv3 nur sichtbar, wenn Sie im Feld **Anmeldeinformationsspeicher-Typ** die Option **CyberArk** auswählen. Wenn Sie keinen Datenschutzschlüssel für CyberArk verwenden, lassen Sie dieses Feld leer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder (Fortsetzung)

Feld	Eingabewert
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld **Nachweis-ID** angezeigt. Eine externe Speicherung von Anmeldeinformationen ist nur verfügbar, wenn das External Credential Storage-Plugin aktiviert und die Ansicht **Externer Speicher** ausgewählt ist.
Anmeldeinformationsspeicher-Typ	Wählen Sie den Provider für den externen Speicher aus. Wählen Sie **CyberArk** nur aus, wenn Sie einen SNMPv3-Datenschutzschlüssel für CyberArk verwenden. Das Feld **Datenschutz-Anmeldeinformations-ID** wird zur Eingabe des Schlüssels angezeigt.
Kontext verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen Kontextwert für diese Anmeldeinformationen hinzuzufügen. Dieses Feld wird in der **Discovery**-Ansicht angezeigt. Kontexte werden derzeit für externe Anmeldeinformationsspeicher nicht unterstützt. **Hinweis:** Ein Kontext ist eine Sammlung von Verwaltungsinformationen, auf die SNMPv3-Anmeldeinformationen zugreifen, in denen auf eine bestimmte OID verwiesen wird. Auf Kontexte wird manchmal verwiesen, damit Informationen über das Gerät gesammelt werden können, auf die mit den normalen Anmeldeinformationen nicht zugegriffen werden kann. Ein Kontext kann vom Hersteller bereitgestellt oder separat konfiguriert werden. Weitere Informationen finden Sie unter Kontextname und Kontext-ID . Wenn Sie über mehrere SNMPv3-Anmeldeinformationen mit demselben Benutzernamen und denselben Schlüsseln verfügen, einige Ihrer Geräte jedoch einen Kontext benötigen und andere nicht, müssen Sie für jedes Gerät separate Datensätze erstellen.
Kontextname	Geben Sie den Kontextnamenswert für diese Anmeldeinformationen ein. Diese Option sollte nur verwendet werden, wenn Sie über Geräte verfügen, die diesen Wert für einen vollständigen Zugriff benötigen. Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Kontext verwenden** aktiviert ist.

SSH-Anmeldeinformationen

Discovery, Orchestration und IntegrationHub untersuchen UNIX - und Linux -Geräte mithilfe von SSH-Anmeldeinformationen, um Befehle über Secure Shell (SSH) auszuführen. SSH-Befehle müssen mit Stammberechtigungen ausgeführt werden, entweder mit Stamm-Anmeldeinformationen oder mit Sudo. Private SSH-Schlüsselanmeldeinformationen bieten zusätzliche Sicherheit.

Stammberechtigungen erteilen

Bevor Sie Stammberechtigungen gewähren, überprüfen Sie Ihre Sicherheitsrichtlinie und -optionen mit dem Sicherheitsteam Ihrer Organisation.

Verwenden Sie eine dieser Methoden, um Benutzern die Ausführung von SSH-Befehlen mit Stammberechtigungen zu ermöglichen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erteilen Sie andere Anmeldeinformationen für Discovery, Orchestration oder IntegrationHub, aber gewähren Sie dem Benutzer in diesen Anmeldeinformationen das Recht, bestimmte Befehle mit Stammberechtigungen über sudo auszuführen. Dies ist eine sichere Methode zum Gewähren eingeschränkter Berechtigungen. Von Discovery, Orchestration oder IntegrationHub wird „sudo“ für jede Probe verwendet, für die der Parameter `must_sudo` auf **true** gesetzt ist (Standardeinstellung ist **false**). Hierfür muss allerdings jedes System so konfiguriert werden, dass es die Ausführung von sudo gestattet. Dies erfolgt durch Bearbeiten der Datei **/etc/sudoers** mit dem Befehl **visudo**.
- Teilen Sie **Stamm**-Anmeldeinformationen zu. Dies sind offenkundig die leistungsstärksten Anmeldeinformationen, unter Sicherheitsgründen aber möglicherweise nicht erstrebenswert. Wenn Discovery, Orchestration oder IntegrationHub über die Stammanmeldeinformationen für UNIX- oder Linux-Systeme verfügen, ist keine weitere Konfiguration erforderlich.

Privilegierte Befehle

Die Plattform bietet standardisierte privilegierte Befehle, die der MID Server verwenden kann, und die Möglichkeit, dem System zusätzliche Befehle hinzuzufügen. Weitere Informationen zur Verwendung von sudo und anderen privilegierten Befehlen finden Sie unter Berechtigte MID Server-Befehle .

Anmeldeinformationstyp „Privater SSH-Schlüssel“

Hinweis:
Die Anmeldeinformationen mit dem privaten SSH-Schlüssel bieten eine größere Sicherheit als die Anmeldeinformationen mit dem SSH-Passwort.

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SSH Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie einen UNIX- oder Linux-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt.
Passwort	Geben Sie das UNIX- oder Linux-Passwort ein. Geben Sie für Anmeldeinformationen vom Typ **Privater SSH-Schlüssel** das sudo-Passwort ein, wenn für den Benutzernamen ein Passwort erforderlich ist.
SSH-Passphrase	Geben Sie einen sicheren SSH-Passwortsatz ein. Dieses Feld ist nur für Anmeldeinformationen mit dem Typ **Privater SSH-Schlüssel** verfügbar.
Privater SSH-Schlüssel	Geben Sie einen sicheren, privaten RSA-, DSA- oder ECDSA-Schlüssel ein, der anstelle eines Passworts für SSH-Anmeldungen verwendet werden kann. Der private Schlüssel muss im richtigen Format eingegeben werden, um sicherzustellen, dass er ordnungsgemäß verschlüsselt ist. Der private Schlüssel muss mit der Zeichenfolge `-----BEGIN` beginnen. Hier ein Beispiel für einen korrekt formatierten privaten RSA-Schlüssel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	-----BEGIN RSA PRIVATE KEY----- MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8E RaStRZsh3IWz+x... ...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i 1Fs -----END RSA PRIVATE KEY----- Beispiel für einen DSA-Schlüssel: -----BEGIN DSA PRIVATE KEY----- MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8E RaStRZsh3IWz+x... ...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i 1Fs -----END DSA PRIVATE KEY----- Und ein Beispiel für einen ECDSA-Schlüssel: -----BEGIN EC PRIVATE KEY----- MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8E RaStRZsh3IWz+x... ...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i 1Fs -----END EC PRIVATE KEY----- Die Now Platform unterstützt private Schlüssel im PEM-Format, das vom OpenSSH-Dienstprogramm ssh-keygen generiert wird. So konvertieren Sie PPK-Schlüssel, die von PuTTY generiert wurden: • Öffnen Sie Ihren privaten Schlüssel in PuTTYGen. • Exportieren Sie sie im OpenSSH-Format aus dem Menü **Konvertierungen** > **Exportieren Sie den OpenSSH-Schlüssel**. • Speichern Sie den neuen OpenSSH-Schlüssel.
SSH-Zertifikat	Geben Sie ein RSA-basiertes OpenSSH-Zertifikat für die SSH-Anmeldung mit Zertifikaten ein. Wenn das Zertifikat eingegeben wird, wird ein privater Schlüssel für die zertifikatsbasierte Authentifizierung verwendet. Diese Authentifizierung wird ab OpenSSH 7.8 unterstützt.
Anmeldeinformationsalias	• Erlauben Sie Flow Designern die Verwendung von Aliassen zur Verwaltung von Verbindungs- und Berechtigungsinformationen. Wenn Sie ein Alias verwenden, müssen Sie nicht mehrere Anmeldeinformations- und Verbindungsinformationsprofile konfigurieren, wenn Sie mehrere Umgebungen verwenden. Wenn sich die Verbindungs- oder Anmeldeinformationen ändern, müssen Sie Aktionen, die die Verbindung verwenden, nicht aktualisieren. Weitere Informationen finden Sie unter Verbindung und Anmeldeinformationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	• Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
MID Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezielle MID-Server** aus dem Feld **Betrifft** auswählen.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
Bestellung	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn Benutzer nach drei fehlgeschlagenen Anmeldeversuchen von den Sicherheitsfunktionen gesperrt werden. Wenn alle Anmeldeinformationen dieselbe Nummer (oder keine) in der Reihenfolge haben, testet Discovery oder Orchestration die Anmeldeinformationen in zufälliger Reihenfolge.

SSH-Anmeldeinformationstyp

Diese Felder sind im SSH-Anmeldeinformationsformular verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	• Erlauben Sie Flow Designern die Verwendung von Aliassen zur Verwaltung von Verbindungs- und Berechtigungsinformationen. Wenn Sie ein Alias verwenden, müssen Sie nicht mehrere Anmeldeinformations- und Verbindungsinformationsprofile konfigurieren, wenn Sie mehrere Umgebungen verwenden. Wenn sich die Verbindungs- oder Anmeldeinformationen ändern, müssen Sie Aktionen, die die Verbindung verwenden, nicht aktualisieren. Weitere Informationen finden Sie unter Verbindung und Anmeldeinformationen. • Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen. Weitere Informationen finden Sie unter Ändern der Anmeldeinformationen auf Nicht-Standard.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Bestellung	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Befehle, die Stammberechtigungen für Discovery, Orchestration und IntegrationHub erfordern

Diese Beispiele setzen voraus, dass der Benutzername **Disco** lautet. Setzen Sie den tatsächlichen Benutzernamen ein, und stellen Sie sicher, dass die Pfade für die Befehle mit den Pfaden im System übereinstimmen.

Hinweis:
Sudo-Befehle funktionieren nicht mit Anmeldeinformationen mit privaten Schlüsseln, da für den Sudo-Befehl kein Passwort angegeben werden muss. Eine Lösung ist das Hinzufügen der Option *NOPASSWD* zur Sudo-Konfiguration. Zum Beispiel könnten Sie Folgendes eingeben: `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind

Befehl	Zweck
HP-UX	
adb	Erfasst CPU-Geschwindigkeit und Speicher. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/adb • **Verwendet von:** Discovery
Alle Linux- und UNIX-Versionen	
chage	Ändert die Anzahl der Tage zwischen Passwortänderungen und dem Datum der letzten Passwortänderung. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/chage • **Verwendet von**: Orchestration und IntegrationHub
chpasswd	Ändert Benutzerpasswörter. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /etc/chpasswd • **Verwendet von**: Orchestration und IntegrationHub
Alle Linux-Versionen	
dmidecode	Sammelt Informationen über die Hardware, einschließlich der Seriennummer des Motherboard.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
	• **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /sbin/dmidecode • **Verwendet von:** Discovery
fdisk	Sammelt die Informationen über Datenträger und Größen im System. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/fdisk -l • **Verwendet von:** Discovery
multipath	Sammelt Gerätezuordnungen für MPIO. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/multipath -ll • **Verwendet von:** Discovery
Linux und Solaris	
dmsetup	Untersucht einen Low-Level-Datenträger. • **Beispiel einer /etc/sudoers-Zeile**: ◦ Disco ALL=(root) /usr/bin/dmsetup table * ◦ Disco ALL=(root) /usr/bin/dmsetup ls • **Verwendet von:** Discovery
Alle UNIX-Versionen	
lsof	Ermittelt die Beziehung zwischen Prozessen und den Verbindungen, die zum System hergestellt werden. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /sbin/lsof • **Verwendet von:** Discovery
oratab	Ermöglicht den Lesezugriff auf die oratab-Datei zum Auffinden von Oracle Home und der Parameterdatei (pfile). • **Beispiel einer /etc/sudoers-Zeile**: Nicht zutreffend • **Verwendet von:** Discovery
Solaris	
iscsiadm	Ruft iSCSI-IQNs ab • **Beispiel einer /etc/sudoers-Zeile**: ${sudo:iscsiadm list target -S} • **Verwendet von:** Discovery
fcinfo	Ruft WWPNs für Ports ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
	• **Beispiel einer /etc/sudoers-Zeile**: ${sudo:fcinfo remote-port -sl -p $port} • **Verwendet von:** Discovery
prtvtoc	Liefert Informationen zu Datenträgerpartitionen. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/prtvtoc • **Verwendet von:** Discovery
pfiles	Wird zum Sammeln von TCP-Verbindungsinformationen verwendet. • Beispiel**einer /etc/sudoers** -Zeile: Disco ALL=(root) /usr/bin/pfiles • **Verwendet von:** Discovery
pgrep	Wird zum Auflisten von Prozess-IDs einer bestimmten Region verwendet, für die Profildateien ausgeführt werden sollen. • Beispiel**einer /etc/sudoers-Zeile** : Disco ALL=(root) /usr/bin/pgrep • **Verwendet von:** Discovery
/usr/bin/ps	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/ps • **Verwendet von:** Discovery
/usr/ucb/ps	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu. Die Verwendung des Befehls `/usr/ucb/ps` ist ab Solaris 11 veraltet. Weil Discovery, Orchestration und IntegrationHub die Verwendung dieses Befehls für alle Solaris-Versionen erfordern, müssen Sie das ucb-Dienstprogramm auf Solaris 11-Systemen manuell installieren. Anweisungen dazu finden Sie in KB0564262 . • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/ucb/ps • **Verwendet von:** Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service Mapping commands requiring a privileged user - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Zugriffsanforderungen für Anmeldeinformationen ohne Root-Berechtigungen

Wenn Sie Discovery Anmeldeinformationen ohne Root-Zugriffsrechte erteilen, müssen Sie die folgenden Zugriffsanforderungen angeben.

Anwendung	Datei oder Verzeichnis	Erforderlicher Zugriff
Apache	httpd.conf	Lesen
Hbase	hbase-site.xml	Lesen
JBoss	jboss-service.xml	Lesen
	JBoss-Stammverzeichnis	Lesen
	web.xml	Lesen
MySQL	my.cnf	Lesen
NGINX	nginx.conf	Lesen
Oracle	oratab	Lesen
	Zugehörige Parameterdateien/Serverparameterdateien	Lesen
Oracle-Listener	lsnrctl	Ausführen
	listener.ora	Lesen
Tomcat	catalina.jar	Lesen
	server.xml	Lesen
	web.xml	Lesen
Unix	/etc/*release	Lesen
	/etc/bashrc	Lesen
	/etc/profile	Lesen
	/proc/cpuinfo	Lesen
	/proc/vmware/sched/ncpus	Lesen
	/var/log/dmesg	Lesen
	APD-Verzeichnis	Lesen
WebSphere	cell.xml	Lesen
	server.xml	Lesen
	serverindex.xml	Lesen

VMware-Anmeldeinformationen

Der VMware-Anmeldeinformationstyp verwaltet den Zugriff auf vCenter-Anmeldeinformationen.

Anwendungen, mit denen auf VMware-Cloud-Ressourcen zugegriffen wird, benötigen Zugriff auf VMware-Anmeldeinformationen. Zum Beispiel ermöglicht der VMware-Anmeldeinformationstyp Discovery die Untersuchung von VMware vCenter, das auf einem Windows-Computer ausgeführt wird, um ESX-Computer,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

virtuelle Computer und Ressourcenpools zu erkennen. VMware Discovery und die Automatisierungs-API (vCenter-API) stellen jetzt die global eindeutige Seriennummer für Computer-CIs bereit. CIM-Anmeldeinformationen sind nicht erforderlich, um den Zugriff auf jeden VMware-Host zu ermöglichen.

Hinweis:
Windows-Anmeldeinformationen sind für vCenter Discoverynicht erforderlich, wenn gültige VMware-Anmeldeinformationen verwendet werden.

Wichtig:
Verwenden Sie Anmeldeinformationen vom Typ **VMware** nicht für Orchestration-Aktivitäten, die auf den einzelnen von vCenter geklonten virtuellen Maschinen Aufgaben ausführen (z. B. Neustarten einer Linux-VM). Für diese Aktivitäten hängt der **Typ** der Anmeldeinformationen vom Betriebssystem der virtuellen Maschine ab (entweder **SSH** oder **Windows**).

Formular für VMWare-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für die VMware-Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzernamen	Geben Sie den Benutzernamen ein, den Sie für Ihr VMware-Konto verwenden. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Die VMware-Anmeldeinformationen müssen in vCenter über die Rolle mit Lesezugriff verfügen.
Passwort	Geben Sie das Passwort für das VMware-Konto ein.
Betrifft	Wählen Sie einen oder mehrere MID Servers aus der Liste der verfügbaren MID Serversaus. Die in diesem Datensatz konfigurierten Anmeldeinformationen sind für MID Servers in dieser Liste verfügbar. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Windows-Anmeldeinformationen

Windows-Anmeldeinformationen ermöglichen den Zugriff auf Windows-Computer. Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen für Anmeldeinformationen

Für Discovery und Orchestration gelten die folgenden Anforderungen für Windows-Anmeldeinformationen:

- Installieren Sie einen MID Server auf einem Windows-Host als Service.
- Fügen Sie einer der folgenden Stellen Windows-Anmeldeinformationen hinzu:
  - Einem Eintrag in der Tabelle „Anmeldeinformationen“ [windows_credentials]
  - Einem MID Server-Service-Account, der als bestimmter Windows-Benutzer oder als Domänen-Account ausgeführt werden soll.

Richtige Berechtigungen erteilen

Um ausreichende Berechtigungen bereitzustellen, müssen Windows-Anmeldeinformationen eines der folgenden sein:

- Ein Domänenbenutzer mit lokalem Administratorzugriff auf Windows-Zielhosts
- Ein lokaler Account mit Administratorrechten und deaktivierter Benutzerzugriffssteuerung (User Access Control, UAC) auf demselben Zielhost
- Ein Benutzer, der die Anforderungen von Windows Probes und Berechtigungen erfüllt (nurDiscovery).
- Ein Benutzer, der die Anforderungen der auszuführenden Orchestration-Aktivität erfüllt (nur Orchestration)

Hinweis:
Es sind keine Anmeldeberechtigungen erforderlich. Account muss NICHT interaktiv sein.

Die Sicherheit beim Gewähren von privilegiertem Zugriff kann durch die Verwendung von JEA-Profilen zum Ausführen von Discoveryverbessert werden. Weitere Informationen finden Sie unter Microsoft Just Enough Administration (JEA) für Discovery .

Arbeitsgruppencomputer

Konfigurieren Sie die MID Server-Anmeldeinformationen für einen dieser Benutzer, um PowerShell-Befehle zum Ermitteln eines Arbeitsgruppencomputers auszuführen:

- Integrierter Administrator-Account auf dem Arbeitsgruppencomputer
- Domänenbenutzer auf dem Arbeitsgruppencomputer

Konfiguration für mehrere Domänen

Stellen Sie sicher, dass Sie die richtigen Namensformate und die richtige MID-Server-Konfiguration verwenden, damit Windows-Anmeldeinformationen für mehrere Domänen genutzt werden können.

Discovery und Orchestration unterstützen Windows-Domänenanmeldeinformationen der Benutzernamensformate **Benutzerprinzipalname** und **Kompatibler Anmeldename**. Zum Beispiel: **Domäne\Benutzername** oder **Benutzername@beispiel.domäne.com**. Sie können Anmeldeinformationen für Windows-Arbeitsgruppen im folgenden Format angeben: ARBEITSGRUPPE\Benutzername.

Hinweis:
Sie können auch einen lokalen Account angeben, indem Sie den Benutzernamen **.** verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese zusätzlichen Aktionen sind erforderlich, damit die Anmeldeinformationen für mehrere Windows-Domänen verwendet werden können.

Bedingung	Zusätzlich erforderliche Aktionen
MID Server-Host in derselben Domäne wie das Windows-Ziel	Keine
MID Server-Host in einer anderen Domäne als das Windows-Ziel	Stellen Sie sicher, dass PowerShell 3.0 (oder höher bis 5.1) auf dem MID Server-Host installiert ist.
MID Server-Host in einer anderen Domäne als das Microsoft SQL Server-Ziel	Weitere Informationen finden Sie unter MSSQL-Servererkennung .

Windows-Anmeldeinformationstyp

Diese Felder sind im Anmeldeinformationsformular für Windows verfügbar:

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen. Weitere Informationen finden Sie unter Ändern der Anmeldeinformationen auf Nicht-Standard.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie den MID Servers an, der diese Anmeldeinformationen im Feld **MID Server** verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifisch **Spezifische MID-Server** wirkt sich nicht auf die MID-Server-Auswahl aus. Sie wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz), in der Discovery diese Anmeldeinformationen beim Versuch, sich bei -Geräten anzumelden, testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

Windows-Anmeldeinformationen für den MID Server konfigurieren

Konfigurieren Sie den MID Server für die Verwendung der Anmeldeinformationen seines Windows-Service oder der Anmeldeinformationen aus der Tabelle „Anmeldeinformationen“ [discovery_credentials].

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Konfigurieren Sie den MID Server für die Verwendung von Anmeldeinformationen aus dem Service-Account des MID Servers.
   a. Legen Sie die Anmeldeinformationen für den Windows MID Server-Service konfigurieren auf einen Benutzer fest, der die Berechtigungsanforderungen erfüllt.
   b. Stellen Sie sicher, dass der Benutzername den Namensformatanforderungen entspricht.
   c. Füllen Sie die entsprechenden Felder im Formular aus.
   d. Stellen Sie sicher, dass die Anmeldeinformationen den Anforderungen der Domäne entsprechen.
2. Konfigurieren Sie den MID Server für die Verwendung der Anmeldeinformationen aus der Tabelle „Anmeldeinformationen“ [discovery_credentials].
   a. Fügen Sie der Tabelle „Anmeldeinformationen“ [windows_credentials] Windows-Anmeldeinformationen hinzu.
      - Stellen Sie sicher, dass jede Anmeldeinformation die Berechtigungsanforderungen erfüllt.
      - Stellen Sie sicher, dass jeder Benutzername den Namensformatanforderungen entspricht.
      - Stellen Sie sicher, dass jede Anmeldeinformation den Windows-Domänenanforderungen entspricht.
   b. **Wahlweise:** Konfigurieren Sie den MID Server für die Verwendung von Powershell, indem Sie den Parameter mid.use_powershell auf **true**setzen.
   Weitere Informationen finden Sie unter MID Server konfigurieren .
   c. Aktivieren Sie das Kontrollkästchen Windows MID Server-Servicekonto, um Anmeldeinformationen zu erstellen, die das Windows MID Server-Servicekonto darstellen, das als bestimmtes Windows-Benutzer- oder Domänenkonto ausgeführt werden soll.

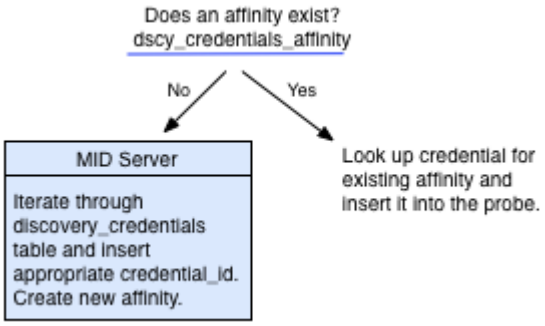
Berechtigungsaffinität für Discovery und Orchestration

Berechtigungsaffinität ist eine Verbindung zwischen einer Reihe von Anmeldeinformationen und einem Gerät im Netzwerk.

Beim ersten Versuch von Discovery oder Orchestration auf ein Gerät zuzugreifen, werden alle verfügbaren Anmeldeinformationen getestet, bis die richtigen gefunden werden. Nach der Ermittlung der Anmeldeinformationen für ein Gerät erstellen Discovery und Orchestration anhand der Tabelle „Anmeldeinformationsaffinität“ [dscy_credentials_affinity] eine Affinität zwischen den Anmeldeinformationen und dem Gerät. Bei allen nachfolgenden Ermittlungen oder Orchestration-Aktivitäten wird versucht, die Anmeldeinformationen in dieser Tabelle einem Gerät zuzuordnen, für das eine Affinität besteht. Wenn sich die Anmeldeinformationen für ein Gerät ändern, testen Discovery und Orchestration alle verfügbaren Anmeldeinformationen erneut, bis sie eine neue Affinität herstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungsaffinitäts-Diagramm



Hinweis:
Wenn Orchestration und Discovery installiert sind und der Anmeldeinformationsalias aktiviert ist, können mehrere Affinitäten vorhanden sein. In diesem Fall sucht die Plattform nach Anmeldeinformationen für jede Affinität und fügt die Anmeldeinformation für die Affinität mit der niedrigsten Reihenfolgenummer in die Probe ein.

Behebung von Fehlern bei Anmeldeinformationen

Überprüfen Sie den Abschnitt `<credentials_debug>` des ECC-Warteschlangen-Payload, um Probleme mit Anmeldeinformationen zu beheben.

Bestimmte Probes unterstützen das Debuggen von Anmeldeinformationen. Beim Debugging von Anmeldeinformationen wird der Abschnitt `<credentials_debug>` in das Payload eingefügt, das der MID Server an die Instanz-ECC-Warteschlange zurückgibt. Sie können den Abschnitt `<credentials_debug>` anzeigen, um detaillierte Informationen zur Suche nach Anmeldeinformationen zu erhalten.

Der Abschnitt `<credentials_debug>` erscheint im Payload, wenn:

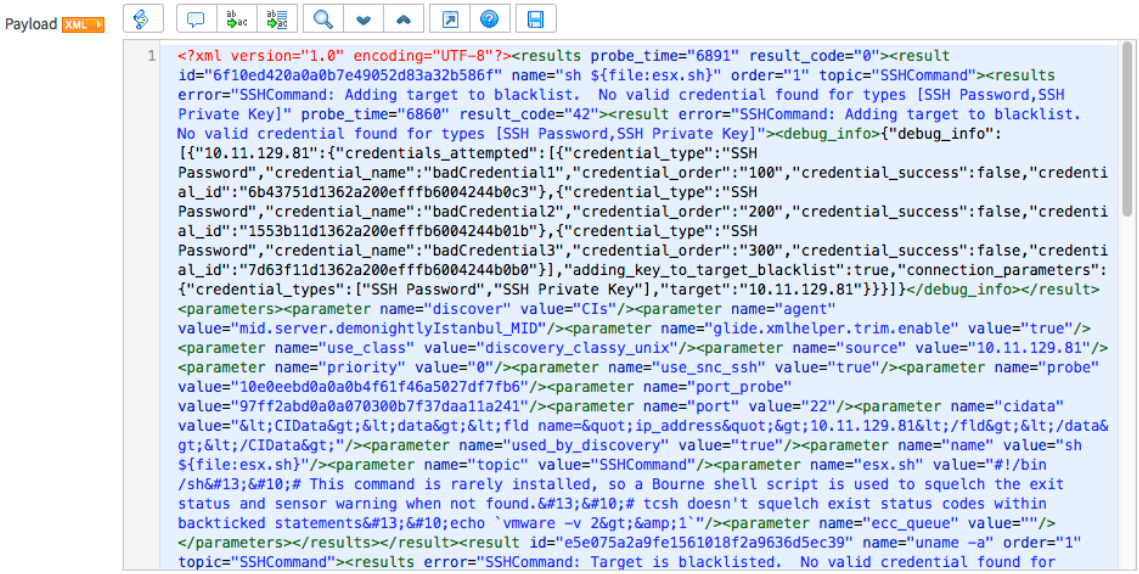
- Fehler bei den Anmeldeinformationen für die Probe „WMIRunner“, „ PowerShell “, „ JMS“ oder „SSHCommand“ .
- Setzen Sie den Parameter *`credentials_debug`* für die WMIRunner-, PowerShell- oder SSHCommand-Proben auf **true**. Wenn Sie diesen Parameter auf „true“ setzen, wird der Abschnitt `<credentials_debug>` auch dann angezeigt, wenn die Suche nach Anmeldeinformationen erfolgreich war.

Der Abschnitt `<credentials_debug>` enthält:

- Informationen über die Suche nach Anmeldeinformationen, z. B. Anmeldeinformationstypen, Tags und Affinitäten.
- Die Ziel-IP-Adresse.
- Informationen zu allen Anmeldeinformationen (in der Reihenfolge), die der MID Server verwendet hat, einschließlich Typ, Klassifizierung, Tag, Name, Sys-ID und externe Anmeldeinformations-ID, falls vorhanden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Payload mit ungültigen Anmeldeinformationen



Für den PowerShell-Parameter werden Details angezeigt:

- Wenn die lokalen MID Server-Anmeldeinformationen verwendet wurden, nachdem alle Windows-Anmeldeinformationen fehlgeschlagen sind.
- Wenn die Anmeldeinformationen übersprungen wurden, da Sie versuchen, denselben Computer zu erkennen, auf dem sich der MID Server befindet.
- Wenn der Parameter mid.powershell.use_credentials auf truefestgelegt ist.

Details werden für SSHCommand angezeigt:

- Wenn die Suche nach Anmeldeinformationen übersprungen wurde, da die Ziel-IP ausgeschlossen ist.
- Wenn die Ziel-IP der Ausschlussliste hinzugefügt wurde.

Hinweis:
Der MID Server speichert IP-Adressen für fehlgeschlagene Anmeldeinformationssuchen in einer Ausschlussliste im Cache-Speicher. Diese Ausschlussliste gibt an, auf welche Geräte der MID Server nicht mehr zugreifen soll. IP-Adressen werden der Ausschlussliste hinzugefügt, nachdem alle Anmeldeinformationen fehlgeschlagen sind. Die IP-Adressen werden entweder nach fünf Minuten aus dem Cache der Ausschlussliste gelöscht, wenn der MID Server neu gestartet wird oder wenn die Anmeldeinformationsdatensätze in der Instanz aktualisiert werden.

Externer Anmeldeinformationsspeicher

Eine Instanz kann Anmeldeinformationen, die von Discovery, Orchestration und Service-Mapping verwendet werden, in einem externen Anmeldeinformations-Repository anstatt direkt in einem ServiceNow-Anmeldeinformationsdatensatz speichern.

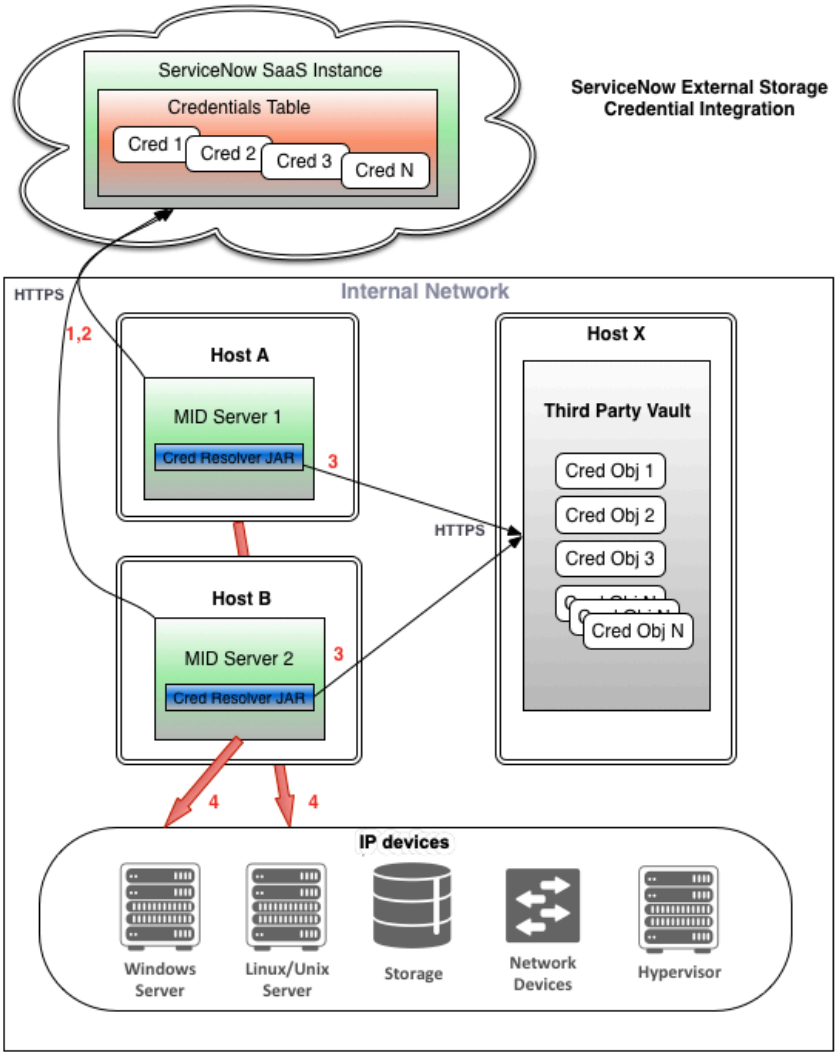
Die Instanz verwaltet einen eindeutigen Bezeichner für jede Anmeldeinformation, den Anmeldeinformationstyp (z. B. SSH, SNMP oder Windows) und alle Berechtigungsaffinitäten. Der MID Server erhält den Nachweis-Bezeichner von der Instanz und löst dann mithilfe einer vom Kunden bereitgestellten JAR-Datei den Bezeichner aus dem Repository in verwendbare Anmeldeinformationen auf. Derzeit unterstützt die ServiceNow®-Plattform CyberArk-Tresor als externen Anmeldeinformationsspeicher.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Architektur des externen Anmeldeinformationsspeichers

Architektur des externen Anmeldeinformationsspeichers



Prozessablauf für Anmeldeinformationen

Der MID Server ruft Anmeldeinformationen anhand dieses Prozesses aus einem externen Speicher ab:

1. Der MID Server lädt Anmeldeinformationsobjekte aus der ServiceNow-Tabelle „Anmeldeinformationen“ [discovery_credentials] herunter, die die entsprechende Nachweis-ID aus dem Zieltresor enthalten.
2. Wenn eine Probe oder ein Muster von Discovery - oder Orchestration -Jobs ausgeführt wird, fordert der MID Server die Anmeldeinformationen an, indem Informationen wie Anmeldeinformations-ID, Ziel-IP-Adresse und Anmeldeinformationstyp an die Java-JAR-Datei des Credential Resolver übergeben werden. Die Details zum richtigen Anmeldeinformationsobjekt, das aus dem Tresor abgerufen werden soll, werden vom Credential Resolver bestimmt.

   Viele Resolver für Anmeldeinformationen wie CyberArk rufen eine Anwendung auf, die von einem Drittanbieter für Vault bereitgestellt wird, der auf demselben Computer wie der MID Server ausgeführt wird. Diese Anwendung kann häufig so konfiguriert werden, dass sie Anmeldeinformationen zwischenspeichert und den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cache aktualisiert, wenn sich Anmeldeinformationen im Tresor ändern. Dies ist sehr wichtig, um unnötige Netzwerkaufrufe beim Tresor zu vermeiden, wenn der MID Server Anmeldeinformationen anfordert. Der Credential Resolver (unter Verwendung der optionalen Lieferantenanwendung, falls vorhanden) ruft den Tresor auf, um den tatsächlichen Benutzernamen, das Passwort usw. abzurufen.

Für vordefinierte Resolver für Anmeldeinformationen (heute nur CyberArk) speichert der MID Server Anmeldeinformationen nur für bis zu mehrere Sekunden im Cache des MID Server-Prozessspeichers. Dies bedeutet, dass der MID Server mehrere Anforderungen an den Credential Resolver für dieselben Anmeldeinformationen stellen kann, auch wenn ein einzelnes Gerät erkannt wird. Wenden Sie sich an Drittanbieter, um Informationen zur Zwischenspeicherung von Implementierungen für andere Resolver für Anmeldeinformationen zu erhalten.

3. Der MID Server führt die Probe mit den entsprechenden Anmeldeinformationen aus.

Hinweis:
Berechtigungsaffinitäten gelten weiterhin. Der Mechanismus bleibt derselbe, da der einzige wirkliche Unterschied aus Sicht des MID Servers darin besteht, dass die tatsächlichen Anmeldeinformationen (Benutzername und Passwort) aus dem Tresor einer Drittpartei stammen.

Protokollierung des externen Anmeldeinformationsspeichers

Der MID Server gibt Protokollnachrichten über den externen Anmeldeinformationsspeicher aus.

Wenn vom Repository beim Versuch, eine Anforderung für Anmeldeinformationen zu lösen, ein Fehler festgestellt wird, werden vom MID-Server Protokollnachrichten mit diesem Präfix ausgegeben: `Problem with client's CredentialResolver:` (Problem mit dem CredentialResolver des Clients).

Mit dem externen Anmeldeinformationsspeicher installierte Komponenten

Geschäftsregel

Mit der Geschäftsregel für externe Anmeldeinformationsspeicher werden die folgenden Aufgaben ausgeführt, wenn ein Administrator Änderungen an der Eigenschaft „Externen Anmeldeinformationsspeicher aktivieren“ vornimmt:

- Ändern der Ansicht für die Datensatzliste und des Formulars für Anmeldeinformationen in die Ansicht „Externer Speicher“. In dieser Ansicht können Benutzer die Spalte **„Anmeldeinformations-ID** “ in der Liste anzeigen.
- Weist den MID-Server an, den Cache für Anmeldeinformationen zu aktualisieren. Dies dient der Vorbereitung auf eine geänderte Vorgehensweise zum Abrufen von Anmeldeinformationen.

Eigenschaft

Eine Eigenschaft mit der Bezeichnung Externen Anmeldeinformationsspeicher aktivieren [com.snc.use_external_credentials] aktiviert oder deaktiviert das Plugin „Externer Anmeldeinformationsspeicher“, nachdem es aktiviert wurde. Die Eigenschaft befindet sich in **Discovery-Definition** > **Eigenschaften** und **Orchestration** > **MID-Server-Eigenschaften**, und sind aktiviert, wenn Sie das Plugin aktivieren.

Wenn Sie die Speicherung von externen Anmeldeinformationen mit der Systemeigenschaft deaktivieren, werden alle externen Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in der Instanz vom System automatisch auf inaktiv festgelegt. Wenn Sie die Funktion mit dieser Eigenschaft erneut aktivieren, setzt das System die externen Anmeldeinformationsdatensätze nicht auf „Aktiv“ zurück. Sie müssen jeden Anmeldeinformationsdatensatz manuell erneut aktivieren.

Fordern Sie einen externen Anmeldeinformationsspeicher für Discovery und Orchestration an

Das Plugin „Externer Anmeldeinformationsspeicher“ ist auf Anfrage erhältlich.

Vorbereitungen

Erforderliche Rolle: admin

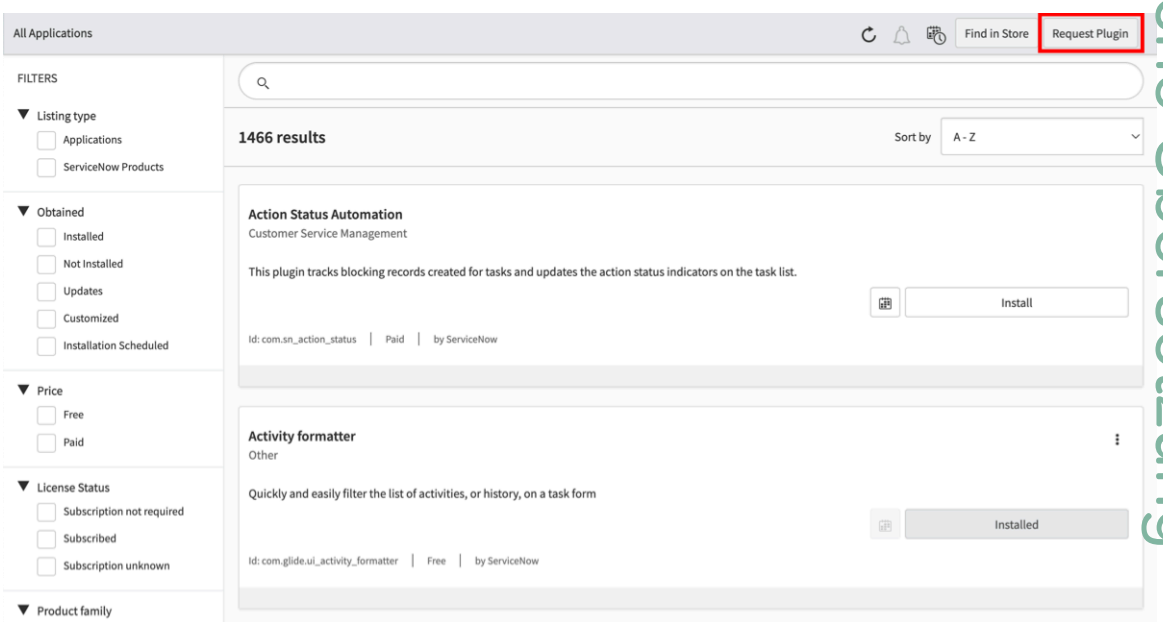
Warum und wann dieser Vorgang ausgeführt wird

Es gibt zwei Möglichkeiten, ein Plugin anzufordern:

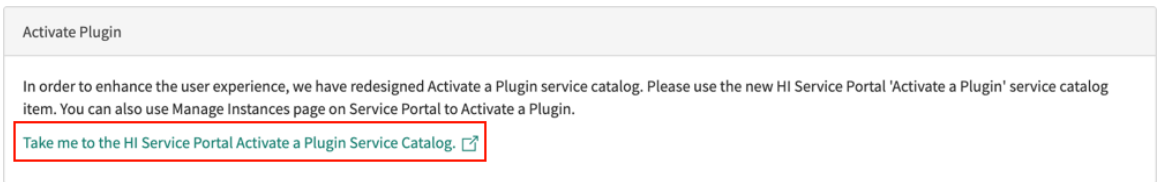
- Greifen Sie direkt auf den Servicekatalog Now Support zu, indem Sie auswählen **Alle** > **Servicekatalog** > **Plugin aktivieren** auf Now Support.
- Greifen Sie über die Seite „Alle Anwendungen“ in Ihrer Instanz auf den Now Support-Servicekatalog zu, indem Sie die folgenden Schritte ausführen.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

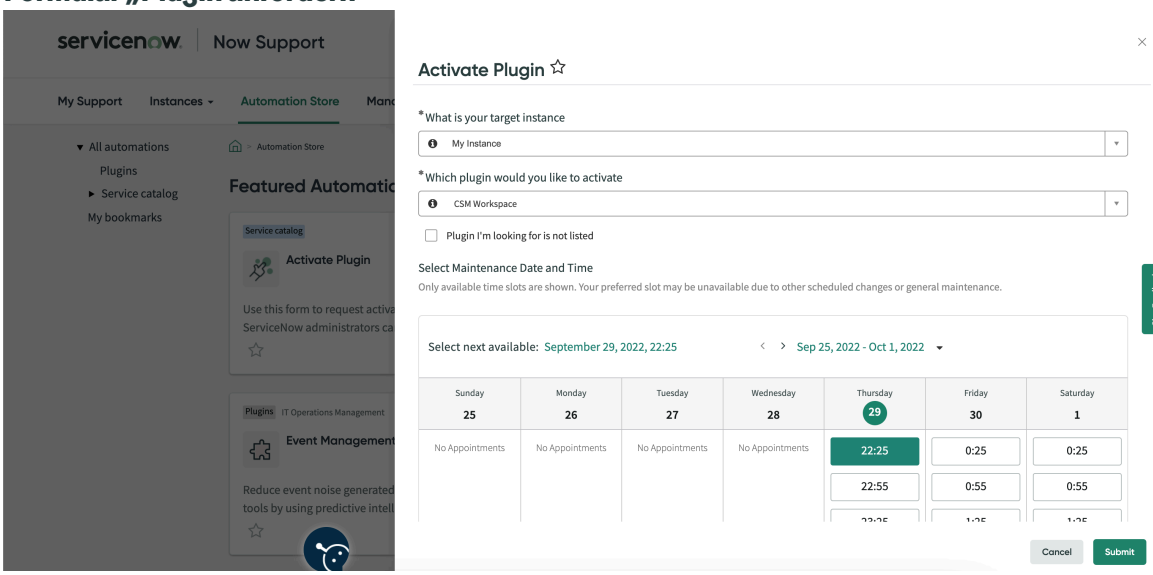
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
Weitere Informationen zum Anfordern eines Plugins finden Sie unter Plugins aus dem Servicekatalog anfordern [KB0751715] im Now Support Knowledge Base.

Konfiguration des externen Anmeldeinformationsspeichers

Konfigurieren Sie Ihre Instanz so, dass Anmeldeinformationen von einem Remote-Repository abgerufen werden.

Bei diesen Verfahren wird davon ausgegangen, dass Sie bereits ein externes Repository mit den Anmeldeinformationen konfiguriert haben, die Sie schützen möchten. Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss über die JAR-Datei den tatsächlichen Anmeldeinformationen im Repository zugeordnet werden.

Hinweis:
ServiceNow unterstützt zwei externe Tresore gleichzeitig: einen standardmäßigen CyberArk-Anmeldeinformations-Resolver und einen benutzerdefinierten externen Anmeldeinformations-Resolver. Beim Erstellen eines benutzerdefinierten CyberArk-Anmeldeinformations-Resolvers wird weiterhin der zweite benutzerdefinierte externe Tresor verwendet, und es können keine zusätzlichen benutzerdefinierten externen Tresore verwendet werden.

Führen Sie zum Konfigurieren des externen Anmeldeinformationsspeichers die folgenden Aufgaben in der angegebenen Reihenfolge aus.

JAR-Datei zum Auflösen der Anmeldeinformationen erstellen

Erstellen Sie eine JAR-Datei, um die vom MID Server gesendeten Anmeldeinformationen in tatsächliche Anmeldeinformationen aus dem Repository aufzulösen.

Vorbereitungen
Erforderliche Rolle: agent_admin oder admin

Stellen Sie sicher, dass alle Anmeldeinformationen enthalten sind, die die Instanz erwartet, wie z. B. der private Schlüssel.

So erstellen Sie eine JAR-Datei zum Auflösen von Anmeldeinformationen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Verwenden Sie entweder die Vorlagen, die auf dem GitHub ServiceNow bereitgestellt werden, oder die Java-Beispieldatei.

> **⚠ Vorsicht:**
> Diese Beispiele sind nur als Vorlage gedacht. Verwenden Sie diesen Code **NICHT** in der Produktion, ohne ihn für Ihre Umgebung zu ändern.

a. Laden Sie die Open Source-JAR-Dateien mit Anweisungen aus dem GitHub ServiceNow herunter:

- Resolver für externe HashiCorp-Anmeldeinformationen
- CyberArk – Resolver für externe Anmeldeinformationen

b. Verwenden Sie die folgende Java-Beispieldatei als Vorlage, und passen Sie sie an Ihre Umgebung an:

Example

```
package com.snc.discovery;

import java.util.*;
import java.io.*;

/**
 * Basic implementation of a CredentialResolver that uses a properties file.
 */

public class CredentialResolver {

 private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
 private static String DEFAULT_PROP_FILE_PATH = "C:\\dummycredentials.properties";

 // These are the permissible names of arguments passed INTO the resolve()
 // method.

 // the string identifier as configured on the ServiceNow instance...
 public static final String ARG_ID = "id";

 // a dotted-form string IPv4 address (like "10.22.231.12") of the target
 // system...
 public static final String ARG_IP = "ip";

 // the string type (ssh, snmp, etc.) of credential as configured on the
 // instance...
 public static final String ARG_TYPE = "type";

 // the string MID server making the request, as configured on the
 // instance...
 public static final String ARG_MID = "mid";

 // These are the permissible names of values returned FROM the resolve()
 // method.

 // the string user name for the credential, if needed...
 public static final String VAL_USER = "user";
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
// the string password for the credential, if needed...
public static final String VAL_PSWD = "pswd";

// the string pass phrase for the credential if needed:
public static final String VAL_PASSPHRASE = "passphrase";

// the string private key for the credential, if needed...
public static final String VAL_PKEY = "pkey";

// the string authentication protocol for the credential, if needed...
public static final String VAL_AUTHPROTO = "authprotocol";

// the string authentication key for the credential, if needed...
public static final String VAL_AUTHKEY = "authkey";

// the string privacy protocol for the credential, if needed...
public static final String VAL_PRIVPROTO = "privprotocol";

// the string privacy key for the credential, if needed...
public static final String VAL_PRIVKEY = "privkey";


private Properties fProps;

public CredentialResolver() {
}

private void loadProps() {
 if(fProps == null)
  fProps = new Properties();

 try {
  String propFilePath = System.getenv(ENV_VAR);
  if(propFilePath == null) {
   System.err.println("Environment var "+ENV_VAR+" not found. Using default file:
"+DEFAULT_PROP_FILE_PATH);
   propFilePath = DEFAULT_PROP_FILE_PATH;
  }

  File propFile = new File(propFilePath);
  if(!propFile.exists() || !propFile.canRead()) {
   System.err.println("Can't open "+propFile.getAbsolutePath());
  }
  else {
   InputStream propsIn = new FileInputStream(propFile);
   fProps.load(propsIn);
  }

 //fProps.load(CredentialResolver.class.getClassLoader().getResourceAsStream("dummycred
entials.properties"));
 } catch (IOException e) {
  System.err.println("Problem loading credentials file:");
  e.printStackTrace();
 }
}
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
/**
 * Resolve a credential.
 */
public Map resolve(Map args) {
 loadProps();
 String id = (String) args.get(ARG_ID);
 String type = (String) args.get(ARG_TYPE);
 String keyPrefix = id+"."+type+".";

 if(id.equalsIgnoreCase("misbehave"))
  throw new RuntimeException("I've been a baaaaaaaaad CredentialResolver!");

 // the resolved credential is returned in a HashMap...
 Map result = new HashMap();
 result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
 result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
 result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
 result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
 result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
 result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
 result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
 result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));

 System.err.println("Error while resolving credential id/type["+id+"/"+type+"]");

 return result;
}


/**
 * Return the API version supported by this class.
 */
public String getVersion() {
 return "1.0";
}

public static void main(String[] args) {
 CredentialResolver obj = new CredentialResolver();
 obj.loadProps();

 System.err.println("I spy the following credentials: ");
 for(Object key: obj.fProps.keySet()) {
  System.err.println(key+": "+obj.fProps.get(key));
 }

}
}
```

JAR-Datei zum Auflösen der Anmeldeinformationen importieren

Importieren Sie eine JAR-Datei, um die vom MID Server gesendeten Nachweis-Bezeichner in tatsächliche Anmeldeinformationen aus dem Repository aufzulösen.

Vorbereitungen
Erforderliche Rolle: agent_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach dem Erstellen der JAR-Datei importieren Sie sie in die Instanz; dort kann der MID Server darauf zugreifen.

Prozedur

1. Kopieren Sie nach dem Erstellen der JAR- und Eigenschaftendateien die Eigenschaftendatei auf den MID Server.
2. Navigieren zu **MID-Server** > **JAR-Dateien**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die folgenden Felder aus:

Feld	Beschreibung
Name	Ein eindeutiger und beschreibender Name zum Identifizieren der Datei in der Instanz.
Version	Eine Versionsnummer für die Datei, sofern verfügbar.
Quelle	Speicherort der JAR-Datei zu Referenzzwecken. Quellinformationen werden vom System nicht verwendet.
Beschreibung	Kurzbeschreibung der JAR-Datei und ihres Zwecks in der Instanz.

5. Klicken Sie auf das Büroklammersymbol im Banner, und hängen Sie die JAR-Datei an den Datensatz an.

Example

Eine JAR-Datei anhängen

6. Klicken Sie auf **Absenden**.
7. Starten Sie den MID-Server-Service neu.
   Die Plattform stellt die JAR-Datei jedem MID Server zur Verfügung, der für die Kommunikation mit der Instanz konfiguriert ist.

Nachweis-Bezeichner konfigurieren

Konfigurieren Sie den Nachweis-Bezeichner in der Instanz.

Vorbereitungen

Erforderliche Rolle: admin

Überprüfen Sie Folgendes:

- Das Plugin Externer Anmeldeinformationsspeicher muss aktiv sein.
- Die Discovery-Eigenschaft Externen Anmeldeinformationsspeicher aktivieren ist aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Berechtigungen** oder **Orchestration** > **Berechtigungen**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie einen Anmeldeinformationstyp aus.
4. Aktivieren Sie das Kontrollkästchen **Externer Anmeldeinformationsspeicher**.
   Die Felder **Benutzername** und **Passwort** werden ausgeblendet, und das Feld **Anmeldeinformations-ID** sowie das Menü **„Speicherung** von Anmeldeinformationen“ werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Menü Tresor für Anmeldeinformationsspeicher entweder Keine, den **CyberArk** -Tresor oder einen benutzerdefinierten Tresor für den externen Anmeldeinformationsspeicher aus.

> **Hinweis:**
>
> Wenn CyberArk Vault ausgewählt ist, wird das **Suchschlüsselmenü** mit vier Suchschlüsseloptionen angezeigt: Anmeldeinformations-ID, Suchschlüssel, FQDN, Alle oben genannten. Wenn Sie Alle auswählen, kann dies die Leistung beeinträchtigen, da ein mehrmaliger Zugriff auf den Tresor erforderlich ist.

a. Um einen benutzerdefinierten Tresor für externe Anmeldeinformationen zu verwenden, navigieren Sie in der -Instanz zu Vault-Konfigurationen [vault_configuration.list].

b. Erstellen Sie einen neuen Datensatz mit einem Namen, der einer importierten JAR-Datei für einen benutzerdefinierten Resolver für Anmeldeinformationen zugeordnet ist.

Informationen zum Erstellen eines benutzerdefinierten Tresors zum Speichern externer Anmeldeinformationen finden Sie in den Verfahren JAR-Datei zum Auflösen der Anmeldeinformationen erstellen und JAR-Datei zum Auflösen der Anmeldeinformationen importieren.

6. Füllen Sie das Formular „Anmeldeinformationen“ mit den Feldern aus der folgenden Tabelle aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Dies ist die ID, die an die Java-Klasse in der Parameterzuordnung übergeben wird: `public static final String ARG_ID = "id";` Der MID-Server verwendet diesen Identifier, um die tatsächlichen Anmeldeinformationen im Repositorium aufzulösen. **Hinweis:** Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Tag	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn das Plugin „Externer Anmeldeinformationsspeicher“ aktiviert ist.
Anmeldeinformationsspeicher-Tresor	Wählen Sie den Tresor für den externen Anmeldeinformationsspeicher aus einer Liste der verfügbaren Tresore aus. Das Menü besteht aus Datensätzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	aus den Vault-Konfigurationen [vault_configuration.list]. Neue Datensätze können hinzugefügt werden und Namen verwenden, die benutzerdefinierten JAR-Dateien für die Auflösung von Anmeldeinformationen zugeordnet sind. Informationen zum Erstellen eines benutzerdefinierten Tresors zum Speichern externer Anmeldeinformationen finden Sie in den Verfahren JAR-Datei zum Auflösen der Anmeldeinformationen erstellen und JAR-Datei zum Auflösen der Anmeldeinformationen importieren.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Bestellung	Geben Sie die Reihenfolge ein, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto weiter oben werden diese Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn Benutzer nach drei fehlgeschlagenen Anmeldeversuchen von den Sicherheitsfunktionen gesperrt werden. Wenn alle Anmeldeinformationen dieselbe Nummer (oder keine) in der Reihenfolge haben, testet Discovery oder Orchestration die Anmeldeinformationen in zufälliger Reihenfolge.

7. Klicken Sie auf **Absenden**.

Nachweis-Bezeichner für AWS konfigurieren

Konfigurieren Sie Ihre Instanz so, dass Anmeldeinformationen von einem Remote-Repository abgerufen werden.

Vorbereitungen

Erforderliche Rolle: cloud_admin

Vergewissern Sie sich, dass die folgenden Plugins aktiv sind und der MID Server installiert wurde:

- Discovery [com.snc.discovery]
- Cloud Provisioning and Governance [com.snc.cloud.mgmt]
- Externer Anmeldeinformationsspeicher [com.snc.discovery.external_credentials]

Warum und wann dieser Vorgang ausgeführt wird

Bei diesen Verfahren wird davon ausgegangen, dass Sie bereits ein externes Repository mit den Anmeldeinformationen konfiguriert haben, die Sie schützen möchten. Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss über die JAR-Datei den tatsächlichen Anmeldeinformationen im Repository zugeordnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Berechtigungen**.
2. Wählen Sie Anmeldeinformationen aus, die Ihr externer Anbieter für die Speicherung von Anmeldeinformationen unterstützt.
3. Füllen Sie das Formular mithilfe der Felder aus der Tabelle aus.

Feld	Beschreibung
Name	Ein eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel „Amazon Web Services“.
Betrifft	Wählen Sie die MID Server aus, die diese Anmeldeinformationen verwenden können. Die Auswahlmöglichkeiten sind **Alle MID Server** oder **Bestimmte MID Server**. Wenn Sie Letzteres auswählen, wird das Feld **MID Server** angezeigt.
Aktiv	Kontrollkästchen zum Aktivieren oder Deaktivieren der Anmeldeinformationen.
AWS-Konto	Geben Sie Ihre AWS-Konto-ID ein, wenn sich Ihre AWS-Anmeldeinformationen bei einem externen Speicheranbieter befinden.
MID-Server	Wählen Sie einen oder mehrere MID Server aus, die diese Anmeldeinformationen verwenden können.
Anmeldeinformations-ID	Geben Sie den Namen ein, unter dem diese Anmeldeinformationen beim Anbieter für externe Anmeldeinformationsspeicher gespeichert werden.
Datenschutz-Anmeldeinformations-ID	Geben Sie den Namen eines SNMPv3-Datenschutzschlüssels von CyberArk ein. Dieses Feld ist für SNMPv3 nur sichtbar, wenn Sie im Feld **Anmeldeinformationsspeicher-Typ** die Option **CyberArk** auswählen. Wenn Sie keinen Datenschutzschlüssel für CyberArk verwenden, lassen Sie dieses Feld leer.
Anmeldeinformationsalias	Wählen Sie einen Alias für diese Anmeldeinformationen aus, der bestimmte Verhaltensweisen enthält. Weitere Informationen finden Sie unter Anmeldeinformationsaliasse für Discovery.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld **Nachweis-ID** angezeigt. Wenn dieses Kontrollkästchen nicht sichtbar ist, klicken Sie auf das Menüsymbol in der Kopfzeile, und wählen Sie **Ansicht** > **Externer Speicher** aus dem Kontextmenü.
Anmeldeinformationsspeicher-Typ	Wählen Sie **CyberArk** nur aus, wenn Sie einen SNMPv3-Datenschutzschlüssel für CyberArk verwenden. Das Feld **Datenschutz-Anmeldeinformations-ID** wird zur Eingabe des Schlüssels angezeigt.

4. Klicken Sie auf **Absenden**.

CyberArk Integration des Anmeldeinformationsspeichers

Die Integration von MID-Server mit dem Tresor [CyberArk ermöglicht die Ausführung von ServiceNow® Orchestration, ServiceNow® Discoveryund ServiceNow® Service-Mapping, ohne Anmeldeinformationen für die Instanz zu speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einführung in CyberArk

Das ProduktCyberArk Application Identity Management (AIM) verwendet die Lösung Privileged Account Security, um die Notwendigkeit des Speicherns von Anwendungspasswörtern in Anwendungen, Skripts oder Konfigurationsdateien zu beseitigen und die zentrale Speicherung, Protokollierung und Verwaltung dieser hochsensiblen Passwörter innerhalb des CyberArk zu ermöglichen. Tresor. Dieser Ansatz ermöglicht es Organisationen, die internen und behördlichen Anforderungen hinsichtlich der periodischen Ersetzung von Passwörtern zu erfüllen und Aktivitäten zu überwachen, die mit allen Arten von privilegierten Identitäten verbunden sind, ob vor Ort oder in der Cloud.

Die Instanz verwaltet einen eindeutigen Bezeichner für jeden Anmeldeinformationstyp, den Anmeldeinformationstyp (z. B. SSH, SNMP oder Windows) und alle Anmeldeinformationsaffinitäten. MID-Server ruft den Bezeichner der Anmeldeinformationen, den Anmeldeinformationstyp und die IP-Adresse von der Instanz ab und verwendet dann den Tresor CyberArk, um diese Elemente in verwendbare Anmeldeinformationen aufzulösen. Der Anmeldeinformations-Resolver kann auch den Hostnamen fqdn suchen und die umgekehrte DNS-Suche verwenden, um fqdn abzurufen.

Die CyberArk -Integration erfordert das ServiceNow® Plugin „External Credential Storage“, das in verfügbar ist **Systemdefinitionen** > **Plugins**. Der AIM/API-Client MID-Server und CyberArk müssen auf demselben Computer installiert sein. Version 12.0.1 und höher von CyberArk Application Access Manager (AAM) wird unterstützt.

Mit CyberArk installierte Komponenten

- **Business-Regel**: Die Business-Regel „Externer Anmeldeinformationsspeicher“ führt die folgenden Aufgaben aus, wenn ein Administrator Änderungen an der Eigenschaft „Externer Anmeldeinformationsspeicher“ vornimmt:
  - Ändern der Ansicht für die Datensatzliste und des Formulars für Anmeldeinformationen in die Ansicht „Externer Speicher“. In dieser Ansicht können Benutzer die Spalte „Nachweis-ID“ in der Liste sehen.
  - Weist den MID-Server an, seinen Cache für nicht externe Anmeldeinformationen zu aktualisieren, um eine Änderung der Art und Weise vorzubereiten, wie Anmeldeinformationen abgerufen werden.
- **Systemeigenschaft**: Die Eigenschaft „Externen Anmeldeinformationsspeicher aktivieren“ [com.snc.use_external_credentials] aktiviert oder deaktiviert das Plugin „Externer Anmeldeinformationsspeicher“, nachdem es aktiviert wurde. Diese Eigenschaft befindet sich in**Discovery-Definition** > **Eigenschaften**und**Orchestration** > **MID-Server-Eigenschaften**, und sind aktiviert, wenn Sie das Plugin aktivieren.

Hinweis:
Wenn Sie die Einsatzbereitschaft des externen Anmeldeinformationsspeichers über die Systemeigenschaft widerrufen, setzt das System automatisch alle externen Anmeldeinformationen in der Instanz auf „Inaktiv“. Wenn Sie die Funktion mithilfe dieser Eigenschaft erneut in Einsatzbereitschaft versetzen, setzt das System die externen Anmeldeinformationsdatensätze nicht wieder auf „Aktiv“. Sie müssen jeden Anmeldeinformationsdatensatz manuell neu aktivieren.

Unterstützte Anmeldeinformationstypen

Die CyberArk -Integration unterstützt die folgenden ServiceNow -Anmeldeinformationstypen:

- GCP
- Azure

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CIM
- JMS
- SNMP-Forum
- SNMPv3
- Basisauth.
- SSH-Schlüsselpaar
- Privater SSH-Schlüssel (mit Schlüssel, Passphrase und Passwort)
- VMware
- Windows
- Applicative-Anmeldeinformationen

Hinweis:
Um die Integration CyberArk mit dem GCP-Anmeldeinformationstyp zu verwenden, müssen Sie die JAR-Datei für den externen Anmeldeinformationsspeicher ändern. Weitere Informationen finden Sie unter ServiceNow GCP Credential Resolver mit CyberArk .

Now Platform -Funktionen, die diese Netzwerkprotokolle verwenden, unterstützen auch die Verwendung von Anmeldeinformationen, die in einem CyberArk Tresor gespeichert sind.

Vom Netzwerkprotokoll unterstützte Anmeldeinformationen

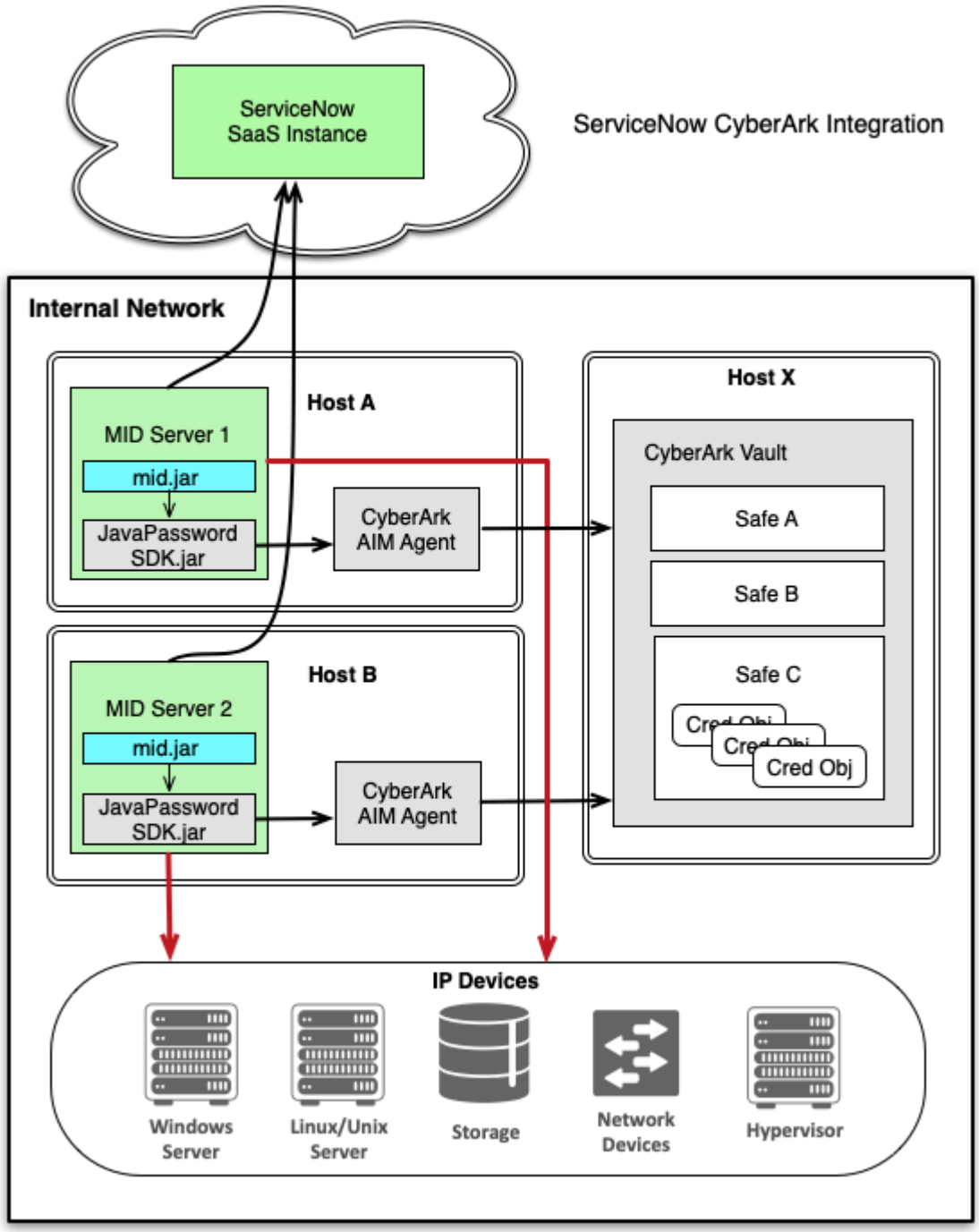
Netzwerkprotokoll	ServiceNow® Flow Designer Unterstützung	Orchestration -Unterstützung
SOAP	SOAP-Schritt	Erstellen Sie eine SOAP Web Service-Aktivität mit Überschreibungen der Basic Authentication
REST	REST-Schritt	Erstellen Sie eine REST-Webserviceaktivität mit Überschreibungen der Basic Authentication
JDBC	JDBC-Schritt	JDBC-Aktivität
SSH	SSH-Schritt	SSH-Aktivität
PowerShell	PowerShell-Schritt	PowerShell-Aktivität
SFTP	SFTP-Schritt	SFTP-Aktivität
JMS		JMS-Aktivität

Wichtig:
Sie können Anmeldeinformationen, die in einem CyberArk Tresor gespeichert sind, und ein benutzerdefiniertes externes Speichersystem für Anmeldeinformationen nicht mit demselben MID-Serververwalten. Der AIM/API-Client MID-Server und CyberArk müssen auf demselben Computer installiert sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CyberArk-Architektur

CyberArk -Speicherarchitektur



Hinweis:
CyberArk verwendet die `mid.jar` -Datei des Basissystems zum Auflösen von Anmeldeinformationen.

Wie MID-Server mit Konten von Windows umgeht

Bei der Suche nach Anmeldeinformationen wird zunächst versucht, die angegebene Anmeldeinformations-ID mit einem vorhandenen Wert im Feld **Name** des Tresors

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CyberArk abzugleichen. Wenn eine Übereinstimmung gefunden wird, werden die Anmeldeinformationen ausgegeben. Wenn keine Übereinstimmung gefunden wird, versucht die Anmeldeinformationssuche, mithilfe der IP-Adresse eine Übereinstimmung zu finden. Wenn bei der IP-Adresssuche mehrere Anmeldeinformationen übereinstimmen, z. B. Windows und Tomcat auf demselben Server, schlägt die Suche fehl. Um dieses Problem zu vermeiden, legen Sie den Parameter *ext.cred.type_specifier* in der Datei MID-Server config.xml auf „ **true** “ fest, um CyberArk zur Rückgabe von Anmeldeinformationen zu zwingen, die sowohl dem Anmeldeinformationstyp als auch der IP-Adresse entsprechen. Beispiel: Wenn eine IP-Adresse von Windows und Tomcatgemeinsam genutzt wird, gibt der Anmeldeinformationstyp Windows nur die Anmeldeinformationen Windows zurück.

Konfiguration der CyberArk-Integration

Diese Verfahren umfassen sowohl Konfigurationsaufgaben für CyberArk als auch ServiceNow, einschließlich Verweisen auf die entsprechende CyberArk-Dokumentation.

Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss dem Anmeldeinformationsnamen im CyberArk-Tresor zugeordnet sein. Bei der Suche nach Anmeldeinformationen ermittelt der MID Server die Anmeldeinformationen durch den Abgleich des Nachweis-Bezeichners mit einem Namen im Tresor, der eindeutig sein muss. Wenn der Nachweis-Bezeichner leer ist, ermittelt der MID Server die Anmeldeinformationen anhand der IP-Adresse. Um die Anmeldeinformationen anhand der IP-Adresse zu ermitteln, prüft das System den Anmeldeinformationstyp, um sicherzustellen, dass sich an dieser Adresse nur eine Anmeldeinformation dieses Typs befindet. Ein Beispiel hierfür könnte die Ausführung eines Windows-Servers und von vCenter auf derselben IP-Adresse sein. Um die strengen Anforderungen für Anmeldeinformationen in einer SSH-Umgebung zu unterstützen, können Sie in einem MID Server-Konfigurationsparameter angeben, dass der angeforderte Anmeldeinformationstyp dem von CyberArk zurückgegebenen Typ entsprechen muss.

Hinweis:
Das Feld **Anmeldeinformations-ID** ist in allen Fällen mit Ausnahme von SNMPv3 das einzige Feld, das erforderlich ist, um Ihre Anmeldeinformationen CyberArk zuzuordnen. Das Feld **ID für Datenschutz-Anmeldeinformationen** ist optional und nur erforderlich, wenn SNMPv3-Anmeldeinformationen und ein Datenschutzprotokoll für die Anmeldeinformationen verwendet werden. Unter CyberArk-Nachweis-Bezeichner konfigurieren finden Sie weitere Details.

Um Ihre Instanz so zu konfigurieren, dass Anmeldeinformationen von einem CyberArk-Tresor abgerufen werden, führen Sie diese Aufgaben in der angegebenen Reihenfolge aus.

CyberArk-Tresor konfigurieren und die AIM-API installieren

Konfigurieren Sie den CyberArk-Tresor so, dass er dem MID Server Zugriff gewährt, und installieren Sie die CyberArk AIM-API auf dem MID Server-Computer.

Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass das Plugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. Version 12.0.1 und höher von CyberArk Application Access Manager (AAM) wird unterstützt.

Prozedur

1. Konfigurieren Sie den CyberArk-Tresor mit der Anwendungs-ID und den Authentifizierungsdetails, die alle MID Server, die Anmeldeinformationen anfordern, verwenden.
   Weitere Informationen finden Sie im Handbuch „CyberArk Credential Provider and ASCP Implementation“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Konfigurieren Sie CyberArk so, dass der MID Server auf den Tresor zugreifen kann, indem Sie in CyberArk die App-ID `ServiceNow_MID_Server` erstellen.

b. Stellen Sie sicher, dass jede Anmeldeinformation, die der MID Server benötigt, Zugriff auf die App-ID `ServiceNow_MID_Server` erhält.

> **Hinweis:**
> Sie können die Standard-App-ID **ServiceNow_MID_Server** in der MID-Server-Datei config.xml mit dem Parameter ext.cred.app_id überschreiben. Wenn Sie den Wert in diesem Parameter ändern, müssen Sie einen entsprechenden Wert im Tresor konfigurieren.

2. Installieren Sie den Credential Provider von CyberArk, einschließlich der AIM-API, auf jedem Computer, der einen für den Zugriff auf den Anmeldeinformationsspeicher verwendeten MID Server-Service hostet.
3. Stellen Sie CyberArk-Accounts bereit, und legen Sie Berechtigungen für den Anwendungszugriff fest. Weitere Informationen finden Sie im Handbuch „CyberArk Privileged Account Security Implementation“.
   a. Erstellen Sie in CyberArk-Passwortsafe die privilegierten Accounts, die von Discovery, Orchestration oder Service Mapping für den Zugriff auf verschiedene Geräte benötigt werden, und stellen Sie sicher, dass diese Accounts zu den Safes gehören, in denen die erforderlichen Anmeldeinformationen gespeichert sind.
   b. Fügen Sie den Credential Provider und die Anwendungsbenutzer als Mitglieder der Passwortsafes hinzu, in denen die Anwendungspasswörter gespeichert werden.

CyberArk-JAR-Datei importieren

Importieren Sie die CyberArk-Datei „JavaPasswordSDK.jar“ in die Instanz, damit der MID Server darauf zugreifen kann.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Bevor Sie mit diesem Verfahren beginnen, müssen Sie CyberArk so konfigurieren, dass der MID Server auf Anmeldeinformationen zugreifen kann. Stellen Sie sicher, dass die CyberArk AIM-API auf jedem Server installiert ist, auf dem sich ein MID Server befindet, der für den Zugriff auf den Tresor verwendet wird.

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie diesen Prozess auch, wenn die Datei „JavaPasswordSDK.jar“ bereits auf dem MID Server vorhanden ist.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **JAR-Dateien**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, indem Sie die Felder in der Tabelle verwenden.

Formularfelder für die JAR-Datei

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name zur Identifizierung der Datei in der Instanz.
Version	Optionale Versionsnummer für die Datei, sofern verfügbar.
Quelle	Provider der JAR-Datei. Quellinformationen werden vom System nicht verwendet.
Beschreibung	Optionale Kurzbeschreibung der JAR-Datei und ihres Zwecks in der Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Hängen Sie die JAR-Datei an diesen Datensatz an.
   Die AIM-Datei JavaPasswordSDK.jar wird mit den AIM-SDK-Installationsdateien geliefert und befindet sich normalerweise auf dem MID-Server im AIM-Installationsverzeichnis unter <Installationsverzeichnis>/CyberArk/ApplicationPasswordSdk.
5. Klicken Sie auf **Absenden**.
6. Starten Sie den MID-Server-Service neu.
   Die Plattform stellt die JAR-Datei jedem MID Server zur Verfügung, der für die Kommunikation mit der Instanz konfiguriert ist.

MID Server für CyberArk konfigurieren

Konfigurieren Sie die Datei config.xml, um dem MID Server Zugriff auf den CyberArk-Tresor zu gewähren.

Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie dieses Verfahren beginnen, müssen Sie die Datei JavaPasswordSDK.jar in die Instanz importieren.

Prozedur

Konfigurieren Sie den MID Server manuell. Fügen Sie eine MID Server-Parameterdatei mit diesen Parametern hinzu.

Diese Konfiguration kann nicht von der Instanz vorgenommen werden.

Erforderliche Konfigurationsparameter

Parameter	Wert	Beschreibung
ext.cred.safe_folder	NameOfFolder	Ordner für alle Suchen nach Anmeldeinformationen. Zum Beispiel: **root**.
ext.cred.use_cyberark	true	Boolescher Parameter, der angibt, dass dieser MID Server in CyberArk integriert ist.

Optionale Konfigurationsparameter

Parameter	Wert	Beschreibung
ext.cred.safe_timeout	5 (Sek.)	Zeitüberschreitung in Sekunden für jede Suche nach Anmeldeinformationen im Tresor.
ext.cred.safe_name	NameOfSafe	Standardname des Safes, der für alle Suchen nach Anmeldeinformationen verwendet wird. Wenn sich Parameter in mehreren Safes befinden, kann die Nachweis-ID im Format *<safeName>:<CredentialID>* angegeben werden. Bei dieser Konfiguration wird das Feld **NameOfSafe** ignoriert. Wenn für alle externen Anmeldeinformationen die Nachweis-IDs in diesem Format angegeben sind, lassen Sie das Feld **NameOfSafe** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert	Beschreibung
		Hinweis: Standardmäßig ist das Trennzeichen in diesem Format ein Doppelpunkt. Um ein beliebiges Zeichen als Trennzeichen zuzuweisen, fügen Sie diese Zeile der Datei CredMap.properties hinzu: safe.cred.split.string = <Zeichenfolge>.
ext.cred.app_id	ServiceNow_MID_Server	Gibt die App-ID an, mit der dem MID-Server die Berechtigung zum Zugriff auf den CyberArk-Tresor erteilt wird. Der Standardwert **ServiceNow_MID_Server** muss im CyberArk-Tresor definiert sein. Mit diesem Parameter können Sie den Standardwert überschreiben und eine eigene App-ID angeben. Wenn Sie die App-ID in diesem Parameter bearbeiten, müssen Sie CyberArk entsprechend konfigurieren.
ext.cred.type_specifier	Wahr	Erzwingt, dass die IP-Adressen-Suche Anmeldeinformationen ausgibt, die sowohl mit der CyberArk-Plattform-ID als auch mit der IP-Adresse übereinstimmen. Wenn zum Beispiel eine IP-Adresse von Windows und Tomcat gemeinsam genutzt wird, geben Anmeldeinformationen mit einer Plattform-ID, die mit **Win** beginnt, nur die Windows-Anmeldeinformationen zurück. Wenn dieser Parameter auf „true“ festgelegt ist, sucht CyberArk nach Plattform-IDs, die mit Folgendem beginnen: • Win: Windows • Unix: SSH • VMWare: VMware
ext.cred.check_ssh_type	false	Ist der Wert auf „true“ festgelegt, müssen die von CyberArk zurückgegebenen SSH-Anmeldeinformationen mit dem angeforderten Anmeldeinformationstyp übereinstimmen. Wenn beispielsweise normale SSH-Anmeldeinformationen mit Benutzername/Passwort angefordert werden und nur SSH-Schlüssel verfügbar sind, schlägt die Suche nach Anmeldeinformationen fehl.

CyberArk für SNMPv2-Anmeldeinformationen konfigurieren

Wenn Ihr System SNMPv2 verwendet, können Sie eine spezielle Datei erstellen, um das Attribut in Anmeldeinformationen der Community-Zeichenfolge zuzuordnen.

Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie dieses Verfahren beginnen, müssen Sie den MID Server für den Zugriff auf den CyberArk-Tresor konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Wenn die Community-Zeichenfolge im Passwortfeld der CyberArk-Anmeldeinformationen angezeigt wird, ist es nicht erforderlich, dieses Verfahren auszuführen.

SNMPv2 wird in CyberArk nicht nativ unterstützt. Wenn Ihre Organisation benutzerdefinierte SNMPv2-Anmeldeinformationen erstellt hat, bei denen die Community-Zeichenfolge nicht im Passwortfeld der Anmeldeinformationen angezeigt wird, verwenden Sie dieses Verfahren, um das Attribut in den Anmeldeinformationen der Community-Zeichenfolge zuzuordnen.

Prozedur

1. Erstellen Sie in einem Texteditor eine Datei mit dem Namen CredMap.properties mit diesem Code: `SNMPv2.Community=attribute_name`
2. Speichern Sie die Datei im Verzeichnis /agent Ihrer MID Server-Installation.
   Beim Suchen nach Anmeldeinformationen versucht der MID Server, dieses Attribut für die Anmeldeinformationen zu finden. Wenn das Attribut nicht gefunden wird, sucht der MID Server im Passwortfeld. Wenn das Passwortfeld leer ist, schlägt die Suche nach Anmeldeinformationen fehl.

CyberArk-Nachweis-Bezeichner konfigurieren

Erstellen Sie den eindeutigen Schlüssel, mit dem CyberArk bestimmte Anmeldeinformationen im externen Repository identifizieren kann.

Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie mit diesem Verfahren beginnen, müssen Sie das Plugin „Externer Anmeldeinformationsspeicher“ aktivieren und die Systemeigenschaft com.snc.use_external_credentials auf „true“ setzen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Berechtigungen** oder **Orchestration** > **Berechtigungen**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie aus der Liste der Anmeldeinformationstypen einen Typ aus, der den externen Speicher von CyberArk unterstützt.
4. Füllen Sie das Formular mit den Feldern des Anmeldeinformationstyps aus.
5. Aktivieren Sie das Kontrollkästchen **Externer Anmeldeinformationsspeicher**.
   Die Felder **Benutzername** und **Passwort** werden durch das Feld **Nachweis-ID** ersetzt.

   Hinweis:
   Wenn das Kontrollkästchen nicht sichtbar ist, klicken Sie auf das Menüsymbol in der Kopfzeile, und wählen Sie **Ansicht** > **Externer Speicher**.

6. Geben Sie im Feld **Nachweis-ID** einen Ausdruck in einem der folgenden Formate ein:
   - Wenn sich alle Anmeldeinformationen im selben Safe befinden, konfigurieren Sie diesen Safe-Namen in der MID-Server-Datei config.xml mit dem Parameter ext.cred.safe_name, und geben Sie die Nachweis-ID nur mit dem Namen als **<Nachweis-ID>** an.
   - Um die Anmeldeinformationen für eine Plattform zu benennen, die sich in einem bestimmten Safe befinden, definieren Sie die Nachweis-ID als **<Safe>:<Nachweis-ID>:<Plattform-ID>**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn sich die Anmeldeinformationen in mehreren Safes befinden, geben Sie die Nachweis-ID in diesem Format an: **<Safe>:<Nachweis-ID>**.
- Wenn CyberArk die Anmeldeinformationen anhand der IP-Adresse suchen soll, verwenden Sie einen alternativen Safe, und geben Sie die Nachweis-ID in diesem Format an: **<Safe>:**.
- Wenn CyberArk die Anmeldeinformationen für eine alternative Plattform-ID im selben Safe suchen soll, verwenden Sie dieses Format: **::<Plattform-ID>**
- Wenn CyberArk die Anmeldeinformationen in einem konfigurierten Safe anhand der IP-Adresse anstelle der Nachweis-ID suchen soll, lassen Sie dieses Feld leer. Dies ist die Best Practice für Installationen, bei denen jeder Server über eindeutige Anmeldeinformationen verfügt. Ohne diese Art von Suche müssen Sie in Ihrer Instanz für jeden Server in der Umgebung einen Nachweis-ID-Datensatz erstellen.

Hinweis:
Die Anmeldeinformations-ID muss mit dem Wert im Feld **Name** für das CyberArk-Konto übereinstimmen. Das Feld **„Anmeldeinformations-ID" darf maximal** 180 Zeichen lang sein.

7. Wenn Sie SNMPv3-Anmeldeinformationen in CyberArk speichern und das Datenschutzprotokoll und den Datenschutzschlüssel verwenden, konfigurieren Sie die ID wie folgt:

   a. Wählen Sie im Feld **Typ des Anmeldeinformationsspeichers** die **Option CyberArk aus**. Das Feld **Datenschutz-Anmeldeinformations-ID** wird angezeigt.

   b. Geben Sie den **Namen** des CyberArk-SNMPv3-Datenschutzkontos in das Feld **Datenschutz-Anmeldeinformations-ID** ein.

8. Klicken Sie auf **Absenden**.

AWS-Anmeldeinformationen in einem CyberArk-Tresor konfigurieren

Konfigurieren Sie Ihren CyberArk-Tresor mit den AWS-Anmeldeinformationen, die für die Verwendung durch Ihre Instanz abgerufen werden sollen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Speichern Sie die Anmeldeinformationen im CyberArk-Tresor als SSH-Schlüssel. Wenn Sie den Zugriff auf den Tresor in Ihrer Instanz konfigurieren, muss der Name, den Sie dem SSH-Schlüssel geben, auch als Nachweis-ID verwendet werden.

Prozedur

1. Wechseln Sie in CyberArk zu **Accounts** > **Fügen Sie den SSH-Schlüssel hinzu**.
2. Geben Sie die folgenden Informationen ein:

CyberArk-Anmeldeinformationen

Feld	Wert
Gerätetyp	Wählen Sie **Cloud Service** aus.
Plattformname	Wählen Sie **Amazon Web Services - AWS - Access Keys** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
AWS Zugangsschlüssel-ID	Geben Sie den AWS-Zugriffsschlüssel, wie von AWS bereitgestellt, ein.
AWS IAM-Benutzername	Geben Sie den AWS IAM-Benutzernamen ein, wie Sie ihn in CyberArk konfiguriert haben.
Passwort	Geben Sie den geheimen AWS-Zugangsschlüssel, wie von AWS bereitgestellt, ein.
Name	Geben Sie einen Namen für diesen Schlüssel ein.

3. Klicken Sie auf **Save**.

Nächste Maßnahme
Wenn Sie dies noch nicht getan haben, erstellen Sie in Ihrer Instanz einen Nachweis-Identifier, um den Zugriff auf den CyberArk-Tresor zu konfigurieren. Weitere Einzelheiten finden Sie unter Zugriff auf den externen Anmeldeinformationsspeicher für AWS konfigurieren.

Konfigurieren Sie Azure-Anmeldeinformationen für einen CyberArk-Tresor

Konfigurieren Sie Ihren CyberArk-Tresor mit den Azure-Anmeldeinformationen, die zur Verwendung durch Ihre Instanz abgerufen werden sollen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Um Azure-Anmeldeinformationen zu speichern, erstellen Sie zuerst eine Azure-Anmeldeinformationsvorlage im CyberArk-Tresor. Dieser Prozess muss für den Tresor nur einmal abgeschlossen werden.

Prozedur
1. Melden Sie sich im Administrationsmodus bei CyberArk an.
2. Navigieren Sie zur Registerkarte **Administration**.
3. Bearbeiten Sie in der **SystemkonfigurationPlatform Management**.
4. Navigieren Sie zu **Cloud-Provider Vorlage**, und duplizieren Sie sie.
5. Bearbeiten Sie die Vorlage für Azure-Anmeldeinformationen.
6. Fügen Sie die folgenden zwei Eigenschaften hinzu:
   - *`Name`* als *`Username`* und *`Display Name`* als *`Client ID`*
   - *`Name`* als *`Address`* und *`DisplayName`* als *`Tenant ID`*
7. Wenden Sie die Änderungen an.
8. Navigieren Sie zum Abschnitt **Account**, und wählen **Sie Account hinzufügen**aus.
9. Wählen Sie **Sicher aus**.
10. Legen Sie den **Gerätetyp** auf **Cloud-Service fest**.
11. Wählen Sie die Azure-Vorlage aus, die zuvor bearbeitet wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Füllen Sie die Informationen in die Felder **Client-ID**, **Mandanten-ID**und **Passwort** aus.
13. Wählen Sie **Speichern**.

Authentifizierungsalgorithmen

Überprüfen Sie die Identität des Absenders mithilfe von Authentifizierungsalgorithmen

Lassen Sie Integrationsschritte zur Authentifizierung bei Webservices zu, die komplexe oder nicht standardmäßige Verbindungs- oder Anmeldeinformationsmechanismen erfordern. Ordnen Sie Anmeldeinformations- und Verbindungsaliassen Authentifizierungsalgorithmen zu, um die Notwendigkeit der manuellen Konfiguration von Integrationsschritten zu reduzieren oder zu beseitigen.

Sie können einen Authentifizierungsalgorithmus verwenden, um benutzerdefinierte Authentifizierungsdaten für Ihre Integrationsschritte zu generieren. Integrationsschritte können diese dynamischen Daten verwenden, um benutzerdefinierte Artefakte zu erstellen, die für die Authentifizierung beim Ziel-Webservice erforderlich sind. Beispielsweise kann ein REST-Schritt einen Authentifizierungsheader, Abfrageparameter oder ein Token erstellen.

Authentifizierungsalgorithmen unterstützen die folgenden Schritte:

- Schritt „Verbindungsinformationen abrufen“
- REST-Schritt
- SOAP-Schritt

Weitere Informationen finden Sie unter Integrationsschritte

Typen des Authentifizierungsalgorithmus

- **Amazon Signature Version 4**: Dies ist ein vorgefertigter Authentifizierungsalgorithmus für die Verbindung mit Amazon Web Services.
- **Benutzerdefinierte Authentifizierung**: Dies ist eine Vorlage, mit der Entwickler ihre eigenen Authentifizierungsalgorithmen erstellen können.

Weitere Informationen zur Konfiguration des Authentifizierungsalgorithmus finden Sie unter Konfigurieren Sie einen Authentifizierungsalgorithmus.

Skripts

Instanzauthentifizierungsskripts befinden sich in Instanzskripts der Tabelle `sys_script_include`.

Instanzauthentifizierungsskripts

RequestAuthInternal	Schreibgeschütztes Skript in Instanz, das die Generierung einer AWS V4-Signatur oder einer benutzerdefinierten Authentifizierung unterstützt, die mit der ausgehenden Anforderung gesendet wird.
RequestAuthAWSV4Signer	Skript, das RequestAuthInternal erweitert, um den Unterzeichner zum Generieren der AWS V4-Signatur zu implementieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanzauthentifizierungsskripts (Fortsetzung)

RequestAuthTwitterSigner	Skript, das RequestAuthInternal erweitert, um den Unterzeichner zu implementieren, um eine Twitter-Signatur mit OAuth 1.0a zu generieren.
RequestAuthSampleCustomSigner	Beispielskript, das „RequestAuthInternal“ erweitert, um zu verstehen, wie ein benutzerdefinierter Unterzeichner für die Instanz geschrieben wird.

MID-Authentifizierungsskripts befinden sich im MID-Skripts-Teil der Tabelle *ecc_agent_script_include*.

MID-Authentifizierungsskripts

RequestAuthInternal	Schreibgeschütztes Skript auf MID, das die Generierung einer AWS V4-Signatur oder einer benutzerdefinierten Authentifizierung unterstützt, die mit der ausgehenden Anforderung gesendet wird.
RequestAuthAWSV4MIDSigner	Skript, das RequestAuthInternal erweitert, um den Unterzeichner zum Generieren der AWS V4-Signatur zu implementieren.
RequestAuthTwitterSigner	Skript, das RequestAuthInternal erweitert, um den Unterzeichner zu implementieren, um eine Twitter-Signatur mit OAuth 1.0a zu generieren.
RequestAuthSampleMidCustomSigner	Beispielskript, das „RequestAuthInternal“ erweitert, um zu verstehen, wie ein benutzerdefinierter Unterzeichner für MID geschrieben wird.

JavaScript-APIs

Im Folgenden finden Sie die JavaScript-APIs für den Authentifizierungsalgorithmus.

- Auth-Anmeldeinformationen
- HTTPRequestAuthedData
- HTTPRequestData
- RequestAuthAPI

Konfigurieren Sie einen Authentifizierungsalgorithmus

Konfigurieren Sie einen Authentifizierungsalgorithmus, damit Sie ausgehende HTTP-Anforderungen signieren können.

Vorbereitungen

Sie sollten eine Skripteinbindung konfigurieren, bevor Sie einen Authentifizierungsalgorithmus konfigurieren.
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Ausgehender Anforderungstyp.
Beschreibung	Beschreibung dessen, was Ihr Algorithmus tut.
Anwendung	Bereich, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie in der Tabelle „Skripteinbindungen“ auswählen
MID-Authentifizierungsskript	Skript, das Sie in der Tabelle „MID Server-Skripteinbindungen“ [Discovery-Ansicht] auswählen.

3. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen Amazon Signaturbasierten benutzerdefinierten Algorithmus

Generieren Sie die signaturbasierten Amazon Daten, die für die Authentifizierung bei einem Webservice erforderlich sind, indem Sie ein Skript ausführen.

Vorbereitungen

- JavaScript-Wissen
- REST-Wissen
- Wissen der Ziel-Webservice-API
- Wissen über Verbindungen, Anmeldeinformationen und Aliasse
- Erforderliche Rolle: Developer

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie für die Authentifizierung einen Alias für Verbindungen und Anmeldeinformationen und einen auf Amazon Signature Version 4 basierenden Algorithmus.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

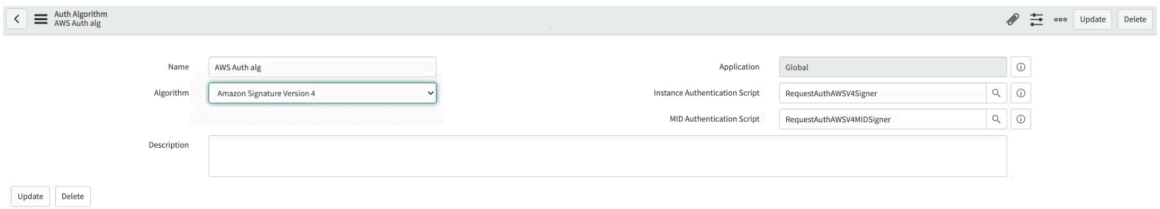
Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

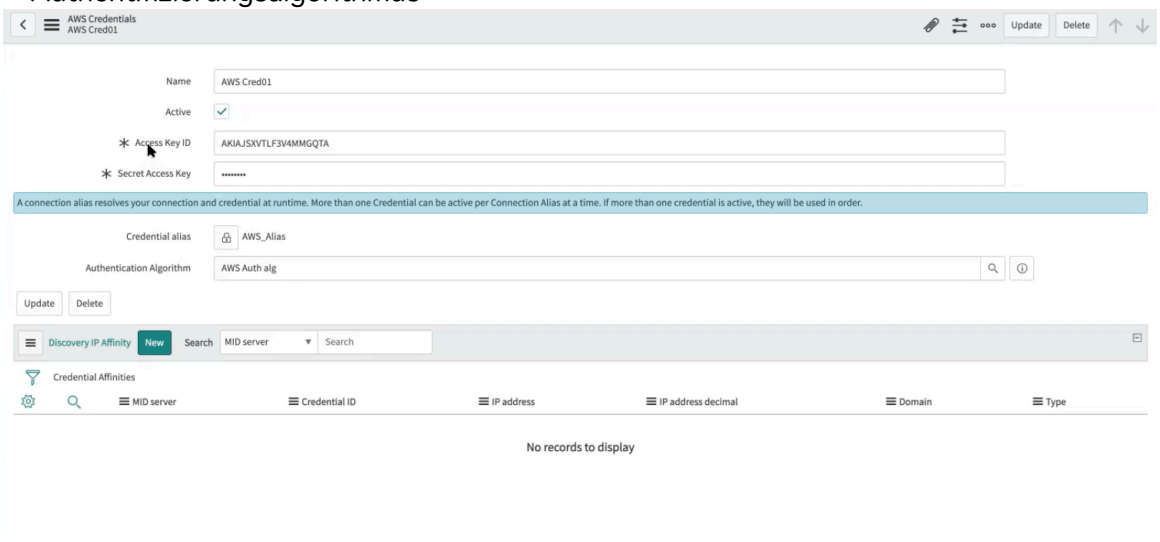
Feld	Beschreibung
Algorithmus	Ausgehender Anforderungstyp. Wählen Sie **Amazon Signature Version 4 aus**.
Beschreibung	Beschreibung dessen, was Ihr Algorithmus tut.
Anwendung	Bereich, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie in der Tabelle „Skripteinbindungen“ auswählen Wählen Sie im Falle des **Amazon Signature Version 4** -Algorithmus **RequestAuthAWSV4Signer aus**. Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner **Hinweis:** Um mehr über das Skript zu erfahren, klicken Sie auf das Informationssymbol neben dem Feld. Die Details des Skripts wie Name, API-Name, Anwendung, Zugänglich von, Skript usw. werden angezeigt.
MID-Authentifizierungsskript	Skript, das Sie in der Tabelle „MID Server-Skripteinbindungen“ [Discovery-Ansicht] auswählen. Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner



3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Berechtigungen**.
5. Klicken Sie auf **Neu**.
6. Erstellen Sie AWS Anmeldeinformationen mit dem Authentifizierungsalgorithmus.
   In diesem Fall **AWS Auth alg**.
7. Geben Sie Folgendes an:
   - Name
   - Aktiv
   - Zugangsschlüssel-ID
   - Geheimer Zugangsschlüssel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anmeldeinformationsalias
- Authentifizierungsalgorithmus



8. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Basierend auf den ausgewählten Skripts und dem Authentifizierungsalgorithmus generieren die konfigurierten Anmeldeinformationen (**Zugriffsschlüssel-ID** und **geheimer Zugriffsschlüssel**) oder die Anmeldeinformationen des Benutzers (**Zugriffsschlüssel-ID**, **geheimer Zugriffsschlüssel**und **Sitzungstoken**) eine Amazon V4-Signatur, die als ausgehende Anforderung von gesendet wird ServiceNow an den Provider (in diesem Fall AWS).

Example: REST-Schritt mit AWS

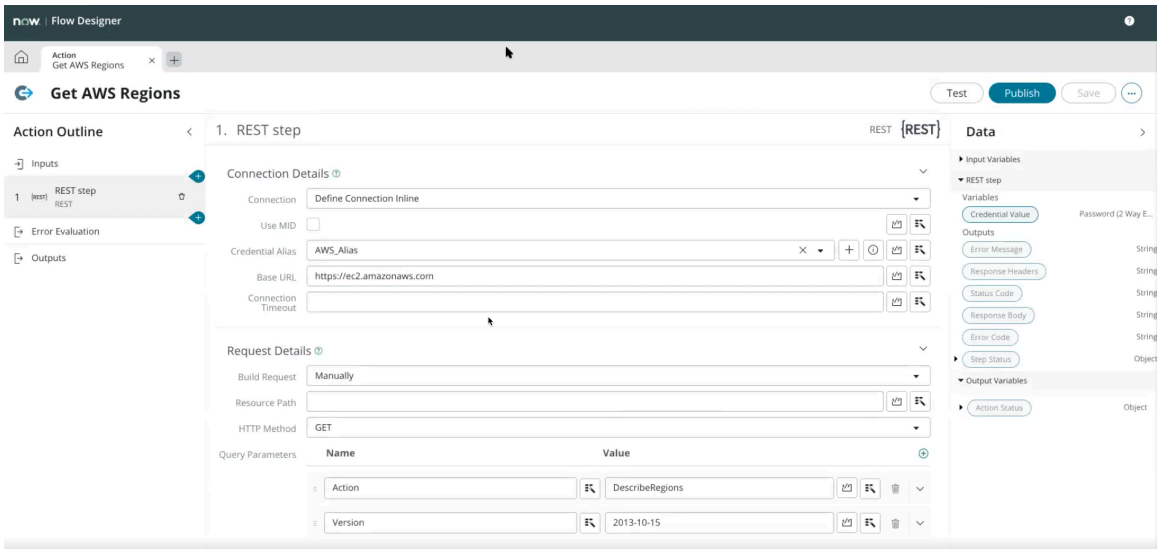
Hinweis:
Amazon Die auf der V4-Signatur basierende Authentifizierung kann auch über den Skripthintergrund verwendet werden.

Aktion: Rufen Sie AWS Regionen ab

Geben Sie den REST-Schritt mit AWS wie folgt ein:

- **Alias für Anmeldeinformationen**: Der Alias, der für AWSerstellt wird.
- **Basis-URL**: Basis-URL-Details von AWS.
- **HTTPS-Methode**: In diesem Fall ist es die GET-Methode.
- **Abfrageparameter**: **Aktion** als **DescribeRegions**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Aktion testen, die zugehörigen Regionen werden angezeigt. Der Antworttext lautet wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Amazon V4 ist mit einem Standardsatz von Algorithmen definiert, der den Authentifizierungsmechanismus unterstützt. Wenn dieser Algorithmus verwendet wird, wird die Signatur als Autorisierungskopfzeile für die Authentifizierung (HTTP-Anforderung) mit dem REST-Schritt hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen benutzerdefinierten Authentifizierungsalgorithmus

Generieren Sie die benutzerdefinierten Daten, die für die Authentifizierung bei einem Webservice erforderlich sind, indem Sie ein Skript ausführen.

Vorbereitungen

- JavaScript-Wissen
- REST-Wissen
- Wissen der Ziel-Webservice-API
- Wissen über Verbindungen, Anmeldeinformationen und Aliasse
- Erforderliche Rolle: Developer

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie für die Authentifizierung einen Alias für Verbindungen und Anmeldeinformationen und einen benutzerdefinierten authentifizierungsbasierten Algorithmus.

Prozedur

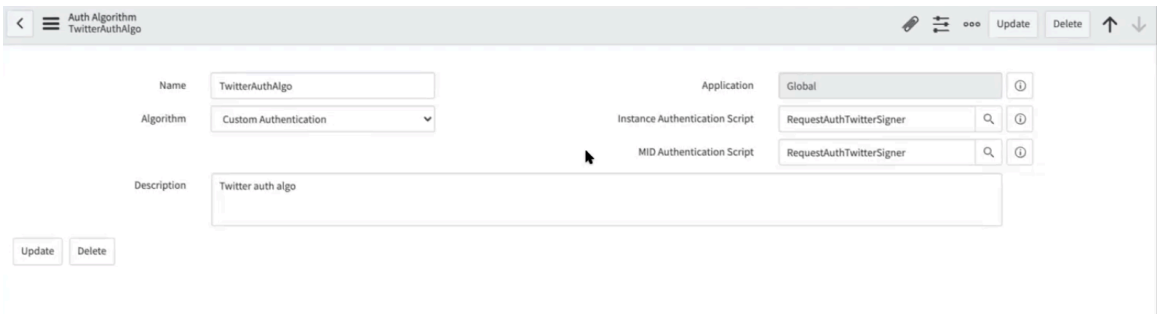
1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Ausgehender Anforderungstyp. Wählen Sie **Benutzerdefinierte Authentifizierung aus**.
Beschreibung	Beschreibung dessen, was Ihr Algorithmus tut.
Anwendung	Bereich, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie in der Tabelle „Skripteinbindungen“ auswählen Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Um mehr über das Skript zu erfahren, klicken Sie auf das Informationssymbol neben dem Feld. Die Details des Skripts wie Name, API-Name, Anwendung, Zugänglich von, Skript usw. werden angezeigt. ○ Im Falle einer benutzerdefinierten Authentifizierung mit Twitter können Sie **RequestAuthTwitterSigner**wählen, da eine OAuth 1.0a-Authentifizierungsmethode verwendet wird. Dies erfordert Informationen wie **API-Schlüssel und Geheimschlüssel** sowie **Zugriffstoken und Geheimschlüssel**, die zum Erstellen von Signaturen verwendet werden können, um einen Autorisierungsheader zu übergeben. Weitere Informationen finden Sie unter Authentifizierung in Twitter.
MID-Authentifizierungsskript	Skript, das Sie in der Tabelle „MID Server-Skripteinbindungen“ [Discovery-Ansicht] auswählen. Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

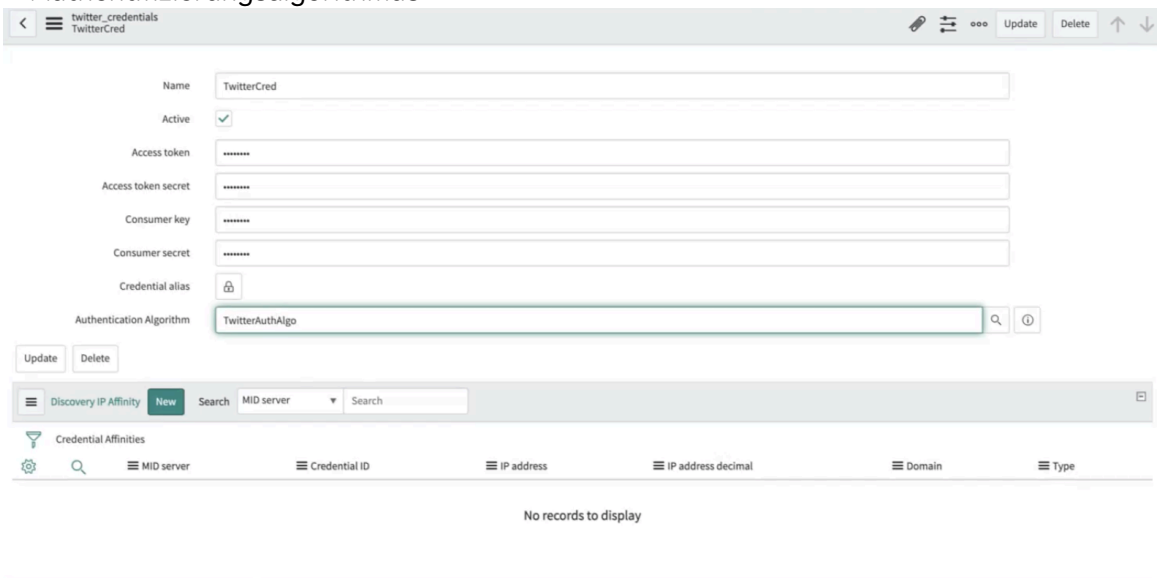


Basierend auf den ausgewählten Skripts und dem Authentifizierungsalgorithmus werden die konfigurierten Anmeldeinformationen als ausgehende Anforderung von ServiceNow an den Provider gesendet.

3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Berechtigungen**.
5. Klicken Sie auf **Neu**.
6. Erstellen Sie Twitter Anmeldeinformationen mit dem Authentifizierungsalgorithmus. In diesem Fall **TwitterAuthAlgo**.
7. Geben Sie die Felder an:
   - Name
   - Aktiv
   - Zugriffstoken
   - Zugriffstokengeheimnis

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verbraucherschlüssel
- Verbrauchergeheimnis
- Anmeldeinformationsalias
- Authentifizierungsalgorithmus



8. Klicken Sie auf **Aktualisieren**.

Example: REST-Schritt mit Twitter

Im Falle von Twittermüssen Sie sicherstellen, dass die folgenden Spokes oder Anmeldeinformationen verfügbar sind:

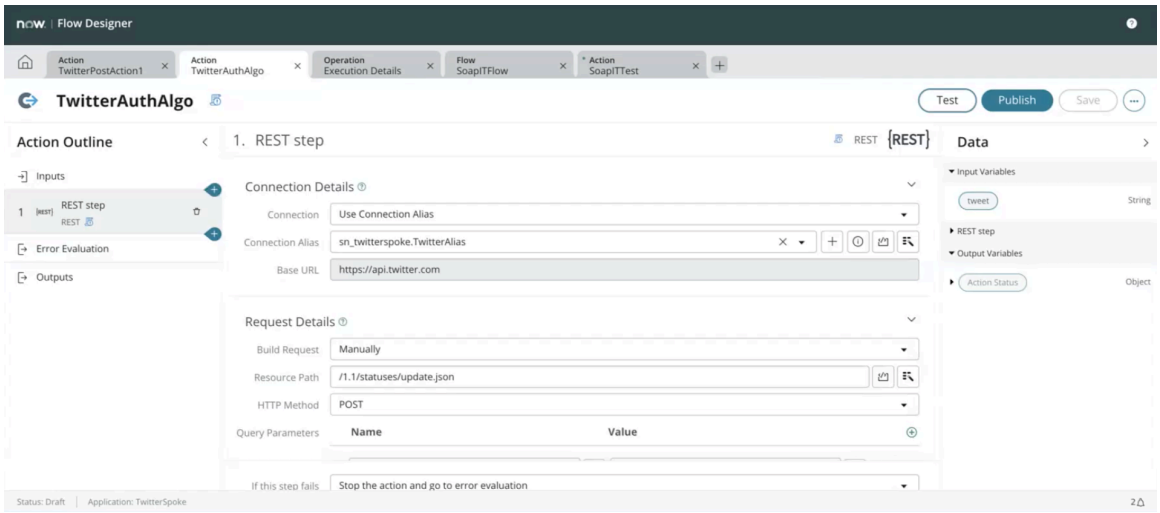
- Zugriffstoken
- Zugriffstokengeheimnis
- Verbraucherschlüssel
- Verbrauchergeheimnis
- Authentifizierungsalgorithmus

Aktion: TwitterAuthAlgo.

Geben Sie den REST-Schritt mit Twitter wie folgt ein:

- **Alias für Anmeldeinformationen**: Der Alias, der für Twittererstellt wird.
- **Basis-URL**: Basis-URL-Details von Twitter.
- **HTTPS-Methode**: In diesem Fall handelt es sich um die POST-Methode. Einen Tweet veröffentlichen.
- **Abfrageparameter**: **Aktion** als **Tweet**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Aktion testen. Der Tweet wird auf der Seite Twitter veröffentlicht.

IP-Service-Affinität für Discovery und Orchestration prüfen

Sie können in der Tabelle „IP-Services“ nach einer Liste von IP-Adressen suchen, die einem Protokoll zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „IP-Services“ ordnet einen Port einem Protokoll zu. Für häufig verwendete Port-Protokoll-Kombinationen werden standardmäßig Zuordnungen bereitgestellt, z. B. Port 80 für HTTP, Port 22 für SSH und Port 161 für SNMP.

Mithilfe der Systemeigenschaft `glide.discovery.ip_service_affinity` kann sich Discovery den letzten Port der erkannten IP-Adresse merken. Diese Eigenschaft ist standardmäßig auf **false** festgelegt.

Wichtig:
Sie sollten IP-Services nur dann ändern, wenn Ihre Organisation benutzerdefinierte Ports verwendet.

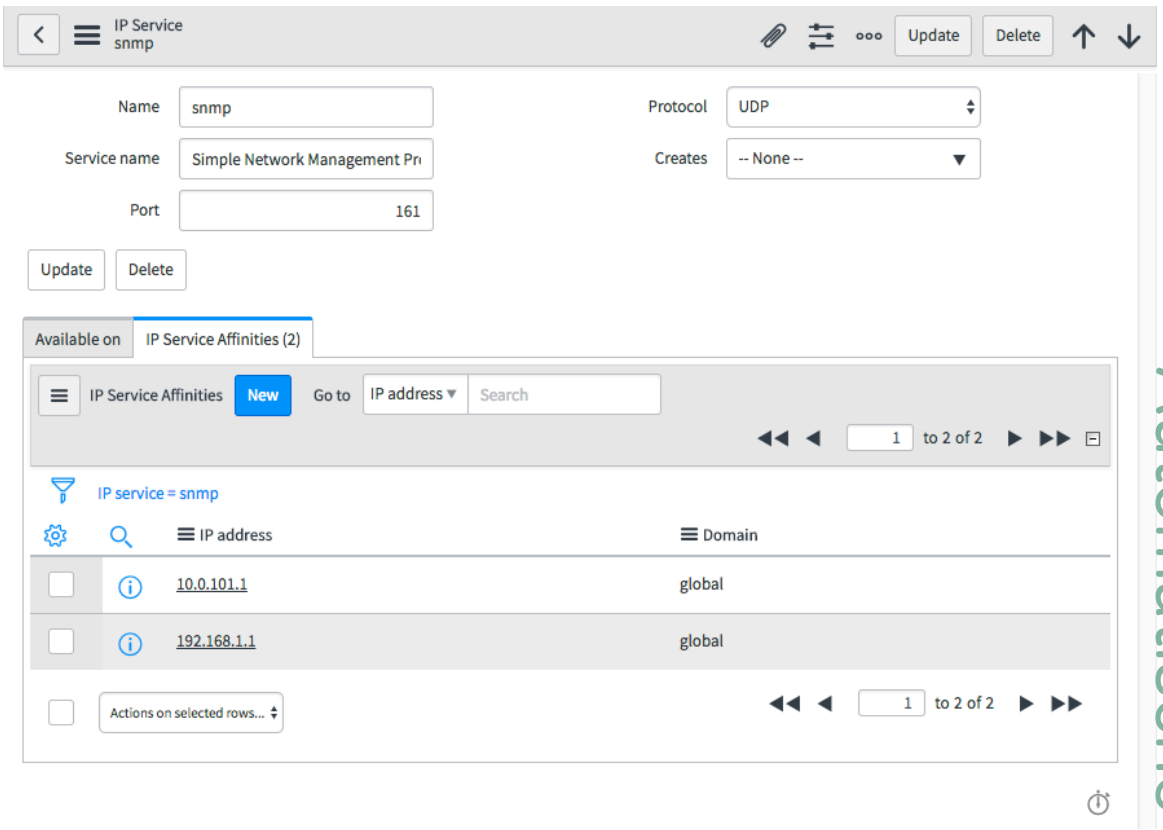
Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **IP-Services**.
2. Filtern Sie die Liste, um den entsprechenden IP-Service zu finden.
3. Klicken Sie auf den Namen des Service, um zu dieser IP-Serviceseite zu gelangen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **IP-Serviceaffinitäten**, um die Liste der IP-Adressen anzuzeigen, die diesem Service zugeordnet sind.

IP-Serviceaffinitäten



Sicherheit bei Anmeldung und Authentifizierung

Konfigurieren Sie Anmeldesicherheitsoptionen, um den Zugriff auf Ihre Instanz zu steuern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie die Sicherheit bei Anmeldung und Authentifizierung

Lernen Sie die Funktionen und Geschäftsvorteile der Anmeldesicherheit kennen.

Konfigurieren Sie Ihre Anmeldesicherheit

Machen Sie sich mit der Konfiguration der Anmeldesicherheit vertraut.

Definieren Sie Anmeldeszenarien

Definieren Sie Anmeldeszenarien.

Passwortzurücksetzung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über das Zurücksetzen des Anmeldepassworts.

Erkunden der Sicherheit bei Anmeldung und Authentifizierung

Konfigurieren Sie Anmeldesicherheitsoptionen, um den Zugriff auf Ihre Instanz zu steuern.

Sicherheitsoptionen

Sie können verschiedene Aspekte der Sicherheit der Benutzeranmeldung und -authentifizierung steuern:

Funktion	Beschreibung	Verwandte Themen
Steuerelemente zum Anmelden und Abmelden	Steuern Sie verschiedene Dimensionen des Anmelde- und Abmeldevorgangs für Benutzer, z. B. die Angabe einer Zielseite, die dem Benutzer bei der Anmeldung angezeigt wird, und steuern Sie, wie sich Benutzer abmelden.	• Anmeldeszenarien definieren • Bestätigungsaufforderung für Abmeldung konfigurieren • Entfernen Sie die Schaltfläche Abmelden • Die Installation wird beendet • Sperrung für fehlgeschlagene Anmeldeversuche angeben
Authentifizierungssicherheit	Steuern Sie den Prozess zum Zurücksetzen des Passworts und Funktionen wie die Option „Benutzernamen speichern“. Sie können auch IP-adressbasierte Steuerungen für den Zugriff auf die Instanz verwenden und eine Nonce implementieren, die mit der Single Sign-on Digest-Authentifizierung verwendet werden soll.	• Passwortrichtlinie konfigurieren • Verstärken Sie die Passwortvalidierungsregeln • Referenzbeispiel: Der Standard-Selfservice-Prozess Passwortzurücksetzung . • Ändern Sie die Einstellungen für das Kontrollkästchen Benutzernamen speichern und Cookies • IP-Bereichsbasierte Authentifizierung • Implementieren einer Nonce

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestätigungsaufforderung für Abmeldung konfigurieren

Sie können eine Bestätigungsaufforderung für die Abmeldung aktivieren, um zu verhindern, dass Benutzer sich versehentlich abmelden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Hinweis:
Das folgende Verfahren funktioniert nur in UI-Versionen vor Core-UI, der neuesten und am häufigsten verwendeten.

Prozedur
1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**.
2. Suchen Sie die Eigenschaft **Benutzer auffordern, eine Abmeldeanforderung zu bestätigen**, und aktivieren Sie das Kontrollkästchen.
3. Wenn der Benutzer auf die Schaltfläche **Abmelden** klickt, wird ein Bestätigungsdialogfeld angezeigt.

Eigenschaften von Passwortzurücksetzung konfigurieren

Sie können Eigenschaften angeben, die die Passwortzurücksetzung-Erfahrung für Endbenutzer konfigurieren.

Vorbereitungen
Erforderliche Rolle: password_reset_admin

Warum und wann dieser Vorgang ausgeführt wird
Es gibt zwar keine Bereichsgrenzen für die Werte, die Sie für Eigenschaften eingeben können, es sollten jedoch nur positive Ganzzahlwerte ab 1 verwendet werden. Wenn Sie den Grenzwert für den oberen Bereich einer Eigenschaft festlegen, müssen Sie die vom Benutzer ausgeführte Aufgabe berücksichtigen.

Sie werden beispielsweise nicht zulassen wollen, dass Benutzer 100 Versuche haben, um ihre Identität zu bestätigen. Ein üblicherer Wert sind 3 Versuche. Ebenso wenig werden Sie wollen, dass Benutzer während des Registrierungsprozesses 30 Sicherheitsfragen auswählen und beantworten müssen. Eine häufiger verwendete Anzahl von Sicherheitsfragen liegt zwischen 5 und 7.

Prozedur
1. Navigieren zu **Alle** > **Passwortzurücksetzung** > **Eigenschaften**.
   Weitere Informationen zu den Passwortzurücksetzung -Eigenschaften finden Sie unter Passwortzurücksetzung globalen Eigenschaften.
2. Aktualisieren Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Anmeldeszenarien definieren

Sie können alle Benutzer nach der Anmeldung auf dieselbe Seite leiten.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn sich Benutzer direkt bei einer Instanz anmelden, z. B. bei http://{instance_name}.service-now.com/, geht das System wie folgt vor:

1. Greift auf den Wert in der Eigenschaft `glide.entry.page.script`zu. Der Standardwert der Eigenschaft wird von einer Skripteinbindung mit dem Namen *CMSEntryPage abgeleitet*.
2. Leitet den Benutzer zur Anmeldeseite der Instanz weiter, wenn für die Einstiegsseite eine Anmeldung erforderlich ist.
3. Wendet, falls vorhanden, Anmelderegeln auf den Benutzer an.

So erzwingen Sie, dass das System alle Benutzer nach der Anmeldung auf dieselbe Seite leitet:

Prozedur

1. Navigieren zu **Alle** > **Inhaltsmanagement** > **Konfiguration** > **Konfigurationsseite**.
2. Wählen Sie einen Wert für das Feld *Anmeldeseite* aus, oder erstellen Sie nach Bedarf eine neue Seite. Wenn diese Seite nicht die Standardseite der Website ist, wird immer hierher umgeleitet. Wenn es sich um eine Standardseite einer Website handelt, werden Anmelderegeln angewendet. Wenn dieser Wert NULL ist, verwendet das System navpage.do als Einstiegsseite. Geben Sie hier keine Anmeldeseite ein. andernfalls müssen sich Benutzer zweimal anmelden.

   Melden Sie sich bei einer Instanz an, um auf einen Datensatz zuzugreifen:

   Wenn sich Benutzer bei einer Instanz anmelden, um über ihren global eindeutigen Bezeichner (sys_id) auf einen Datensatz zuzugreifen, z. B. http://{instance}.service-now.com/incident.do?sys_id={sys_id}, führt das System Folgendes aus: Folgendes:

   a. Leitet den Benutzer zu einer Anmeldeseite weiter, wenn er nicht bereits angemeldet ist.

   b. Leitet den Benutzer zum entsprechenden Datensatz weiter, wenn er darauf zugreifen darf. Wenn der Benutzer keine Zugriffsrechte für den Datensatz hat, wird eine Nachricht über die Zugriffsverweigerung angezeigt.

   Anmelden beim Service Portal oder einer CMS-Website:

   Wenn sich Benutzer beim Service Portal oder einer CMS-Website anmelden, z. B. http://<instance> .service-now.com/site-name/page.do, führt das System folgende Schritte aus:

   - Wenn im Service Portal- oder im CMS-Site-Formular ein Wert im Feld *Anmeldeseite* vorhanden ist, wird der Benutzer zu dieser Anmeldeseite weitergeleitet und es werden ggf. Anmelderegeln auf den Benutzer angewendet.
   - Wenn keine Anmeldeseite angegeben ist, wird der Benutzer an den Wert im Feld *Homepage* im Service Portal oder im CMS-Site-Formular weitergeleitet.

   Melden Sie sich beim Service Portal oder einer CMS-Site an, um auf einen Datensatz zuzugreifen:

   Wenn sich Benutzer beim Service Portal oder einer CMS-Website anmelden, um auf einen Datensatz zuzugreifen, z. B. http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id}, folgt das System das gleiche Verfahren und führt den Benutzer schließlich zum Datensatz. Wenn der Benutzer keine Zugriffsrechte für den Datensatz hat, wird eine Nachricht über die Zugriffsverweigerung angezeigt.

Anmeldungen und das Mitarbeiter-Selfserviceportal

Das System verfolgt die erste Startseite, auf die ein Benutzer zugreifen versucht, auch wenn sich der Benutzer beim Mitarbeiter-Selfserviceportal anmelden möchte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betrachten Sie die folgenden Szenarien.

Beispiel 1:

1. Ein Benutzer ist nicht angemeldet und versucht dann, mit einer bestimmten SYS-ID in der URL auf einen Datensatz zuzugreifen.
2. Das System leitet den Benutzer zur Anmeldeseite um.
3. Anstatt sich anzumelden, versucht der Benutzer, auf eine andere Website zuzugreifen, z. B. auf das Mitarbeiter-Selfserviceportal (/ess).
4. Das System leitet den Benutzer erneut zur Anmeldeseite um.
5. Der Benutzer meldet sich an und wird zu dem Datensatz weitergeleitet, auf den der Benutzer zuerst versucht hat, zuzugreifen, und nicht zum Mitarbeiter-Selfserviceportal.

Beispiel 2:

1. Ein Benutzer ist nicht angemeldet und versucht dann, über das Mitarbeiter-Selfserviceportal (/ess) mit einer bestimmten SYS-ID in der URL auf einen Datensatz zuzugreifen.
2. Das System leitet den Benutzer zur Anmeldeseite um.
3. Anstatt sich anzumelden, versucht der Benutzer, über das Mitarbeiter-Selfserviceportal auf einen anderen Datensatz zuzugreifen.
4. Das System leitet den Benutzer erneut zur Anmeldeseite um.
5. Der Benutzer meldet sich an und wird zum ersten und nicht zum zweiten Datensatz weitergeleitet.

Geben Sie eine Zielseite für die Anmeldung an

Standardmäßig sehen Benutzer bei der Anmeldung ihre Homepage. Sie können eine andere Anmeldezielseite angeben, indem Sie eine Systemeigenschaft oder das Content Management System verwenden.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Um eine Anmeldezielseite für alle Benutzer anzugeben, ändern Sie den Eigenschaftswert in der Tabelle „sys_properties“.

Prozedur

1. Geben Sie sys_properties.list in den Navigationsfilter ein.
2. Suchen Sie die Systemeigenschaft **glide.login.home**.
3. Geben Sie im Feld **Wert** den Namen der Seite ein, die allen Benutzern bei der Anmeldung angezeigt wird.

   Verwenden<page name> .do; Sie können den Teil http://"instance".service-now.com/ der URL auslassen. Um den Seitennamen oder die URL einer Seite im System zu ermitteln, können Sie auf einen Link verweisen. Einige mögliche Seiten sind „welcome.do“ und „ incident.do“.

   Um eine Dashboard-Zielseite anzugeben, legen Sie die Eigenschaft auf $dashboards.do?dashboard=fest<SYS_ID> . Ersetzen<SYS_ID> mit der sys_id des Dashboards.

   Um Benutzer an das Service Portal weiterzuleiten, legen Sie die Eigenschaft auf /spfest

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Diese Eigenschaft ist systemweit, daher wirkt sich ihre Einstellung auf alle Benutzer aus. Um eine Anmeldung speziell für Benutzer ohne Rollen festzulegen, können Sie dieselben Schritte ausführen und die Eigenschaft **glide.entry.loggedin.page_ess** verwenden.

Sie können auch eine Anmeldezielseite mit dem Content Management System angeben.

Sperrung für fehlgeschlagene Anmeldeversuche angeben

Das System bietet inaktive Skriptaktionen, mit denen Sie die Anzahl der fehlgeschlagenen Anmeldeversuche angeben können, bevor ein Benutzeraccount gesperrt wird, und mit denen die Anzahl nach einer erfolgreichen Anmeldung zurückgesetzt wird.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

Navigieren zu **Alle** > **Systemrichtlinie** > **Skriptaktionen** , um die Skripts anzuzeigen oder zu aktivieren.

Hinweis:
Ab der Kingston-Release werden die Skriptaktionen **SNC-Benutzersperrprüfung mit automatischer Entsperrung** und **SNC-Benutzerlöschung** nach einem zBoot aktiviert.

Weitere Informationen zu Eigenschaften, die sich auf fehlgeschlagene Anmeldeversuche auswirken, finden Sie unter Fehlgeschlagene Anmeldeversuche verwalten (Härtung der Instanzsicherheit) in den Einstellungen für die Härtung der Instanzsicherheit.

Skriptaktion	Beschreibung
SNC-Benutzersperrprüfung mit automatischer Entsperrung	• Verwendet den Wert der Eigenschaft `glide.user.max_unlock_attempts`, um den Grenzwert für fehlgeschlagene Anmeldeversuche festzulegen. • Entsperrt den Benutzeraccount nach dem für die Eigenschaft `glide.user.unlock_timeout_in_mins` angegebenen Zeitraum. Wenn kein Wert angegeben ist, entsperrt das System den Benutzeraccount nach dem Standardzeitraum von 15 Minuten.
SNC-Benutzersperrprüfung	Verfolgt die Anzahl der fehlgeschlagenen Anmeldeversuche und sperrt den Benutzeraccount nach einer angegebenen Anzahl von fehlgeschlagenen Anmeldeversuchen (Standard: 5).
SNC-Benutzerlöschung	Aktualisiert den Benutzerdatensatz nach einer erfolgreichen Anmeldung: Setzt die Anzahl der fehlgeschlagenen Anmeldeversuche zurück und aktualisiert das Datum der letzten Anmeldung.

Nächste Maßnahme
Jedes Mal, wenn ein Benutzer versucht, sich anzumelden, wird die Aktion in einem Ereignisprotokoll aufgezeichnet. Sie können ein Protokoll der fehlgeschlagenen Anmeldeversuche anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Systemrichtlinie** > **Ereignisprotokolle**.
2. Filtern Sie im Feld **Name** nach **login.failed**. Sie können den versuchten Anmeldenamen, das Datum und die IP-Adresse anzeigen, die für den Versuch protokolliert wurden.

Machen Sie UI-Seiten öffentlich oder privat

Sie können Seiten öffentlich machen, wenn Sie möchten, dass Ihre Benutzer die Seiten sehen, ohne sich anzumelden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die meisten Seiten können nur von angemeldeten Benutzern angezeigt werden. Eine begrenzte Anzahl von Seiten ist öffentlich, sodass Benutzer sich nicht anmelden müssen, um sie anzuzeigen, z. B. die Willkommensseite, die Startseite sowie die Anmelde- und Abmeldeseiten.

⚠ Warnung:
Für die Funktionalität vieler -Funktionen sind mehrere öffentliche Seiten des Basissystems erforderlich. Deaktivieren Sie nicht die öffentlichen Seiten des Basissystems.

Prozedur

1. Geben Sie im Anwendungsnavigator-Filter `sys_public.list` ein.
2. Klicken Sie auf **Neu**.
3. Erstellen Sie in der Tabelle „sys_public“ einen Datensatz mit den folgenden Werten.

Feld	Beschreibung
Seite	Der Name der Seite. Beispiel: $sp
Aktiv	Wenn diese Option ausgewählt ist, ist die Seite öffentlich zugänglich. Deaktivieren Sie die Option Aktiv, wenn die Seite privat sein soll.

4. Klicken Sie auf **Speichern**.
   Wenn Sie „active“ auf „true“ setzen, ist die Seite öffentlich, also für jeden, der sie besucht<instance_name> `/sp` oder `/$sp.do` kann auf die Seite zugreifen.

Referenzbeispiel: Der Standard-Selfservice-Prozess Passwortzurücksetzung .

Der standardmäßige Self-Service-Passwortzurücksetzung-Prozess ermöglicht es einem Benutzer, das Passwort ohne Hilfe von Service-Desk-Mitarbeitern zurückzusetzen.

Example: Der standardmäßige Self-Service-Ablauf für das Zurücksetzen des Passworts

1. Wenn sich ein Benutzer nicht an das Passwort erinnert, kann er auf den Link **Passwort vergessen?** auf dem Anmeldebildschirm klicken.
2. Die Anwendung Passwortzurücksetzung wird gestartet. Auf der Seite **Identität** identifiziert sich der Benutzer durch Eingabe eines **Benutzernamens**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Auf der Seite **Überprüfen** weist der Benutzer nach, dass er die Person ist, die mit dem Benutzernamen verknüpft ist. In diesem Beispiel gibt der Benutzer die E-Mail-Adresse ein, die dem Benutzerprofil zugeordnet ist. Der Administrator kann eine andere Überprüfungsmethode konfigurieren oder zusätzliche Überprüfungen erfordern, z. B. eine persönliche Frage, die nur der Benutzer beantworten kann.
4. Auf der Seite **Zurücksetzen** wird der Benutzer angewiesen, die E-Mail auf Anweisungen zu überprüfen.
5. Der Benutzer öffnet die E-Mail und klickt auf den Link **Hier**, um das Passwort zurückzusetzen. Der Link ist für einen von Ihnen angegebenen Zeitraum gültig (verwenden Sie die Eigenschaft **password_reset.request.expiry**).
6. Die Seite **Passwort zurücksetzen** führt den Benutzer durch den Prozess zum Zurücksetzen des Passworts.

Der standardmäßige Self-Service-Passwortzurücksetzung-Prozess (com.glideapp.password_reset) definiert:

- Den URI, der angibt, wohin Benutzer beim Klicken auf **Passwort vergessen?** umgeleitet werden. Standardmäßig lautet dieser Wert **/$pwd_reset.do?sysparm_url=ss_default**. Dies ist derselbe Wert, der in der Eigenschaft *glide.security.password_reset.uri* verwendet wird. In früheren Releases wurde dieser Wert auf **/reset_password.do** festgelegt.
- Die Option **URL zum Zurücksetzen des Passworts aktivieren**, die angibt, dass der Benutzer nach dem Klicken auf **Passwort vergessen?** eine E-Mail mit einem Link zum Zurücksetzen des Passworts erhalten sollte.
- Der Verifizierungsablauf „Persönliche Daten – E-Mail-Adresse eingeben“, der den dreischrittigen Prozess für die Passwortzurücksetzung angibt.

Anweisungen zum Zugriff auf dieses Formular und zum Konfigurieren der Felder finden Sie unter Password Reset-Prozess konfigurieren.

Hinweis:

- Diese Funktion steht für lokal authentifizierte Benutzer zur Verfügung, die den in ihrem Benutzerdatensatz angegebenen Benutzernamen und das entsprechende Passwort eingeben. Benutzer, die sich über eine SSO-Lösung oder eine LDAP-Integration bei der Instanz anmelden, können Passwörter nicht mit dem Beispiel-Selfservice-Prozess Passwortzurücksetzung zurücksetzen.
- Der Endbenutzer muss die Benachrichtigungseinstellungen aktivieren und konfigurieren. Weitere Informationen finden Sie unter Benachrichtigungen auf Abonnementbasis . Administratoren können die an den Endbenutzer gesendete E-Mail ändern.

Ändern Sie den E-Mail-Text der Benachrichtigung Passwortzurücksetzung .

Benutzer des Selfservice-Prozesses Passwortzurücksetzung erhalten eine E-Mail-Benachrichtigung, wenn sie die Zurücksetzung des Passworts anfordern. Sie können den Text der E-Mail und andere Aspekte der Benachrichtigung ändern.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Dieser Prozess ist nur relevant, wenn es sich bei den Benutzern um abonnementbasierte Benachrichtigungen handelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systembenachrichtigung** > **Benachrichtigungen**.
2. Klicken Sie auf die Benachrichtigung **Password Reset URL** (Passwortzurücksetzungs-URL).
3. Ändern **Sie den Text der E-Mail im Abschnitt Inhalt**.
   Informationen zum Konfigurieren anderer Aspekte der Benachrichtigung finden Sie unter E-Mail-Benachrichtigungen erstellen .

Entfernen Sie die Schaltfläche Abmelden

Sie können die **Schaltfläche** Abmelden entfernen, um ein versehentliches Abmelden zu verhindern.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Das folgende Verfahren funktioniert nicht in Core-UI.

Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Benutzereinstellungen**.
2. Löschen Sie die Systemeinstellung `user.can.logout`.

Die Installation wird beendet

Installations-Exits sind Anpassungen, die Java verlassen, um ein Skript aufzurufen, bevor zu Java zurückgekehrt wird.

Hinweis:
Die hier beschriebene Funktionalität erfordert die **Admin**-Rolle.

Verfügbare Installationsausgänge

Navigieren zu **Systemdefinition** > **Installationsausgänge**. Einige Namen der Installationsausgänge (Login, Logout, ValidatePassword, ExternalAuthentication) sind reserviert und können nicht geändert werden. Andere Installations-Exits können diese mit einem benutzerdefinierten Skript überschreiben, das das Skript im Standard-Installations-Exit ersetzt.

Die folgenden Installationsausgänge sind im Basissystem verfügbar:

Installationsausgang	Beschreibung
Anmelden	Verwendet ein Benutzername-Passwort-Paar und authentifiziert sich mit dem Benutzerobjekt
Abmelden	Leitet den Anwender beim Abmelden zur Willkommensseite. kann von LogoutRedirect überschrieben werden
LogoutRedirect	Leitet den Anwender beim Abmelden zu einer angegebenen URL weiter
Externe Authentifizierung	Authentifiziert mit Header, Parameter oder Cookie; kann von DigestSingleSignOn und PGPSingleSignOn überschrieben werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installationsausgang	Beschreibung
DigestSingleSignOn	Authentifiziert mithilfe von Header, Parameter oder Cookie und entschlüsselt die Digest-Verschlüsselung
PGPSingleSignOn	Authentifiziert mithilfe von Header, Parameter oder Cookie und entschlüsselt die PGP-Verschlüsselung
ValidierenPasswort	Standardmäßig aktiv, beginnend mit Release Helsinki. ermöglicht Kunden, ihre eigene Passwortvalidierung zu definieren; kann von ValidatePasswordStronger überschrieben werden
ValidierenPasswordStronger	Erfordert, dass Passwörter mindestens 8 Zeichen lang sind und eine Ziffer, einen Großbuchstaben und einen Kleinbuchstaben enthalten
GetIntegrationSessionTimeout	Implementiert das standardmäßige Zeitüberschreitungsverhalten für Integrationssitzungen.

Anmeldeänderungen

Durch die folgende Änderung des **Login** -Installations-Exits wird der Zeitüberschreitungswert für die Sitzung jedes Benutzers festgelegt, wenn sich der Benutzer anmeldet. Wenn der Benutzername in diesem Beispiel *admin*lautet, wird die Sitzung auf eine Zeitüberschreitung in 30 Sekunden festgelegt.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

      process : function() {
        // the request is passed in as a global
        var userName = request.getParameter("user_name");
        var userPassword = request.getParameter("user_password");

        var authed = GlideUser.authenticate(userName, userPassword);
        if (authed) {
          // ************************************************************
          // customization - if the userName == admin, set the session
          // timeout to be 30 seconds. You can implement your own
          // session timeout algorithm here by checking to see if a user
          // belongs to a certain group or has a certain role.
          // Values of setMaxInactiveInterval exceeding 1440 minutes are
          // treated as one day (1440 minutes).

         if (userName == "admin") {
            request.getSession().setMaxInactiveInterval(30);
          }
          // ************************************************************
          return GlideUser.getUser(userName);
        }

        this.loginFailed();

        return "login.failed";
      },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    loginFailed : function() {
      var message = GlideSysMessage.format("login_invalid");
      var gSession = GlideSession.get();
      gSession.addErrorMessage(message);

      var userName = request.getParameter("user_name");
      EventManager.queue("login.failed", "", userName, "");
    }

}
```

Die Sitzungszeitüberschreitung kann auch entsprechend der IP-Adresse festgelegt werden.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

    process : function() {
      // the request is passed in as a global
      var userName = request.getParameter("user_name");
      var userPassword = request.getParameter("user_password");

      var authed = GlideUser.authenticate(userName, userPassword);
      if (authed) {

      // ************************************************************
      // customization - if the user is logging in from a particular IP
      // range starting with XXX.XXX you can implement your own
      // session timeout algorithm here by checking the login IP
      //
      // Values of setMaxInactiveInterval exceeding 1440 minutes are
      // treated as one day (1440 minutes).

      var clientIP = gs.getSession().getClientIP().toString();

      // if client IP starts with specified range
      if (clientIP.indexOf('XXX.XXX') == 0) {
        // set to 10 hours
        request.getSession().setMaxInactiveInterval(60 * 60 * 10);
      }
      // ************************************************************

        return GlideUser.getUser(userName);
      }

      this.loginFailed();

      return "login.failed";
    },

    loginFailed : function() {
      var message = GlideSysMessage.format("login_invalid");
      var gSession = GlideSession.get();
      gSession.addErrorMessage(message);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", "", userName, "");
    }

}
```

Zugehörige Informationen

Erzwingen Sie starke Passwörter

Verstärken Sie die Passwortvalidierungsregeln

Sie können die Validierungsregeln für die Passwortstärke für den Bildschirm „Passwort ändern“ anpassen, indem Sie den mit der Passwortvalidierung verknüpften Installations-Exit überschreiben.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Installationsausgänge**.
2. Suchen Sie nach **ValidatePassword** (standardmäßig inaktiv) und **ValidatePasswordStronger** (standardmäßig aktiv, beginnend mit Release Helsinki.
3. Das `ValidatePasswordStronger-` Skript (unten) ist ein Beispielskript, das das `ValidatePassword` -Skript mithilfe regulärer Ausdrücke überschreibt, um zu verlangen, dass Passwörter mindestens 8 Zeichen lang sind, eine Ziffer enthalten und Buchstaben in Groß-/Kleinschreibung enthalten.

```
gs.include("PrototypeServer");
 var ValidatePasswordStronger = Class.create();
 ValidatePasswordStronger.prototype = {
     process : function() {
       var user_password = request.getParameter("user_password");
       var min_len = 8;
       var rules = "Password must be at least " + min_len +
         " characters long and contain a digit, an uppercase letter, and a lowercase letter.";
       if (user_password.length() < min_len) {
         gs.addErrorMessage("TOO SHORT: " + rules);
         return false;
       }
       var digit_pattern = new RegExp("[0-9]", "g");
       if (!digit_pattern.test(user_password)) {
         gs.addErrorMessage("DIGIT MISSING: " + rules);
         return false;
       }
       var upper_pattern = new RegExp("[A-Z]", "g");
       if (!upper_pattern.test(user_password)) {
         gs.addErrorMessage("UPPERCASE MISSING: " + rules);
         return false;
       }
       var lower_pattern = new RegExp("[a-z]", "g");
       if (!lower_pattern.test(user_password)) {
         gs.addErrorMessage("LOWERCASE MISSING: " + rules);
         return false;
       }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      return true; // password is OK
    }
}
```

Die von `Class.create()` erstellte Skriptvariable muss denselben Namen haben wie der Installationsausgang selbst – in diesem Beispiel „ValidatePasswordStronger“. Das Skript implementiert die Funktion `process()`, die „true“ zurückgibt, wenn das Passwort akzeptabel ist, und „false“, wenn das Passwort überarbeitet werden muss. Die Funktion `gs.addErrorMessage` kann verwendet werden, um Fehlermeldungen auf dem Bildschirm zum Ändern des Passworts zurückzugeben. Sie können diesen Installations-Exit in Ihrer Instanz ausprobieren, indem Sie die *aktive* Kennzeichnung überprüfen und den Datensatz aktualisieren. Leeren Sie anschließend den Cache, damit die Änderung erkannt wird.

Beachten Sie auch, dass das Ändern dieser Skripts das Standardverhalten von ServiceNow nicht ändert: Leere Passwörter sind weiterhin standardmäßig verboten, und die Felder „Passwort“ und „Passwort überprüfen“ müssen übereinstimmen.

Ergebnisse
Aktivieren Sie zum Testen das Kontrollkästchen „ **Passwort muss zurückgesetzt** werden“ in einem Benutzerdatensatz, und melden Sie sich mit diesem Benutzer an. Die Validierung erfolgt an dem Punkt, an dem der Benutzer versucht, das Passwort festzulegen. Die Validierung erfolgt nicht, wenn ein Admin-Benutzer das Passwort im Benutzerdatensatz direkt aktualisiert (der Administrator kann alles in das Passwortfeld eingeben).

Hinweis:
Der Bildschirm „Passwort ändern“ gilt nur für Kunden, die kein Single Sign-on verwenden und nicht in ihr lokales LDAP integriert sind.

Ändern Sie die Einstellungen für das Kontrollkästchen Benutzernamen speichern und Cookies

Wenn bei der **Anmeldung** das Kontrollkästchen Benutzernamen speichern aktiviert ist, wird ein Cookie auf dem Computer des Benutzers gespeichert. Dieses Cookie authentifiziert den Benutzer bei nachfolgenden Besuchen automatisch.

Wenn sich der Benutzer abmeldet, wird das Cookie gelöscht. Der Standardwert des Kontrollkästchens Benutzernamen speichern wird von einer Eigenschaft gesteuert, und ob das Kontrollkästchen auf der **Anmeldeseite** angezeigt wird, wird von einer anderen Eigenschaft gesteuert.

Zwei Eigenschaften, `glide.ui.user_cookie.life_span_in_days` und `glide.ui.user_cookie.max_life_span_in_days`, steuern den vom System generierten Cookie-Ablaufwert von glide_user. Wenn ein Benutzer auf eine Instanz mit aktiviertem „Benutzernamen speichern“ zugreift, wird der Ablaufzeitraum für Cookies durch den Zugriff zurückgesetzt, bis der maximale (glide.ui.user_cookie.max_life_span_in_days) Grenzwert für die Lebensdauer erreicht ist.

Hinweis:
Weitere Informationen zu diesen Eigenschaften finden Sie unter den folgenden Themen unter Härtungseinstellungen für Instanzsicherheit:

- Absolute Zeitüberschreitung für Sitzung
- Zeitüberschreitung für Sitzungsfenster

Ändern Sie den Standardwert des Kontrollkästchens Benutzernamen speichern

Sie können den Standardwert des Kontrollkästchens Benutzernamen **speichern** ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **UI-Eigenschaften**.
2. Suchen Sie die Eigenschaft [*Default value of "Remember me" checkbox on login page* (*glide.ui.remember.me.default*).
3. Um den Standardwert des Kontrollkästchens Benutzernamen speichern auf **Neinfestzulegen**, deaktivieren Sie das Kontrollkästchen für die Eigenschaft.
4. Um den Standardwert des Kontrollkästchens **Benutzernamen** speichern auf **Ja**zurückzusetzen, aktivieren Sie das entsprechende Kontrollkästchen.

Entfernen Sie das Kontrollkästchen Benutzernamen speichern

Sie können das Kontrollkästchen Benutzernamen speichern **entfernen**, damit Benutzer keinen Zugriff auf diese Funktion haben.

Vorbereitungen
Erforderliche Rolle: security_admin

Hinweis:
Weitere Informationen zu dieser Eigenschaft finden Sie unter „Benutzernamen speichern“ entfernen in Härtungseinstellungen für Instanzsicherheit.

Prozedur

1. Erhöhen Sie Ihre Rolle auf security_admin.
2. Navigieren zu **Systemeigenschaften** > **UI-Eigenschaften**.
3. Suchen Sie die Eigenschaft [*Remove "Remember me" checkbox from login page* (*glide.ui.forgetme*).
4. Aktivieren Sie das Kontrollkästchen für die Eigenschaften.
   Mit dieser Einstellung wird das Kontrollkästchen „Benutzernamen speichern“ entfernt, vorhandene **Cookies** werden für ungültig erklärt, und die Funktion „Benutzernamen speichern“ wird vollständig deaktiviert.
5. Um das Kontrollkästchen Benutzernamen speichern auf der Anmeldeseite wiederherzustellen, **deaktivieren Sie** das Kontrollkästchen für die Eigenschaften.

IP-Bereichsbasierte Authentifizierung

Eine Möglichkeit, eine webbasierte Anwendung abzusichern, besteht darin, den Zugriff basierend auf der IP-Adresse einzuschränken.

Sie können den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich blockieren, von denen Sie vermuten, dass sie zu böswilligen Personen gehören. Mit der Instanz können Sie den Zugriff nach IP-Adresse steuern.

Hinweis:
Verwenden Sie die Vorauthentifizierungskontextrichtlinie der adaptiven Authentifizierung (AA), um IP-basierte Authentifizierungen und Einschränkungen für zusätzliche Funktionen zu erzwingen. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Hinweise und Einschränkungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das System lässt Sie nicht zu, dass Sie sich selbst aussperren. Wenn Sie also versuchen, eine Regel hinzuzufügen, durch die Ihre aktuelle Adresse ausgesperrt wird, warnt Sie das System und lehnt die Eingabe ab.
- Wenn Sie sich in einem Unternehmens-Intranet befinden, gehen Sie beim Einrichten Ihrer IP-Regeln sehr vorsichtig vor. Die IP-Adresse, die Sie auf Ihrem Computer sehen (z. B. 10.10.10.25), hat in der Regel keine Beziehung zu der IP-Adresse, als die Sie im Internet angezeigt werden. Ihr Unternehmen stellt Ihre Adresse wahrscheinlich per Proxy und/oder NAT in einen vorhersehbaren Satz ausgehender Adressen um, nach denen Sie wahrscheinlich Ihr Netzwerkteam fragen müssen.
- Ein Benutzer, dessen Zugriff basierend auf einer Zugriffsregel eingeschränkt ist, erhält in seinem Browser den Fehler 403.
- Eingeschränkte Benutzer verwenden keine Transaktionen, Semaphore und zählen nicht für die Anzahl der Serverressourcen.
- Diese Funktion ersetzt oder überschreibt Ihre vorhandenen Zugriffskontrollregeln nicht, wenn Sie beispielsweise ein VPN zu unserem Rechenzentrum ausführen. Dies ist eine zusätzliche Prüfung, die zusätzlich zu den Zugriffskontrollen erfüllt werden muss, die wir möglicherweise für Ihren PIX eingerichtet haben.
- Allow-Regeln haben stets Vorrang vor Deny-Regeln. Wenn also eine Adresse sowohl zulässig (durch eine Regel) als auch abgelehnt (durch eine zweite Regel) ist, ist sie tatsächlich zulässig.
- Sternchen und CIDR-Blöcke werden derzeit nicht unterstützt.
- In Bezug auf weitergeleitete Proxy-Adressen werden die Allow-Regeln auf jede Adresse in der Kette angewendet und dann die Deny-Regeln auf jede Adresse in der Kette angewendet, wenn keine der Allow-Regeln übereinstimmt.
- Die auf dem IP-Bereich basierende Authentifizierung kann sich auf die Übertragung von Update Sets auswirken. Wenn die IP-Adresszugriffssteuerung für die Quellinstanz aktiviert ist, fügen Sie die IP-Adressen aller Anwendungsknoten hinzu, die Ihre Instanz als Ausnahmen unterstützen.

Hinweis:
Um die IP-Informationen Ihrer Instanz zu finden, melden Sie sich bei an ServiceNow NOW-Support , und Suchen Sie nach dem Servicekatalogelement „ **Meine IP-Informationen** “.

Hinweis:
Weitere Informationen zu den Eigenschaften `com.snc.ipauthenticator` und `glide.ip.authenticate.strict`, die den Instanzzugriff auf bestimmte IP-Bereiche einschränken, finden Sie unter den folgenden Themen unter Härtungseinstellungen für Instanzsicherheit:

- Beschränken Sie den Zugriff auf bestimmte IP-Bereiche
- Strikte IP-Einschränkung

IP-Adressen-Zugriffssteuerung

Wenden Sie eine IP-Zugriffssteuerung auf ausgehenden Datenverkehr, eingehenden Datenverkehr oder bidirektionalen Datenverkehr an. Das System blockiert eine IP-Adresse nur, wenn eine übereinstimmende Deny-Regel vorhanden ist und keine übereinstimmende Allow-Regel vorhanden ist. Standardmäßig gibt es keine Einschränkungen für den Zugriff auf Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Verwenden Sie die Vorauthentifizierungskontextrichtlinie der adaptiven Authentifizierung (AA), um IP-basierte Authentifizierungen und Einschränkungen für zusätzliche Funktionen zu erzwingen. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung** , um eine Liste Ihrer IP-Zugriffssteuerungen anzuzeigen.
   Möglicherweise müssen Sie das Plugin „IP Range Based Authentication“ [com.snc.ipauthenticator] aktivieren.
2. Füllen Sie das Formular aus.

Hinweis:
Um die IP-Informationen Ihrer Instanz zu finden, melden Sie sich bei an ServiceNow NOW-Support , und Suchen Sie nach dem Servicekatalogelement „ **Meine IP-Informationen** “.

Feld	Beschreibung
Typ	Typ der einzubeziehenden Zugriffskontrollregel. ○ *Zulassen*: Jede IP-Adresse in diesem Bereich kann mit dieser Instanz interagieren. ○ *Deny*: Eine IP-Adresse in diesem Bereich kann nicht mit dieser Instanz interagieren, es sei denn, sie ist in einer Allow-Regel aufgeführt. Außerdem können Sie beim Hinzufügen von Deny-Regeln Ihre eigene öffentliche IP-Adresse nicht ablehnen, oder Ihre Instanz aktualisiert keine Deny-Regel. **Hinweis:** Zur Unterstützung von Wartung, Upgrades und Kundenservice und Supportkönnen einige interne IP-Adressen von ServiceNow nicht durch Deny-Regeln blockiert werden.
Richtung	Richtung der IP-Zugriffskontrollregel. ○ **Eingehend**: Erlaubt oder verweigert eingehende Transaktionen. Dies sind Transaktionen, die von außerhalb Ihrer Instanz initiiert werden. ○ **Ausgehend**: Erlaubt oder verweigert ausgehende Transaktionen. Dies sind Transaktionen, die von Ihrer Instanz aus initiiert werden. ○ **Bidirektional**: Ermöglicht oder verweigert eingehende und ausgehende Transaktionen.
Aktiv	Wenn diese Option ausgewählt ist, ist das Formular aktiv.
Beschreibung	Beschreibung der Zugriffssteuerung.
Bereichsstart	Startbereich von IP-Adressen, die zugelassen oder verweigert werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Diese Regeln wirken sich auch auf die Übertragung von Update Sets aus. Um sicherzustellen, dass die IP-Adresszugriffssteuerung nicht zum Fehlschlagen von Update Sets führt, fügen Sie die Zielinstanz als Ausnahme hinzu.
Bereichsende	Endbereich von IP-Adressen, die zugelassen oder verweigert werden sollen. **Hinweis:** Um den Zugriff nur auf bestimmte VPN-Adressen zu beschränken, geben Sie in das Feld **Deny** einen Deny-Bereich von **0.0.0.0** bis **255.255.255.255** ein, und geben Sie nur die spezifischen zulässigen VPN-Bereiche ein.

3. Klicken Sie auf **Absenden**.

Suchen Sie nach abgelehnten IP-Adressen

Suchen Sie in den Knotenprotokolldateien der Instanz nach abgelehnten IP-Adressen.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Protokolleinträge für blockierte IP-Adresse werden wie folgt angezeigt: `2015-10-21 18:37:43 (175) http-30 WARNUNG *** WARNUNG *** Sicherheit eingeschränkt: Zugriff eingeschränkt (xx.xx.xxx.xxx nicht autorisiert).`

Hinweis:
Abgelehnte IP-Adressen sind die Knotenprotokolldateien der Instanz, die in den Systemprotokollen nicht angezeigt werden können.

Prozedur

1. Navigieren zu **Alle** > **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Browser**.
2. Durchsuchen Sie die Protokolle nach Kriterien wie Zeitraum und Nachricht.
3. Sie können Protokolldateien auch herunterladen, wenn Sie wissen, nach welchem Protokoll Sie suchen, indem Sie zu navigieren **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**.

Implementieren einer Nonce

Sie können eine Nonce implementieren, die mit der Single Sign-on-Digest-Authentifizierung verwendet werden soll.

Um eine Nonce mit den unverschlüsselten oder verschlüsselten Token-Methoden des Single Sign-on zu verwenden, gelten diese Schritte mit nur wenigen geringfügigen Änderungen.

Hinweis:
Die Nonce wird nur für Anmeldeanforderungen verwendet, nicht für andere Arten von Anforderungen. Wenn das System nach der Anmeldung einen Nonce-Wert erhält, wird die Nonce nicht verbraucht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile

Die Verwendung einer Nonce verhindert, dass ein böswilliger Benutzer einen Wiederholungsangriff ausführt, um sich bei Ihrem System anzumelden.

Nonce-Prozess-Flow

Wenn ein Kunde das Single Sign-on für verarbeitete Token implementiert hat und die Sicherheit einer Nonce hinzufügen möchte, folgt er einem bestimmten Prozess-Flow.

1. Ein Benutzer meldet sich beim Portal des Kunden an.
2. Der Kunde generiert die erforderlichen SSO-Parameter und hängt eine zufällige Nonce an das Ende an. Wenn der Kunde beispielsweise die Authentifizierungsantwort über die Abfragezeichenfolge weitergeleitet hat, kann dies in etwa so aussehen:

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

Die Instanz empfängt diese Anforderung und ruft die Authentifizierungsvariablen ab. Bevor versucht wird, die Integrität der Authentifizierungsantwort zu überprüfen, gleicht die Instanz die Nonce mit einer internen Tabelle (u_authentication_nonce) ab, um sicherzustellen, dass sie noch nicht vorhanden ist. Wenn die Nonce in dieser Tabelle nicht vorhanden ist, wird die Nonce der Tabelle hinzugefügt, und der Authentifizierungsprozess kann fortgesetzt werden. Wenn dieser Nonce-Wert jedoch bereits in der Tabelle vorhanden ist, wird der Authentifizierungsversuch abgebrochen und der Fehlercode „failed_missing_requirement“ zurückgegeben, der den Benutzer normalerweise zur Anmeldeseite zurückführt.

Implementieren Sie eine Nonce

Fügen Sie dem Authentifizierungsheader eine kryptografische Nonce hinzu, um sicherzustellen, dass sie nur einmal verwendet werden kann.

- Erstellen Sie eine Systemeigenschaft mit dem Namen *glide.authenticate.header.nonce_key*, und legen Sie ihren Wert auf den Variablennamen fest, den Sie für die Nonce verwenden, z. B. NONCE oder NCE.
- Erstellen Sie eine neue Tabelle mit dem Namen u_authentication_nonce. Fügen Sie der Tabelle u_nonceein Feld hinzu.
- Gehe zu **Systemeigenschaften** > **Installationsausgänge** und erstellen Sie ein Element namens DigestSingleSignOnNonce, das ExternalAuthentication (*glide.authenticate.external_property*) überschreibt.
- Fügen Sie dem Skriptteil des neu erstellten DigestSingleSignOnNonce den folgenden Code hinzu.

```
gs.include("PrototypeServer");

var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {

 process : function() {

 var headerKey = GlideProperties.get("glide.authenticate.header.key", "SM_USER");
 var headerDigestKey = GlideProperties.get("glide.authenticate.header.encrypted_key",
"DIGEST");
 var headerNonceKey = GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
 var fieldName = GlideProperties.get("glide.authenticate.header.value", "user_name");
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var fkey = GlideProperties.get("glide.authenticate.secret_key");

// Look in the Headers
var data = request.getHeader(headerKey);
var encdata = request.getHeader(headerDigestKey);
var nonce = request.getHeader(headerNonceKey);

// If not, then check the URL Parameters
if (data == null || encdata == null || nonce == null) {
 data = request.getParameter(headerKey);
 encdata = request.getParameter(headerDigestKey);
 nonce = request.getParameter(headerNonceKey);
}

// then maybe its a cookie
if (data == null || encdata == null || nonce == null) {
 var cookies = request.getCookies();
 data = GlideCookieMan.getCookieValue(cookies, headerKey);
 encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
 nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
}

// if found run encryption
if (data != null && encdata != null && nonce != null) {
 try {

  // Replace all spaces with plus(+)'s, converted in url
  encdata = encdata.replaceAll(' ', '+');

  // ----- Encrypt the username|nonce
  var key = this.getDigest( data + "|" + nonce, fkey);

  // Check for match of received encoded data
  // and your encoding of user name
  if (encdata == key) {
   var ugr = new GlideRecord("sys_user");
   ugr.initialize();
   if (!ugr.isValidField(fieldName)) {
    GlideLog.warn("External authorization is set to use field: '"+ fieldName + "' which doesn't
exist");
    return "failed_missing_requirement";
   }
   ugr.addQuery(fieldName, data);
   ugr.query();
   if (!ugr.next()) {
    var userLoad = GlideUser.getUser(data);
    if (userLoad == null)
     return "failed_authentication";

    ugr.initialize();
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next())
     return "failed_authentication";

   }
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    if (this.processNonce(nonce)){
     var userName = ugr.getValue("user_name");
     return userName;
    }
    else return "failed_missing_requirement";
    }
   else {

    return "failed_authentication";
   }
  } catch(e) {
   gs.log(e);
   return "failed_authentication";
  }
  // Encoded data didn't match recieved Encoded data
 } else {

  return "failed_missing_requirement";
 }
},

getDigest : function( data, fkey ) {
 try {
  // default to something JDK 1.4 has
  var MAC_ALG = "HmacSHA1";
  return SncAuthentication.encode(data, fkey, MAC_ALG);

 } catch (e) {
  gs.log(e.toString());
  throw 'failed_missing_requirement';
 }
} ,

processNonce : function( sentNonce ) {
 var ngr = new GlideRecord("u_authentication_nonce");

 ngr.addQuery("u_nonce", sentNonce);
 ngr.query();
 if (ngr.next()) {
  gs.log("This SSO entry has already been processed! (Nonce: " + sentNonce + ")");
  return false;
 }
 var ngrNew = new GlideRecord("u_authentication_nonce");
 ngrNew.initialize();
 ngrNew.u_nonce = sentNonce;
 ngrNew.insert();
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
}
};
```

- Sobald Sie Ihre neue Installations-Exit gespeichert haben, wechseln Sie zur DigestSingleSignOn-Installations-Exit, und stellen Sie sicher, dass Active=false festgelegt ist.

Ihre Instanz sollte jetzt für die Implementierung einer Nonce konfiguriert sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Webservice-Sicherheit

Erzwingen Sie Sicherheit mithilfe von Basic Authentication, gegenseitiger Authentifizierung oder WS-Security.

Untersuchen Sie die Websicherheit

Machen Sie sich mit den Funktionen und Geschäftsnutzen der Webservice-Sicherheit vertraut.

Konfigurieren Sie die gegenseitige Authentifizierung

Machen Sie sich mit der Verwendung und Konfiguration der gegenseitigen Authentifizierung vertraut.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Webservice-Sicherheit

Erfahren Sie mehr über die Sicherheit von Webservices.

Sicherheit von Webservices erkunden

Erzwingen Sie Sicherheit mithilfe von Basic Authentication, gegenseitiger Authentifizierung oder WS-Security.

Standardauthentifizierung

Um die Basic Authentication bei jeder Anforderung für ein WSDL-Dokument oder beim Senden von SOAP-Nachrichten zu erzwingen, können Sie die Eigenschaft *glide.basicauth.required* auf truesetzen. In diesem Fall muss jede WSDL- oder SOAP-Anforderung die Autorisierungskopfzeile enthalten, wie im Standardauthentifizierungsprotokoll angegeben. Da die Anforderung nicht interaktiv ist, ist die **Autorisierungskopfzeile** immer während einer Anforderung erforderlich.

Die Bereitstellung von Basic Authentication-Informationen, unabhängig davon, ob dies erforderlich ist oder nicht, hat den zusätzlichen Vorteil, dass die Daten, die als Ergebnis des Webservice-Aufrufs erstellt oder aktualisiert werden, im Namen des Benutzers ausgeführt werden, der in den Basic Authentication-Anmeldeinformationen angegeben ist. Beispiel: Beim Erstellen eines Incident-Datensatzes enthalten die Journalfelder die Benutzer-ID des authentifizierten Standardbenutzers anstelle des Standardbenutzers **Gast**.

Verwenden Sie die Eigenschaft *glide.security.script.include.name.case.insensitive.list*, damit der Autorisierungsheader die Kapitalisierungsregeln ignoriert. Sie können diese Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] ändern und die Skripteinbindungen hinzufügen, die für die Verarbeitung der Authentifizierung erforderlich sind. Standardmäßig hat diese Eigenschaft die folgenden Werte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- BasicAuth
- CustomAuth

Fügen Sie nach Bedarf weitere Skripteinbindungen hinzu.

Um die Basic Authentication bei Verwendung von Perl und der SOAP::Lite-Bibliotheken bereitzustellen, können Sie die folgende Funktion implementieren:

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return 'user_name' =>
 'password' ; }
```

- Wenn Sie C# .NET VS 2005 oder älter verwenden, können Sie das Objekt „Anmeldeinformationen“ nutzen, z. B.:

```
System.Net . ICredentials cred  = new System.Net . NetworkCredential ( "user_name",
 "password" ) ;

service . ServiceNow proxy  = new service . ServiceNow ( ) ;
service . get getService  = newservice . get ( ) ;
service . getResponse getServiceResponse  = new service . getResponse ( ) ;

 try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse  = proxy . get (getService ) ; catch (Exception ex ) { }
```

- Wenn Sie C# .NET VS 2008 verwenden, können Sie das ClientCredentials-Objekt nutzen, z. B.:

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService . Demo_Incident .
 ServiceNowSoapClient ( ) ;
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

  Suchen Sie dann in Ihrer Datei app.config nach Folgendem, und ändern Sie `None` in `Basic`:

```
<transport clientCredentialType= "None" proxyCredentialType= "None" realm= "" />
```

- Bei der Verwendung von VB .NET würde das Objekt „Anmeldeinformationen“ folgendermaßen aussehen:

```
Sub Main()
        Dim cred  As New System.Net.NetworkCredential( "user_name",  "password")

        Dim proxy  As New VB_Democm.incident.ServiceNow
        Dim getIncident  As New VB_Democm.incident. get Dim getResponse  As New
 VB_Democm.incident.getResponse

       proxy.Credentials = cred

       getIncident.sys_id =  "[your sysID here]"

       getResponse = proxy. get(getIncident)

    End Sub
```

  Die resultierende Antwort, wenn die Basic Authentication aktiviert ist und keine Anmeldeinformationen angegeben werden, sieht folgendermaßen aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<html> <head > <title >Apache Tomcat/5.0.28 - Error report </ title > <style > <!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
 H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;}
 H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;}
   BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;}
 B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}    P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}   A
{color : black;}   A.name {color : black;}   HR {color : #525D76;}--> </
style > </ head > <body > <h1 >HTTP Status 401 -\ </ h1 > <HR size = "1" noshade =
"noshade" > <p >< b >type </ b > Status report </ p > <p >< b >message </ b > <u >< /
u >< / p > <p >< b >description </ b > <u >This request requires HTTP authentication ().
</ u >< / p > <HR size = "1" noshade = "noshade" > <h3 >Apache Tomcat/5.0.28 </ h3 >
</ body > </ html >
```

Konfigurieren der gegenseitigen Authentifizierung

Die gegenseitige Authentifizierung stellt Vertrauen her, indem SSL-Zertifikate (Secure Sockets Layer) ausgetauscht werden.

Vor dem Herstellen einer Verbindung mit einem Server fordert der Client ein SSL-Zertifikat an. Der Server antwortet, indem er anfordert, dass der Client sein eigenes Zertifikat sendet. Beide reagieren, indem sie die Zertifikate validieren und Bestätigungen senden, bevor eine HTTPS-Verbindung initiiert wird.

Administratoren führen die Vorarbeiten durch, indem sie einen Schlüsselspeicher einrichten und Zertifikate generieren, bevor Zertifizierungsanforderungen erfüllt werden.

⚠ Warnung:
Diese Funktion ermöglicht nur die gegenseitige Authentifizierung bei ausgehenden HTTPS-Verbindungen.

Erstellen des Schlüsselspeichers

Die Instanz unterstützt derzeit das Hochladen einer Java-Schlüsselspeicherdatei, die den privaten Schlüssel, das öffentliche Zertifikatpaar und die signierten Zertifikate enthält.

In den folgenden Schritten werden Befehle verwendet, mit denen Sie eine neue Java Keytool-Schlüsselspeicherdatei generieren, eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) erstellen und Zertifikate importieren können. Alle Stamm- oder Zwischenzertifikate müssen importiert werden, bevor das primäre Zertifikat für Ihre Domäne importiert wird. Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein.

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Importieren Sie ein CA-Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Importieren Sie ein signiertes primäres Zertifikat in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

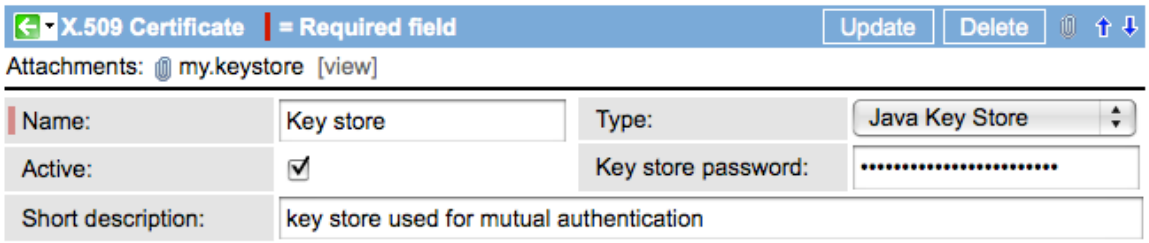
Einrichten des Schlüsselspeichers

Nachdem der Schlüsselspeicher erstellt wurde, kann er in die Zertifikattabelle hochgeladen werden. Auf der **Systemdefinition** > **Zertifikate** Klicken Sie auf der -Seite auf **Neu**, und legen Sie die folgenden Felder fest:

- Geben Sie einen **Zertifikatnamen**ein.
- Speichern Sie den Schlüsselspeicher als **Active**.
- **Typ festlegen = Java Key Store**.
- Geben Sie ein **Passwort für den Schlüsselspeicher an**. Dies ist das Passwort, das zum Erstellen des Schlüsselspeichers verwendet wurde.

Klicken Sie auf **Absenden**, um den Java Key Store-Eintrag zu erstellen.

Schlüsselspeicher



Angeben eines vertrauenswürdigen Serverzertifikats

Während einer ausgehenden SSL-Verbindung, bei der es sich um einen HTTPS-Webservice-Aufruf handelt, kann ein vom Service Provider bereitgestelltes Zertifikat angegeben werden, das die Gültigkeit des Service Providers während der SSL-Verbindung sicherstellt. Zum Beispiel ein Browser, der versucht, eine Verbindung zu einem sicheren Service herzustellen, der sich durch ein Zertifikat identifiziert.

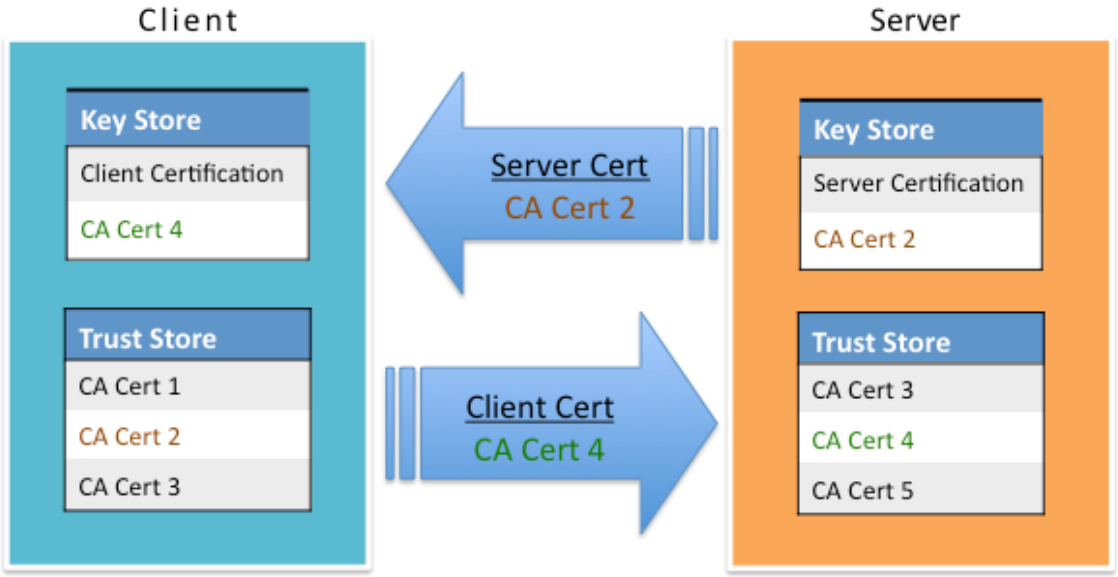
Durch das Hochladen des vertrauenswürdigen Serverzertifikats stellt ServiceNow sicher, dass der Service, mit dem eine Verbindung hergestellt wird, gültig und sicher ist.

Erstellen Sie einen neuen Zertifikateintrag mit dem Typ „Trust Store-Zertifikat“, und hängen Sie ein DER-formatiertes Zertifikat an, oder kopieren Sie das PEM-Format, und fügen Sie es in das Feld **PEM-Zertifikat** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen der gegenseitigen Authentifizierung werden verarbeitet

Zertifikataustausch



- Wenn ein Client das Serverzertifikat zur Authentifizierung anfordert, wird eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) generiert.
- Um auf eine CSR zu antworten, generiert der Server zwei eindeutige kryptografische Schlüssel: einen öffentlichen Schlüssel, der zum Verschlüsseln von Nachrichten an den Server verwendet wird, und einen privaten Schlüssel, der zum Entschlüsseln von Nachrichten verwendet wird. Beide Schlüssel werden im Schlüsselspeicher gespeichert.
- Schlüssel werden verwendet, um die sicheren Nachrichten des Clients zu entschlüsseln, damit sie vom Server gelesen werden können. Jede ausgehende Verbindung, die über HTTPS hergestellt wird, überprüft die Zertifizierung, indem sie den Schlüsselspeicher überprüft, seine öffentliche Zertifizierung anbietet und die Truststore-Zertifikate verwendet, um das gegenseitige Vertrauen zu überprüfen.
- Um die sichere Verbindung zwischen Client und Server herzustellen, gleicht der Server das Zertifikat mit dem entsprechenden privaten Schlüssel ab. Da nur der Server Zugriff auf den privaten Schlüssel hat, kann der Server die Daten vom Client entschlüsseln.

Hier ein Beispiel für einen Befehl, der MYHTTPS mit der Socket Factory `com.glide.certificates.DBKeyStoreSocketFactory` an Port 443 registriert. Die Schlüsselspeicher-Werkseinstellung der Datenbank wird während des SSL-Austauschvorgangs verwendet, um ein Client-Zertifikat für die gegenseitige Authentifizierung bereitzustellen.

```
glide.httpclient.protocol.myhttps.class = "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```

Die obige Konfiguration wirkt sich auf alle ausgehenden `myhttps://host.domain.com/target-URLs` aus, um die benutzerdefinierte Socket-Werkseinstellung zu verwenden und Zertifikate während SSL auszutauschen.

Hinweis:
Das Überschreiben der standardmäßigen HTTPS-Protokoll-Socket-Werkseinstellung wirkt sich auf jede ausgehende HTTPS-Verbindung aus. Dies ist normalerweise unerwünscht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Server antwortet mit dem Senden eines Zertifikats. Ist dies ein Zertifikat, das der Client akzeptiert? Wenn ja, wird eine Nachricht an den Server gesendet, der das Zertifikat akzeptiert, und ein sicherer Kanal wird initiiert. Wenn das Zertifikat nicht akzeptiert wird, kann dies bedeuten, dass die Stammautorität für die Zertifizierung erforderlich ist.

Referenz: WS-Security

Unterstützung für WS-Security 1.1 in Form von WSS X.509-Token-Profil und WSS-Benutzernamen-Token-Profil ist für eingehende SOAP-Anforderungen verfügbar.

Die Konfiguration zur Verwendung von WS-Security ist unabhängig von der Anforderung zum Erzwingen der Standardauthentifizierung und wird erzwungen, wenn der SOAP-Umschlag die WS-Security-Header enthält.

WS-Sicherheitsprofile

Das Modul „ **WS** -Sicherheitsprofil“ listet die derzeit gültigen WS-Sicherheitsprofile auf. Die **Reihenfolge** der Profile gibt die Reihenfolge der Authentifizierung an, die überprüft wird. Alle Profile werden während der eingehenden SOAP-Anforderung überprüft. Wenn die Authentifizierung eines Profils fehlschlägt, wird das nächste Profil in der Reihenfolge nicht ausgeführt. Die **Checkbox Sitzung** binden gibt an, welches Profil verwendet werden soll, um die Identität der Sitzung anzunehmen. Es kann nur eine „gebundene“ Sitzung geben.

WSS X.509-Token-Profil

Verwenden Sie das X.509-Authentifizierungs-Framework, wie durch Webservices-Sicherheit: Spezifikation für die SOAP-Nachrichtensicherheit definiert. Ein X.509-Zertifikat gibt eine Bindung zwischen einem öffentlichen Schlüssel und einem Satz von Attributen an, der (mindestens) einen Antragstellernamen, einen Ausstellernamen, eine Seriennummer und ein Gültigkeitsintervall enthält. Ein X.509-Zertifikat wird zum Überprüfen eines öffentlichen Schlüssels verwendet, mit dem die eingehende SOAP-Nachricht signiert wird. Laden Sie das Zertifikat in das **Zertifikatmodul** hoch, und referenzieren Sie es im Feld **X509-Zertifikat**. Wenn dies eine gebundene Sitzung ist, wählen Sie den Benutzer aus, dessen Identität angenommen werden soll, wenn die WS-Security-Authentifizierung erfolgreich ist.

Weitere Informationen finden Sie im folgenden Dokument: http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf

WSS-Benutzernamen-Token-Profil

Zusätzlich zur Angabe des X.509-Token-Profils kann in der SOAP-Anforderung auch ein UsernameToken angegeben werden. Ein UsernameToken wird verwendet, um die anfordernde Person anhand „username“ zu identifizieren und optional ein Passwort (oder einen gemeinsamen geheimen Schlüssel oder ein entsprechendes Passwort) zu verwenden, um diese Identität gegenüber der Instanz zu authentifizieren. Das UsernameToken-Profil kann derzeit nicht unabhängig vom X.509-Token-Profil verwendet werden.

1. Authentifizieren Sie sich mit dem Benutzernamen der eingehenden SOAP-Anforderung, um einen Benutzer im angegebenen **Feld Benutzer zu suchen, um den Wert UserName abzugleichen**. Der Passwortwert im eingehenden Benutzernamen-Token wird zur Authentifizierung der Anforderung verwendet. Wenn die Option **Sitzung** binden ausgewählt ist, wird der Benutzer, der sich erfolgreich authentifiziert, für die Sitzung verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Authentifizieren Sie sich mit einem separaten Paar aus Benutzername/Passwort, das nicht zu Benutzern in der Benutzertabelle gehört. Wenn die Option **Sitzung** binden ausgewählt ist, wird der Benutzer, der im Feld **Als Benutzer** ausführen angegeben ist, für die Sitzung verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel WS-Security SOAP-Umschlag-Header

Hinweis:

Dieses Beispiel wurde mit Zeilenumbrüchen formatiert, damit der Inhalt in den Frame passt.

```
<SOAP-ENV:Header><wsse:Securityxmlns:wsse =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
SOAP-ENV:mustUnderstand = "1" ><wsse:BinarySecurityTokenxmlns:wsu =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"E
ncodingType =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0
#Base64Binary"ValueType =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X50
9v3"wsu:Id = "CertId-2D914AB929A6719E7F13068829874641"xmlns:wsse =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
 >
  MIIEgzCCA2ugAwIBAgILAQAAAAABLOZQMtEwDQYJKoZIhvcNAQ
  EFBQAwQDEXMBUGA1UEChMOQ3liZXJ0cnVzdCBJbmMxJTAjBg
  NVBAMTHEN5YmVydHJ1c3QgU3VyZWNyZWRlbnRpYWwgQ0Ew
  HhcNMTAxMjE0MTgyMjU1WhcNMTECMjE0MTgyMjU1WjB3MQsw
  CQYDVQQGEwJVUzEUMBIGA1UEChMLU2VydmljZS1Ob3cxKDA
  mBgkqhkiG9w0BCQEWGWRhdmlkLmxvb0BzZXJ2aWNlLW5vdy5jb
  20xKDAmBgNVBAMTH1NlcnZpY2UtTm93IFBhcn3uZXIgRGV2ZWx
  vcG1lbnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
  AQCvtcRIb6zkGnN9uyhtcSDNSIuCW6FgnTbTDUvw2nGlNA9y9iEV
  wTp5TG3eELOOFBCuRLeY5x28lN+cJ72v+zCwi/rZcbEPj8oWyLVA
  OqJThgrzhDabj0vDM/zU8bvAXcw6FoCUDFKkc64WC7Y4HpBdfW4
  JT7FBgDQ3LEudq80Up+TfETiGwrEA3jRgy9fF92TKD7MN3Vkyhz2
  xZLOFiN5HJixl9juNJmLWugqqIG04yZSuCutc1gjCy0U+f0NXKgh0Q
  rRheNpwcqWbbJvLbR9Ybso6l3UAYCQ09hrRnI7VaPvfiueUvuLopap
  o4Kel6iL8aMUAfEUDtkf1AbqRIIQ5AgMBAAGjggFFMIIBQTAfBgNVH
  SMEGDAWgBRJTJlLzUojts557p5VM2taRMAClTA7BgNVHR8ENDA
  yMDCgLqAshipodHRwOi8vY3JsLm9tbmlyb290LmNvbS9TdXJlQ3JlZ
  GVudGlhbC5jcmwwHQYDVR0OBBYEFB+OqIvcdiYmq0enW6mgaV
  wZp9eaMA8GA1UdEwEB/wQFMAMCAQAwDgYDVR0PAQH/BAQD
  AgTwMBEGCWCGSAGG+EIBAQQEAwIFoDBJBg3rBgEFBQcBA1Q
  9MDswOQYIKwYBBQUHMAKGLWh0dHA6Ly9jYWNlcnQub21uaXJv
  b3QuY29tL3N1cmVjcmVkZW50aWFsLmNydDAkBgNVHREEHTAbg
  RlkYXZpZC5sb29Ac2VydmljZS1ub3cuY29tMB0GA1UdJQQWMBQG
  CCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQUFAAO
  CAQEAmeoP0Bgtx2JN1ldLnnK6WLEqDk25zaHP5wTxqVlFxzJy1zi6
  A0lk5U0T5LKYjjGWRIOoSeK8iBU0p7Mq4PE8QCETkjYNyuWJd9zm
  7GPCHdOoL18rQHQRsU8pTDHA10zG+i3zdxAMrHl/H673E4myzvU
  DkJnxNAZdw4h4Ba/Y1+VFCWhOm2GwZdXtzklyZaKtMp+31qmf3bG
  OSU34M/dW40pXgfLDqdGD+6YDQPg25aYeCqcNhwg6VlAWG566g
  aWXYxRaVj0qotSDMdaK8b+7Vlo7KhGGaE62v7f44OSekJeBvTfZCR
  7zRSK8N+0qUpqP/n8vgDkmYIE5IQrRE0rEWA==
 </wsse:BinarySecurityToken><ds:Signature xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#"Id = "Signature-2" ><ds:SignedInfo xmlns:ds
= "http://www.w3.org/2000/09/xmldsig#" ><ds:CanonicalizationMethodAlgorithm
= "http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /><ds:SignatureMethod
Algorithm = "http://www.w3.org/2000/09/xmldsig#rsa-sha1"xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /><ds:Reference URI = "#Timestamp-1"
xmlns:ds = "http://www.w3.org/2000/09/xmldsig#" ><ds:Transforms
xmlns:ds = "http://www.w3.org/2000/09/xmldsig#" ><ds:Transform
Algorithm = "http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /></ds:Transforms><ds:DigestMethod
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

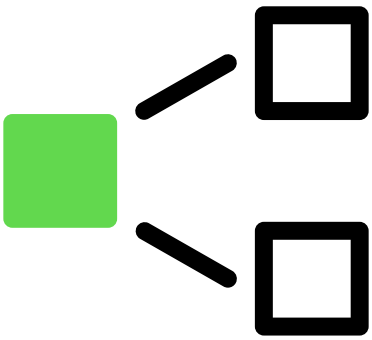
Allgemeine Einstellungen für Plattformsicherheit

Erfahren Sie mehr über die allgemeinen Einstellungen für Plattformsicherheit.

Antivirus-Scanfunktionen

Verwenden Sie Antivirus-Scanning, um Ihre Instanz vor Virusinfektionen zu schützen, die durch Dateianhänge an Ihre Systemdatensätze wie Incidents, Probleme und Storys eingeführt werden können.

HTML-Bereinigung

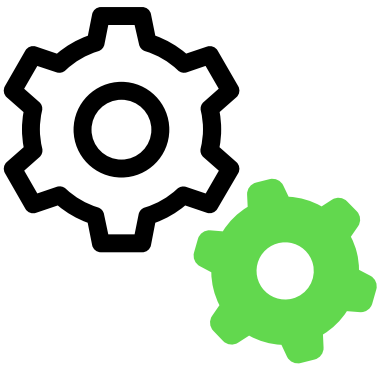


Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Auditing

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Strenge Sicherheitseinstellungen



Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

ServiceNow® Zugriffssteuerung

Mit dem Plugin „SNC Access Control“ können Sie steuern, welche Kundenservice und Support-Mitarbeiter wann auf Ihre Instanz zugreifen können.

Virtuelles privates Netzwerk (VPN)

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere Einstellungen und Sicherheitsressourcen

Legen Sie Sicherheitseigenschaften außerhalb von Instance Security Center fest, das auch andere sicherheitsbezogene Ressourcen enthält.

Antivirus-Scanning

Schützen Sie mit Antivirus-Scanning Ihre Instanz vor Virusinfektionen, die durch Dateianhänge Ihrer Systemdatensätze wie Incidents, Probleme und Storys eingeschleust werden können.

HTML-Bereinigung

Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Auditing

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Strenge Sicherheitseinstellungen

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

ServiceNow®-Zugriffssteuerung

Mit dem Plugin „SNC Access Control“ können Sie steuern, welche Kundenservice und Support-Mitarbeiter wann auf Ihre Instanz zugreifen können.

Andere Einstellungen und Sicherheitsressourcen

Legen Sie Sicherheitseigenschaften außerhalb von Instance Security Center fest, das auch andere sicherheitsbezogene Ressourcen enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtuelles privates Netzwerk (VPN)

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Antivirus-Scanning

Schützen Sie mit Antivirus-Scanning Ihre Instanz vor Virusinfektionen, die durch Dateianhänge Ihrer Systemdatensätze wie Incidents, Probleme und Storys eingeschleust werden können.

Erkunden Sie Antivirus-Scans

Erfahren Sie den Wert von Antivirus Scanning.

Konfigurieren Sie Antivirus-Schutz

Machen Sie sich mit der Konfiguration des Virenschutzes vertraut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Infizierte Dateien auflösen

Erfahren Sie, was mit infizierten Dateien zu tun ist.

Referenz für Antivirus-Scans

Informieren Sie sich über die Wörterbuchattribute für Antivirus-Scans.

Antivirus-Scanning erkunden

Schützen Sie mit Antivirus-Scanning Ihre Instanz vor Virusinfektionen, die durch Dateianhänge Ihrer Systemdatensätze wie Incidents, Probleme und Storys eingeschleust werden können.

Antivirus-Scanning Durchsucht Dateianhänge, die in der Anhangtabelle [sys_attachment] gespeichert sind, um Benutzer vor dem Hochladen und Herunterladen infizierter Dateien zu schützen. Alle von der Plattform unterstützten Dokumenttypen werden von Antivirus Scanning gescannt.

Das Plugin Virenschutz (com.glide.snap) ist in Ihrer Instanz standardmäßig aktiviert. Als Administrator können Sie die Funktion Antivirus-Scanning in Ihrer Instanz per Umschalter deaktivieren und erneut aktivieren, Konfigurationsoptionen festlegen und die Antivirenaktivität für die Instanz überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Antivirus-Scanning ist auch für Kunden in der Government Community Cloud (GCC) und einer kommerziellen Umgebung verfügbar. Benutzer müssen die Eigenschaft (com.glide.snap.fed_enable_scan) auf True festlegen, um die Funktion verwenden zu können.
- Die Kommunikationsprotokolle HTTP und HTTPS werden unterstützt.
- Edge-verschlüsselte Dateien werden von diesem Scan ausgeschlossen.
- Virenschutzdefinitionen werden täglich aktualisiert.
- Dateien mit einer Dateigröße über 100 MB werden nicht gescannt.

Scannen von E-Mails und Anhängen

Eingehende E-Mails werden nicht von Antivirus-Scanning, sondern von den System-E- Mail-Filtern auf Viren gescannt.

Standardmäßig werden nur Anhänge gescannt, die an die Tabellen „zz_yylive_profile“ angehängt sind. Um andere Tabellen mit dem **Spaltentyp file_attachment** zu scannen, erstellen Sie die Systemeigenschaft `glide.snap.scan.zz_yytable`, und fügen Sie den Tabellennamen ein.

Wenn die Tabellennamen zz_yyincident und zz_yycase lauten, muss der Eigenschaftswert `zz_yyincident,zz_yycase`lauten.

Nachdem diese Eigenschaft festgelegt wurde, werden Anhänge für die Tabellen „zz_yyincident“ und „zz_yycase“ gescannt.

Scan-Szenarien

Überprüfen Sie diese Upload- und Download-Szenarien, um zu verstehen, wie das System potenzielle Sicherheitsbedrohungen aus Dateien erkennt, die an Ihre Datensätze angehängt sind.

Szenario 1: Datei hochladen

1. Der Benutzer lädt unwissentlich eine infizierte Datei in einen Datensatz hoch.
2. Das System scannt die Datei und verschiebt sie in die Quarantäne.
3. Die Datei wird im Fenster „Anhänge“ angezeigt, in dem sie als nicht verfügbar markiert ist.
4. Der Benutzer wählt die Datei aus, und diese Fehlermeldung wird angezeigt:
   Die Datei Infected_testing.txt hat die Sicherheitsprüfung nicht bestanden.
   Entfernen Sie die Datei aus Datensatz INC0000059, und versuchen Sie es erneut.
5. Das System sendet eine E-Mail-Benachrichtigung an den Benutzer und den Virenschutzadministrator.
6. Der Benutzer schließt das Fenster „Anhänge“ und kehrt zum Datensatz zurück. Die infizierte Datei wird im Header als nicht verfügbar angezeigt. Beispiel, infizierte_testing123.txtZ [nicht verfügbar].

Szenario 2: Datei herunterladen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Der Benutzer öffnet einen Datensatz, um eine angehängte Datei herunterzuladen.
2. Der Benutzer weiß nicht, dass die Datei infiziert ist, und wählt sie zum Download aus.
3. Das System scannt die Datei, verschiebt sie in die Quarantäne und zeigt eine Meldung ähnlich der folgenden an: Die Datei infiziert_testing123.txt hat die Sicherheitsprüfung nicht bestanden und kann nicht heruntergeladen werden.
4. Der Benutzer schließt die Nachricht, und der Bildschirm wird aktualisiert und zeigt an, dass die Datei nicht verfügbar ist.
5. Das System sendet eine E-Mail-Benachrichtigung an den Benutzer und den Virenschutzadministrator.

Szenario 3: ZIP-Datei herunterladen

1. Ein Benutzer öffnet einen Datensatz und lädt eine angehängte ZIP-Datei herunter.
2. Das System scannt die ZIP-Dateien einzeln.
3. Eine Datei besteht die Sicherheitsprüfung nicht und wird als nicht verfügbar markiert. Die verbleibenden Dateien wurden komprimiert und erfolgreich heruntergeladen.
4. Der Benutzer öffnet die ZIP-Datei und sieht zusätzlich zur erfolgreich heruntergeladenen Datei die Datei „error.txt“. Diese Datei enthält eine Fehlermeldung, die angibt, welche Datei den Scan nicht bestanden hat und daher nicht in die ZIP-Datei aufgenommen wurde.
5. Der Benutzer öffnet den Datensatz erneut und sieht, dass die nicht verfügbare Datei in den Abschnitt „ **Potenzielle Sicherheitsrisiken** “ im Fenster „Anhänge“ verschoben wurde und nicht heruntergeladen werden kann.

Antivirus-Scanning konfigurieren

Konfigurieren Sie Antivirus-Scanning in Ihrer Instanz und auf Tabellenebene.

Vorbereitungen

Erforderliche Rolle: antivirus_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Antivirus-Scanning ist standardmäßig in Ihrer Instanz aktiv, wo Anhänge automatisch gescannt werden, um alle mit Viren infizierten Dateien zu identifizieren. Konfigurieren Sie die Funktion, indem Sie sicherstellen, dass der Scan in Ihrer Instanz aktiviert ist, und indem Sie alle Tabellen identifizieren, die Sie vom Scan ausschließen möchten.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Konfiguration**.
2. Berücksichtigen Sie beim Konfigurieren der Funktion Folgendes.
3. Wählen Sie **Speichern**.
4. Schließen Sie Tabellen vom Virenscan aus, indem Sie sie der **Liste der ausgeschlossenen Tabellen**hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren Sie zu **Systemdefinition** # **Dictionary**

b. Suchen Sie nach der Tabelle, die Sie vom Scan ausschließen möchten, und wählen Sie die Tabelle aus, deren Typ auf Sammlung festgelegt ist.

c. Wählen Sie auf der Registerkarte **Attribute** die Option **Neu**aus.

d. Fügen Sie `Exclude_from_antivirus_scan` im Feld Attribute hinzu, und geben Sie `True` in das Feld **Wert** ein.

e. Wählen Sie **Absenden**.

Ergebnisse
Antivirus-Scanning ist in Ihrer Instanz aktiviert, und die **Liste der ausgeschlossenen Tabellen** auf der Seite Antivirus-Konfiguration wird mit allen Tabellen ausgefüllt, die Sie vom Scan ausgeschlossen haben.

Dateien in Quarantäne werden überprüft

Überprüfen Sie Dateianhänge in Quarantäne, und ergreifen Sie bei Bedarf weitere Maßnahmen.

Vorbereitungen
Erforderliche Rolle: antivirus_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Überwachen Sie Ihre unter Quarantäne gestellten Dateieinträge auf der Seite Antivirus-Quarantäne in regelmäßigen Abständen, um eine der folgenden Aktionen auszuführen.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Quarantäne**.
2. Aktivieren Sie die Checkbox neben jedem unter Quarantäne gestellten Eintrag, für den Sie eine verfügbare Aktion ausführen möchten.
3. Wählen Sie im Banner die Dropdown-Liste **Aktionen für ausgewählte Zeilen** aus, um die Aktion auszuwählen, die für den unter Quarantäne gestellten Eintrag der ausgewählten Zeile ausgeführt werden soll.

Ergebnisse
Das System fordert eine Bestätigung und führt die ausgewählte Aktion gemäß Ihrer Eingabe aus.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Virenschutzmetriken

Antivirenaktivität wird überprüft

Überprüfen Sie das Antivirus-Aktivitätenprotokoll, das alle Aktivitäten für potenziell infizierte Dateien ab dem Zeitpunkt nachverfolgt, an dem sie erkannt und unter Quarantäne gestellt werden.

Vorbereitungen
Erforderliche Rolle: antivirus_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Dieses Protokoll fungiert als Bericht, der Antivirenaktivitäten wie Erkennung, Löschung und andere mögliche Ereignisse für unter Quarantäne gestellte Dateien erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Aktivität**.
2. Überprüfen Sie das Protokoll der unter Quarantäne gestellten Dateien.
   Sie können die Aktionen anzeigen, die in der Spalte Event für jede unter Quarantäne gestellte Datei ausgeführt werden.

Nächste Maßnahme

Bestimmen Sie, welche Datensätze Sie löschen, wiederherstellen, herunterladen oder im Protokoll beibehalten möchten. Siehe Dateien in Quarantäne überprüfen

Wissen über Wörterbuchattribute für Antivirus-Scanning

Wörterbuchattribute ändern das Verhalten der Tabelle oder des Elements, die der Wörterbuchdatensatz beschreibt. Als Administrator können Sie die Werte von Wörterbuchattributen festlegen, um das Verhalten der Standardkonfiguration von Antivirus Scanning zu ändern.

Wörterbuchattribute für Antivirus-Scanning

Name	Wert	Zielelement	Beschreibung
Exclude_from_antivirus_scan	wahr/falsch	beliebige Tabelle	Bei „true“ werden Dateianhänge in der Tabelle von der Antivirenprüfung ausgeschlossen. Siehe Antivirus-Scanning konfigurieren
Supress_antivirus_email_notifications	wahr/falsch	beliebige Tabelle	Bei „wahr“ wird das Senden von von der Plattform generierten E-Mail-Benachrichtigungen beendet, wenn eine potenziell infizierte Datei identifiziert wird.
Suppress_antivirus_ui_notifications	wahr/falsch	beliebige Tabelle	Bei „true“ werden von der Plattform generierte UI-Benachrichtigungen angehalten, wenn eine potenziell infizierte Datei identifiziert wird.

Zugehörige Informationen

Wörterbuchattribute

Auditing

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

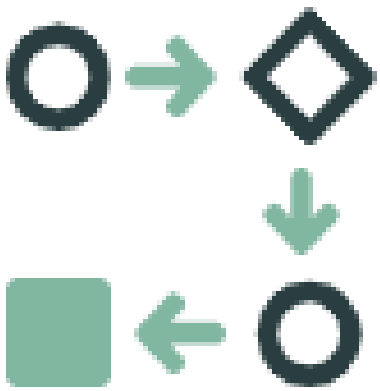
Erkunden

Lernen Sie die Funktionen und den Geschäftsnutzen von Auditing kennen.

Konfigurieren

Machen Sie sich mit der Konfiguration von Auditing vertraut.

Ansicht



Überprüfen Sie die Tabellen „Sys-Audit“ und „Audit-Beziehungsänderung“.

Referenz

Informieren Sie sich über die Verlaufssätze.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditing erkunden

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Wenn Sie Auditing aktivieren, wird die Erstellung, Aktualisierung und Löschung aller Datensätze in der Tabelle nachverfolgt. Wenn Sie einzelne Felder in einer Tabelle prüfen möchten, können Sie Felder, die Sie nicht nachverfolgen möchten, mithilfe eines Dictionary-Attributs ausblenden.

Audit-Informationen werden in den folgenden Tabellen gespeichert:

- Die Audit -Tabelle.
- Die Tabelle Wissen über Verlaufssätze.

⚠ Warnung:
Die Überwachung von Systemtabellen, die eine große Menge Datenverkehr erhalten, z. B. Workflow-Kontexte [wf_context] oder Event Management-Warnungen [em_alert], kann Auswirkungen auf die Leistung haben. Aus diesem Grund können Sie die Tabelle em_alert nicht als Ganzes prüfen. Auditieren Sie stattdessen ausgewählte Interessenbereiche. Legen Sie `audit=true` sowohl für die Tabelle em_alert als auch für die ausgewählten Felder fest. Versuchen Sie, so wenige Felder wie möglich zu prüfen.

Übergeordnete und untergeordnete Tabellen werden geprüft

Tabellen leiten die Audit-Kennzeichnungen nicht von übergeordneten oder untergeordneten geprüften Tabellen ab.

- Wenn Sie beispielsweise Auditing für die Tabelle „Konfigurationselemente“ [cmdb_ci] aktivieren, werden nur CIs geprüft, die in dieser Basistabelle gespeichert sind.
- Wenn Sie analog dazu Auditing für die Tabelle „Computer“ [cmdb_ci_computer] aktivieren, werden nur die Computer-CI-Datensätze geprüft, einschließlich aller Felder in der Tabelle „Computer“ [cmdb_ci_computer], die von der Tabelle „Konfigurationselemente“ [cmdb_ci] abgeleitet ist.

Systemtabellen werden geprüft

Standardmäßig prüft das System nicht, ob ein Datensatz aus Systemtabellen gelöscht wird. Um eine Systemtabelle zu prüfen, fügen Sie sie der Liste der Tabellen in der Eigenschaftsliste `glide.ui.audit_deleted_tables` hinzu.

Audits von Löschungen aus einem Formular oder einer Liste

Standardmäßig prüft das System das Löschen einzelner Datensätze aus einem Formular. Um Auditing zu verhindern, legen Sie das Wörterbuchattribut der Tabelle fest `no_audit_delete`.

Das System prüft Löschungen aus einer Liste, wenn es für das Wörterbuch der **Tabelle** ausgewählt ist und die Tabelle nicht in der Eigenschaft `glide.db.audit.ignore.delete` aufgeführt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Standardmäßig ist die Eigenschaft `glide.db.audit.ignore.delete`] in der Tabelle „Systemeigenschaft“ [sys_properties] nicht vorhanden. Um die Eigenschaft und die zugehörigen Werte zu ändern, müssen Sie sie zuerst manuell hinzufügen. Beim manuellen Hinzufügen werden jedoch die folgenden Standardwerte überschrieben:

glide.db.audit.ignore.delete = sys_mutex,sys_db_cache,sys_lucene_block,sys_lucene_file,sys_lucene_directory,sys_user_preference,sys_auc
cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
cmdb_sam_sw_usage, sam_sw_counter_detail

Weitere Informationen zum Hinzufügen von Systemeigenschaften finden Sie unter Systemeigenschaften hinzufügen

Es ist zu beachten, dass Audit-Löschungen standardmäßig aktiviert sind, unabhängig davon, ob der Datensatz aus der Formularansicht, Listenansicht oder durch ein Skript bzw. eine geplante Aufgabe gelöscht wird.

Informationen geprüft

Auditing verfolgt die folgenden Datensatzänderungen:

- Eindeutiger Datensatzbezeichner (sys_id) des geänderten Datensatzes
- Feld, das sich geändert hat
- Neuer Feldwert
- Alter Feldwert
- Anzahl der Aktualisierungen dieses Datensatzes und Felds
- Datum und Uhrzeit der Änderung
- Benutzer, der die Änderung vorgenommen hat
- Grund für den Change (falls ein Grund mit dem Change verknüpft ist)
- Interne Prüfpunkt-ID für den Datensatz, wenn der Datensatz mehrere Versionen hat.

Informationen, die von der Prüfung ausgenommen sind

Einige Updates werden nicht geprüft, obwohl die Prüfung für eine Tabelle aktiviert ist. Aus diesem Grund werden im Verlauf eines Datensatzes möglicherweise 132 Aktualisierungen angezeigt, aber nur sieben geprüfte.

Auditing schließt die folgenden Informationen aus:

- Durch ein Upgrade vorgenommene Updates.
- Aktualisierungen werden über Import Sets vorgenommen.
- Datensätze in übergeordneten oder untergeordneten Tabellen.
- Felder mit dem Wörterbuchattribut no_audit.
- Systemtabellen sind in der Eigenschaftenliste `glide.ui.audit_deleted_tables` nicht aufgeführt.
- Felder, die mit dem Präfix sys_ beginnen (Systemfelder), mit Ausnahme der Spalten sys_class_name und sys_domain_id.
- UI-Seiten können manchmal Aktualisierungen eines Datensatzes auslösen, ohne ein Audit-Protokoll zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Jedes Mal, wenn eine Inaktivitätsüberwachung einen Datensatz berührt. Dadurch wird verhindert, dass möglicherweise Hunderte von Aktualisierungen für einen Incident angezeigt werden, wobei das Rauschen die nützlichen Daten übertönt.
- Manuelle Änderungen an Performance Analytics Punktzahlen.

Audit einer Tabelle

Anweisungen zum Audit einer Tabelle finden Sie unter Auditing für eine Tabelle konfigurieren.

Standardmäßig verfolgt das System alle Felder in einer geprüften Tabelle. Sie können eine Teilmenge von Feldern in einer Tabelle auf zwei Arten prüfen:

- Sie können Auditing für die gesamte Tabelle aktivieren und dann die Felder ausschließen, die Sie nicht einbeziehen möchten. Es ist angemessen, wenn Sie die meisten, aber nicht alle Felder prüfen möchten, und wird als *Ausschlussliste*bezeichnet. Weitere Informationen finden Sie unter Feld von der Prüfung ausschließen (Ausschlussliste).
- Sie können Auditing für die Tabelle aktivieren, aber nur für angegebene Felder. Dies ist angemessen, wenn Sie nur eine kleine Anzahl von Feldern der Tabelle prüfen möchten, und wird als *Aufnahmeliste*bezeichnet. Informationen zum Einbeziehen eines Felds mithilfe einer Aufnahmeliste finden Sie unter Tabellenfelder in Audits einbeziehen (Inklusionsliste).

Audit-Datensätze, die nicht abgebrochen werden können

Reduzieren Sie mit der neuen Standardeinstellung die Wahrscheinlichkeit, dass Audit-Datensätze nicht aufgezeichnet werden, wenn eine Transaktion abgebrochen wird.

Audits wurden so festgelegt, dass ein Datensatz sofort in derselben Transaktion mit den Schreibvorgängen für den Zieldatensatz erstellt wird. Wenn der Zieldatensatz gelöscht wird, wird das Audit weiterhin erstellt und im Modul **„NCA Test Audit Delete“** gespeichert.

Hinweis:
Der erweiterte Auditprozess ist standardmäßig aktiviert. Wenn die Eigenschaft `glide.db.audit.lazy` auf `True`festgelegt ist, ist der erweiterte Audit-Prozess deaktiviert.

Wenn vor Release Washington DC eine Transaktion abgebrochen wurde, konnten bestimmte auditierbare Vorgänge nicht aufgezeichnet werden. Dies liegt daran, dass die Plattform einige Vorgänge zwischen der Datensatzänderung ausführt und vor der Audit-Erstellung abgebrochen wird. Jetzt werden Audits jedoch unmittelbar nach der Änderung des Datensatzes erstellt, wodurch die Wahrscheinlichkeit verringert wird, dass eine abgebrochene Transaktion den Vorgang abbricht, bevor das Audit aufgezeichnet wird.

Audits werden jetzt im selben Thread wie die Transaktion aufgezeichnet. Frühere Audits wurden in einem Hintergrund-Thread erstellt. Durch diese Änderung wird der Standardwert der Eigenschaft `glide.db.audit.lazy` von True in False neu definiert. Diese Eigenschaft wird normalerweise nicht in der Tabelle „Eigenschaften“ definiert, da die meisten Instanzen den neuen Standardwert und das neue Verhalten verwenden. In einigen Instanzen ist diese Eigenschaft möglicherweise bereits vorhanden und auf True festgelegt, was bedeutet, dass diese Instanzen diese Änderung nicht zum Audit-Verhalten verwenden können.

Hinweis:
Es wird empfohlen, diese Eigenschaft zu löschen, um das Update zu nutzen.

Auditing für eine Tabelle konfigurieren

Sie können die Tabellenprüfung aktivieren, um Änderungen an allen oder einigen der Felder der Tabelle nachzuverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin.

Hinweis:
Verschlüsselte Felder werden nicht vom Design geprüft. Dieses Verhalten ist nicht konfigurierbar.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**.
   Das System zeigt die Liste der Dictionary-Einträge an. Die Liste enthält eine Zeile für jede Tabelle sowie eine Zeile für jede Spalte (Feld) in der Tabelle.
2. Suchen Sie in der Liste der Wörterbucheinträge die Zeile, die der Tabelle entspricht, die Sie prüfen möchten, z. B. `cmdb_ci_computer`.
   Sie können die Zeile für die Tabelle selbst – von einer Zeile für eine Spalte in der Tabelle – unterscheiden, indem Sie die Zeile mit dem richtigen Tabellennamen, einem leeren Eintrag für den **Spaltennamen** und dem **TypSammlung**suchen.
3. Wählen Sie den Wörterbucheintrag für die Tabelle aus.
   Das System zeigt das Wörterbucheintragsformular an.
4. Aktivieren Sie das Kontrollkästchen **Audit**.
5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme
Wenn Sie nur einige Felder in der Tabelle Aktivieren der Aufnahmelistenprüfung für eine Tabelleprüfen möchten. Wenn Sie die meisten Felder prüfen, aber einige ausschließen möchten, lesen Sie Feld von der Prüfung ausschließen (Ausschlussliste).

Aktivieren der Aufnahmelistenprüfung für eine Tabelle

Aktivieren Sie eine Tabelle, um nur die Felder zu prüfen, die Sie explizit angeben. Dies ist nützlich, wenn Sie nur eine kleine Anzahl von Feldern in einer geprüften Tabelle prüfen möchten.

Vorbereitungen
Erforderliche Rolle: admin
Die Tabelle muss für Auditing aktiviertsein.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**.
   Das System zeigt die Liste der Dictionary-Einträge an. Die Liste enthält eine Zeile für jede Tabelle sowie eine Zeile für jede Spalte (Feld) in der Tabelle.
2. Passen Sie bei Bedarf die Listenansicht an, um die Spalte **Attribute** anzuzeigen.
3. Suchen Sie in der Liste der Wörterbucheinträge die Zeile, die der Tabelle entspricht, die Sie prüfen möchten, z. B. `cmdb_ci_computer`.
   Sie können die Zeile für die Tabelle selbst von einer Zeile für eine Spalte in der Tabelle unterscheiden, indem Sie die Zeile mit dem richtigen Tabellennamen, einem leeren Eintrag für Spaltenname und dem Typ *`collection`*suchen.
4. Geben Sie im Feld **Attribute** für diese Zeile *`audit_type=whitelist`*ein.

Nächste Maßnahme
Geben Sie an, welche Felder Sie in dieser Tabelle prüfen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld von der Prüfung ausschließen (Ausschlussliste)

Verhindern Sie, dass Now Platform eine Teilmenge von Feldern in einer geprüften Tabelle nachverfolgt, indem Sie diese Felder von einem Audit ausschließen.

Vorbereitungen

Erforderliche Rolle: admin

Um ein Feld in einer Tabelle von der Prüfung auszuschließen, müssen Sie zuerst die Prüfung für diese Tabelle aktivieren.

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie einer Ausschlussliste eine Reihe von Feldern hinzu, wenn Sie die meisten Felder in einer überprüfbaren Tabelle prüfen möchten. Wenn Sie nur einige Felder prüfen möchten, folgen Sie stattdessen dem Aufnahmelistenverfahren.

Hinweis:
Das Deaktivieren der Überwachung für journalbasierte Felder kann sich auf die Funktionalität von Funktionen wie dem Aktivitätsformatierer auswirken. Weitere Informationen finden Sie unter KB0743142 .

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**.
2. Passen Sie bei Bedarf die Listenansicht an, um die Spalte **Attribute** anzuzeigen.
3. Navigieren Sie zu der Zeile, die der Tabelle und dem Feld (Spalte) entspricht, die Sie von der Prüfung ausschließen möchten.
4. Geben Sie in der Spalte **Attribute** für diese Zeile `no_audit`ein.

Tabellenfelder in Audits einbeziehen (Inklusionsliste)

Verfolgen Sie eine Teilmenge von Feldern in einer geprüften Tabelle nach, indem Sie diese Felder einer Aufnahmeliste hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin

Um Felder in einer Tabelle zu einer Aufnahmeliste hinzuzufügen, müssen Sie zuerst Auditing für diese Tabelle und Aufnahmelisten-Audit für diese Tabelle aktiviert haben.

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie einer Aufnahmeliste eine Reihe von Feldern hinzu, wenn Sie nur eine kleine Anzahl von Feldern einer geprüften Tabelle prüfen möchten. Wenn Sie die meisten Felder prüfen und nur einige ausschließen müssen, folgen Sie stattdessen dem Ausschlusslistenverfahren.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**.
2. Passen Sie bei Bedarf die Listenansicht so an, dass die Spalte **Attribute** angezeigt wird.
3. Navigieren Sie zu der Tabelle und dem Feld (Spalte), das Sie in die Aufnahmeliste aufnehmen möchten.
4. Geben Sie im Feld **Attribute***`audit=true`*ein.

Aktivieren Sie Auditing für eine Systemtabelle

Löschungen aus Tabellen mit einem sys_-Präfix werden standardmäßig nicht geprüft. Um Löschvorgänge aus diesen Tabellen nachzuverfolgen, fügen Sie den Tabellennamen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Eigenschaft *glide.ui.audit_deleted_tables* hinzu. Durch Aktivieren des Plugins „Gelöschte Datensätze wiederherstellen“ werden dieser Eigenschaft mehrere Standardwerte hinzugefügt.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **UI-Eigenschaften**.
2. Suchen Sie die **Liste der Systemtabellen (beginnend mit „sys_“, durch Kommas getrennt), die die geprüfte Eigenschaft zum Löschen enthalten**.
3. Fügen Sie Tabellennamen hinzu, oder entfernen Sie sie.
   Tabellennamen müssen durch Kommas ohne Leerzeichen getrennt werden.
4. Klicken Sie auf **Speichern**.

Hinweis:
Weitere Informationen zu Audits finden Sie unter Tabelle „sys audit“ verstehen.

Anzeigen von Sys-Audit- und Audit-Beziehungsänderungstabellen

Now Platform verfolgt Einfügungen und Aktualisierungen an geprüften Datensätzen in den Tabellen „Sys-Audit“ (sys_audit) und „Audit-Beziehungsänderung“ (sys_audit_relation).

Now Platform verfolgt Audit-Tabellen. Um Tabellen nachzuverfolgen, aktivieren Sie das Kontrollkästchen **Audit** im Wörterbuchdatensatz, um den Wert auf true zu setzen. Standardmäßig werden keine Datensätze aus Systemtabellen geprüft, z. B. Update Set-Tabellen.

Hinweis:
Um Leistungsprobleme und Endlosschleifen zu vermeiden, überspringt das System alle Geschäftsregeln oder Workflows, die durch Einfügungen in die Sys-Audit-Tabelle ausgelöst werden.

Sys-Audit-Tabellenspalten

Die folgenden Spalten werden in den Datensätzen der Tabelle „sys_audit“ angezeigt:

Feld	Beschreibung
Tabellenname	Tabelle, für die der Audit-Datensatz gilt (z. B. „Incident“)
Feldname	Spalte in der Tabelle, für die der Audit-Datensatz gilt (z. B. „assigned_to“)
Dokumentenschlüssel	Sys_id (Unique Record Identifier) für den Ursprungsdatensatz, der dem Audit-Datensatz zugeordnet ist.
Benutzer	Name des Benutzers, der den Change erstellt hat. **Hinweis:** Einige automatisierte Prozesse verwenden das System oder den Gastbenutzer, um Änderungen an Datensätzen anzuwenden und nachzuverfolgen. Weitere Informationen finden Sie unter System- und Gastbenutzer .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Alter Wert	Alter Wert der Feldänderung, die durch diesen sys_audit-Datensatz dargestellt wird. • Referenzfelder: Eindeutiger sys_id-Wert des geänderten Datensatzes. • Datums- und Uhrzeitfelder: Wert in Coordinated Universal Time (UTC), wie in der Datenbank gespeichert.
Neuer Wert	Neuer Wert der Feldänderung, die durch diesen sys_audit-Datensatz dargestellt wird. • Referenzfelder: Eindeutiger sys_id-Wert des geänderten Datensatzes. • Datums- und Uhrzeitfelder: Wert in Coordinated Universal Time (UTC), wie in der Datenbank gespeichert.

Funktionsweise der Tabelle „Audit-Beziehungsänderung“ (sys_audit_relation).

Die Sys-Audit-Tabelle [sys_audit] verfolgt Aktivitäten in Tabellen, die für die Prüfung gekennzeichnet sind. Diese Aktivität umfasst Journalfeldeinträge und Verlaufssätze. Die Tabelle „Audit-Beziehungsänderung“ [sys_audit_relation] verfolgt Beziehungsänderungen zwischen Datensätzen der Tabelle „sys_audit“ und den Quelltabellen, aus denen die geprüften Datensätze stammen. Es wird auch nachverfolgt, wann ein Datensatz möglicherweise gelöscht wurde.

- Immer wenn Sie einen Datensatz in einer Tabelle prüfen, wird eine Beziehung zwischen den verschiedenen Ursprungstabellen und dem Speicher erstellt, der Daten aufzeichnet. Diese Beziehungsinformationen werden in den Tabellen sys_history_set, sys_history_line und sys_journal gespeichert.
- Wenn Sie ein Feld löschen, das zu einem geprüften Tabellendatensatz gehört, wird die Löschung in der Tabelle „sys_audit_relation“ aufgezeichnet. Mit anderen Worten: Jedes Mal, wenn Sie einen geprüften Datensatz ändern, werden zuerst vergangene Elemente gelöscht und dann eine Beziehung in der Tabelle „sys_audit_relation“ mit neuen Dokument-IDs erstellt.

Wissen über Verlaufssätze

Das System generiert bei Bedarf automatisch Verlaufssatzdatensätze aus der Audit-Tabelle, wenn ein Benutzer einen Datensatz erstellt oder seinen Verlauf anzeigt.

Wenn sich ein Datensatz in einer geprüften Tabelle befindet, wird sein Verlaufssatz generiert, wenn der Datensatz eingefügt wird oder wenn ein Benutzer den Datensatz anzeigt.

Hinweis:
Verwenden Sie keine Verlaufssätze, um Berichte zu generieren.

Mehrere Informationsfelder werden im Verlaufssatz-Datensatz erfasst, der in der Listenansicht angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatzfelder der Listenansicht

Feld	Eingabewert
ID	Dokument-ID für den Datensatz, dessen Verlauf aufgezeichnet wird.
Tabelle	Geprüfte Tabelle für den Datensatz, dessen Verlauf aufgezeichnet wird.
Ladezeit	Zeit, die zum Generieren des Verlaufssatzes benötigt wurde.

Felder des Audit-Verlaufsdatensatzes

Feld	Eingabewert
Bezeichnung	Die Bezeichnung des Felds, das geändert wurde.
Alt	Wert vor der Änderung.
Neu	Wert nach der Änderung.
Typ	Gibt an, ob der Eintrag für ein normales Feld, einen E-Mail-Datensatz oder einen Beziehungsänderungsdatensatz gilt.
Updateanzahl	Die Häufigkeit, mit der dieses Feld geändert wurde. Ein Wert von -1 gibt an, wann der Datensatz erstellt oder gelöscht wurde.
Update-Zeit	Datum und Uhrzeit des Change. **Hinweis:** Die Aktualisierungszeit für automatisch generierte Verlaufszeilen stimmt nicht mit der Erstellungs- oder Aktualisierungszeit für einen Datensatz in einer bestimmten Verarbeitungssituation überein. Wenn Sie einen Verlaufssatz eines Datensatzes zum ersten Mal anzeigen, wird automatisch ein anfänglicher Satz von Verlaufszeilendatensätzen generiert. Da Dateiänderungen in einem Upgrade nicht geprüft werden, tritt diese Datumsabweichung in folgenden Fällen auf: • Sie können einen Verlaufssatz anzeigen, nachdem eine Änderung an einem Datensatz vorgenommen wurde, aber • Bevor in einem zukünftigen Upgrade eine weitere Änderung daran vorgenommen wird.
Benutzername	Name des Benutzers, der den Change erstellt hat.

Verlaufssätze in einer Kalenderansicht

Nachdem Verlaufssätze aktiv sind, wird die Kontextmenüauswahl Verlauf mit Informationen aus dem Verlaufssatz und nicht aus der Tabelle „sys_audit“ ausgefüllt. Aus der Perspektive des Benutzers sind dieselben Verlaufsdaten in derselben Benutzeroberfläche verfügbar, aber die Art und Weise, wie die Informationen gespeichert werden, ist unterschiedlich.

Da die Verlaufsansicht eine Kalenderansicht enthält, aber nicht die normale Listenschnittstelle zum Filtern und Interagieren mit den Verlaufsdatensätzen verwendet, ermöglicht sie Folgendes:

- Historische Daten durchsuchen und filtern
- Verlaufsdaten werden exportiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeigen von Verlaufssätzen

Es gibt zwei Möglichkeiten, den Verlaufssatz anzuzeigen, auf die über die Kontextmenüaktion **Verlauf**zugegriffen werden kann.

Unterschiede zwischen Audit- und Verlaufssätzen

In den Tabellen „Audit“ [sys_audit], „Verlaufssätze“ [sys_history_set] und „Verlauf“ [sys_history_line] werden dieselben Daten gespeichert, sie dienen jedoch unterschiedlichen Zwecken und verwalten Daten unterschiedlich.

Audit-Tabelle [sys_audit].

In der Audit-Tabelle [sys_audit] speichert das System Verlaufsinformationen für alle Datensätze. Diese Datensätze sollen für immer aufbewahrt werden, damit Administratoren den Verlauf der geprüften Datensätze jederzeit nachverfolgen können. Wenn die Anzahl der Audit-Datensätze im Laufe der Zeit zunimmt, wird es ineffizienter, die Audit-Tabelle direkt nach Verlaufsinformationen abzufragen. Es ist viel effizienter, Abfragen nur für die kleineren Teilmengendatensätze auszuführen, für die Sie tatsächlich Verlaufsinformationen anzeigen möchten.

Tabelle „Verlaufssatz“ [sys_history_set].

Die Tabelle „Verlaufssatz“ [sys_history_set] gibt an, welche bestimmten Datensätze aus einer geprüften Tabelle Verlaufsinformationen enthalten. In der Tabelle „Verlauf“ [sys_history_line] werden die tatsächlichen Änderungen an Feldwerten gespeichert, die aufgetreten sind.

- Das System generiert nach Bedarf automatisch Verlaufssatz- und Verlaufsdatensätze aus der Audit-Tabelle, wenn ein Benutzer entweder einen Datensatz erstellt oder seinen Verlauf anfordert.
- Anstatt einen vollständigen Verlauf aller Änderungen im System zu enthalten, enthalten Verlaufssatz- und Verlaufsdatensätze nur eine aktuelle Teilmenge von Verlaufsinformationen für Datensätze, in denen Benutzer solche Informationen erstellt oder angefordert haben.
- Zusätzlich zu den Audit-Daten enthalten Verlaufssätze auch die Informationen, die beim Einfügen von Datensätzen festgelegt werden, einschließlich Journalfeldeinträgen. Journalfeldeinträge, die Sie vor dem Erstellen eines Datensatzes erstellen, werden auf die gleiche Weise behandelt wie Journaleinträge, die zum Zeitpunkt der Datensatzerstellung erstellt werden. Diese Journaleinträge werden in Verlaufssätzen mit derselben Erstellungszeit angezeigt und von Daten wie der zugehörige Datensatz selbst erstellt.

Das System begrenzt Verlaufssätze und Verlaufsdatensätze nach:

- Lassen Sie die Tabellenbereinigung Verlaufssatz-Datensätze löschen, die seit 30 Tagen nicht aktualisiert wurden.
- Verwenden der Tabellenrotation, um alle sieben Tage zwischen vier Verlaufstabellen zu rotieren. Das System verwirft Verlaufsdatensätze, die älter als 28 Tage sind.

Sollte jemand zu einem späteren Zeitpunkt erneut Verlaufsinformationen benötigen, kann das System diese aus Audit-Quelldatensätzen erneut generieren.

Nachdem das System Verlaufssatz-Datensätze generiert hat, verwendet die Kontextmenüauswahl **Verlauf** den Verlaufssatz anstelle von Audit-Datensätzen. Aus der Perspektive des Benutzers sind dieselben Verlaufsdaten in derselben Benutzeroberfläche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verfügbar, aber die Art und Weise, wie die Informationen gespeichert werden, ist unterschiedlich.

Steuern Sie den Zugriff auf den Verlauf

Sie können einer Rolle Zugriff zum Anzeigen des Auditverlaufs gewähren, indem Sie eine Systemeigenschaft festlegen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**.
2. Wählen Sie die Eigenschaft `glide.history.role` aus der Tabelle aus.
3. Wählen Sie in `List of roles (comma-separated) that can access the history of a record` die Benutzerrollen aus, auf die Sie auf den Verlauf zugreifen möchten.
4. Wählen Sie **Speichern**.

Ergebnisse

Alle Änderungen an einem Feld werden ausgelassen, wenn ein Benutzer ohne Lesezugriff den Verlauf eines Datensatzes anzeigt.

Ändern Sie die Anzahl der Verlaufseinträge

Standardmäßig zeigt der Verlauf maximal 250 Verlaufseinträge an, Sie können diesen Wert jedoch ändern.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

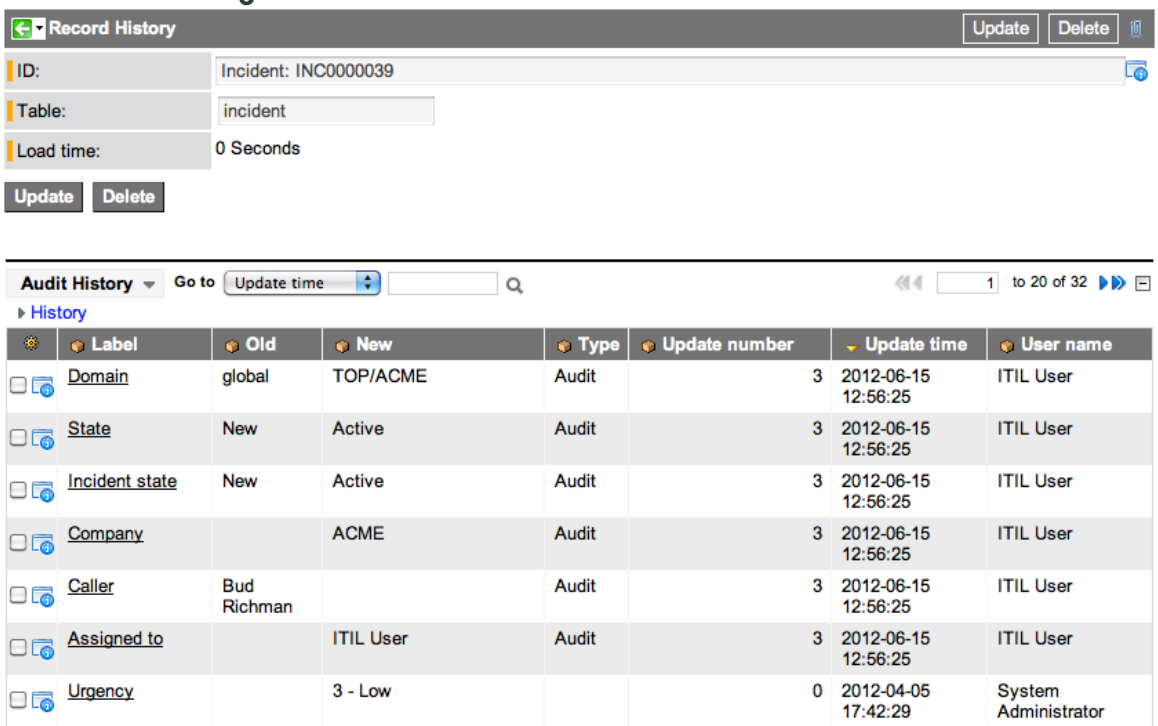
1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**.
2. Wählen Sie die Eigenschaft `glide.history.max_entries` aus.
3. Legen Sie den Wert `Maximum number of field entries displayed in record history, default is 250` auf eine neue maximale Anzahl von Einträgen fest, die angezeigt werden sollen.

Verlaufsliste

In der Verlaufsliste wird jeder Change als eigene Zeile in der Change-Liste angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

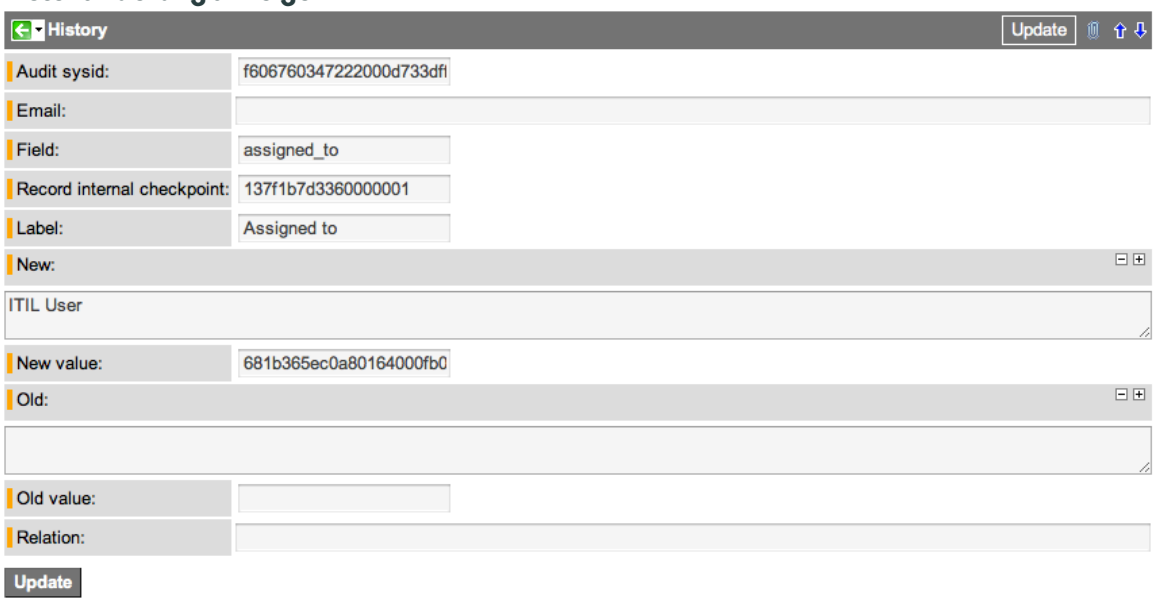
Verlaufsliste anzeigen



	Label	Old	New	Type	Update number	Update time	User name
	Domain	global	TOP/ACME	Audit	3	2012-06-15 12:56:25	ITIL User
	State	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
	Incident state	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
	Company		ACME	Audit	3	2012-06-15 12:56:25	ITIL User
	Caller	Bud Richman		Audit	3	2012-06-15 12:56:25	ITIL User
	Assigned to		ITIL User	Audit	3	2012-06-15 12:56:25	ITIL User
	Urgency		3 - Low		0	2012-04-05 17:42:29	System Administrator

Klicken Sie auf ein Zeilenelement, um zusätzliche Details zum Change anzuzeigen.

Listenänderung anzeigen



Anforderungen

Um eine Verlaufsliste anzuzeigen, müssen die folgenden Anforderungen erfüllt sein.

Auditing

Auditing für die Tabelle muss aktiviert sein, um eine Verlaufsliste anzuzeigen.

ACLs

Standardmäßig ist die Option *Listenverlauf* nur für Benutzer mit der Administrator-Benutzerrolle verfügbar. Um diese Option für Nicht-Administratoren zu aktivieren, erstellen Sie eine benutzerdefinierte ACL-Regel, die Lesezugriff auf die Tabelle „Datensatzverlauf“ [sys_history_set] gewährt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen

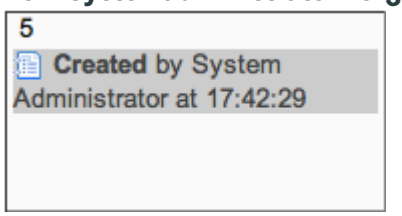
Mindestens eine der Rollen des Benutzers muss in der Eigenschaft `glide.history.role` enthalten sein, die standardmäßig die Rolle itil enthält.

Verlaufskalender

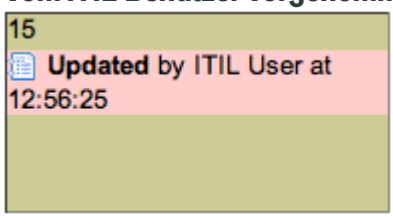
Der Verlaufskalender zeigt die Tage an, an denen der Datensatz geändert wurde, wer die Änderung vorgenommen hat und wann.

Der Verlaufskalender wird nach Aktualisierungsnummer sortiert. Jedem Benutzer ist eine Farbe zugewiesen, sodass Sie auf einen Blick erkennen können, wie oft ein Datensatz von einem bestimmten Benutzer geändert wurde. Beispiel:

Vom Systemadministrator vorgenommene Änderungen



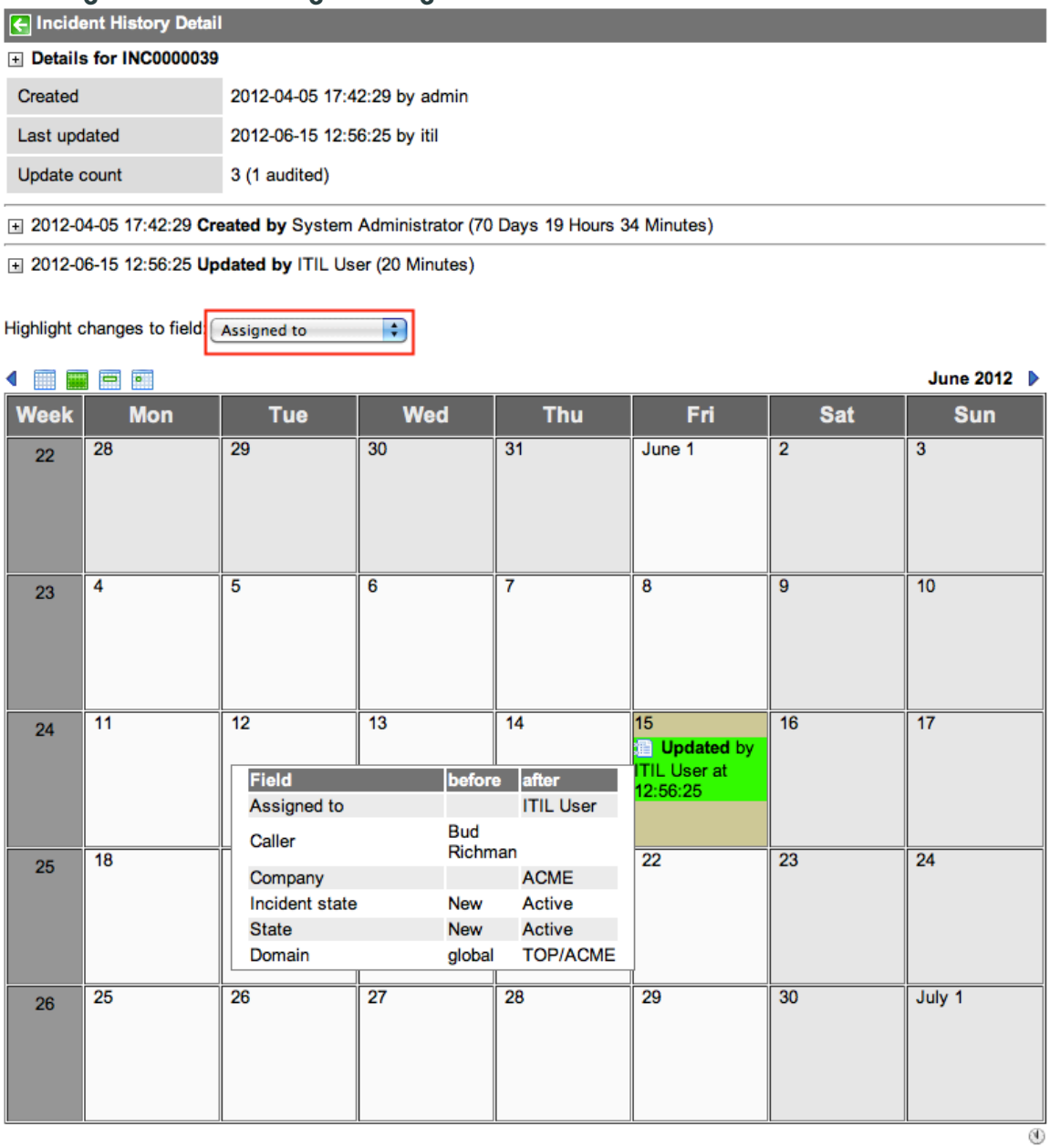
Vom ITIL-Benutzer vorgenommene Änderungen



Um Änderungen an einem bestimmten Feld hervorzuheben, wählen Sie das Feld im Auswahlfeld **Änderungen an Feld** hervorheben aus. Wenn Sie ein Feld aus diesem Auswahlfeld auswählen, wird der Kalender so geändert, dass die Zeiten hervorgehoben werden, zu denen dieses Feld geändert wurde. Bewegen Sie den Mauszeiger über den Text einer hervorgehobenen Änderung, um die Änderung des Werts anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

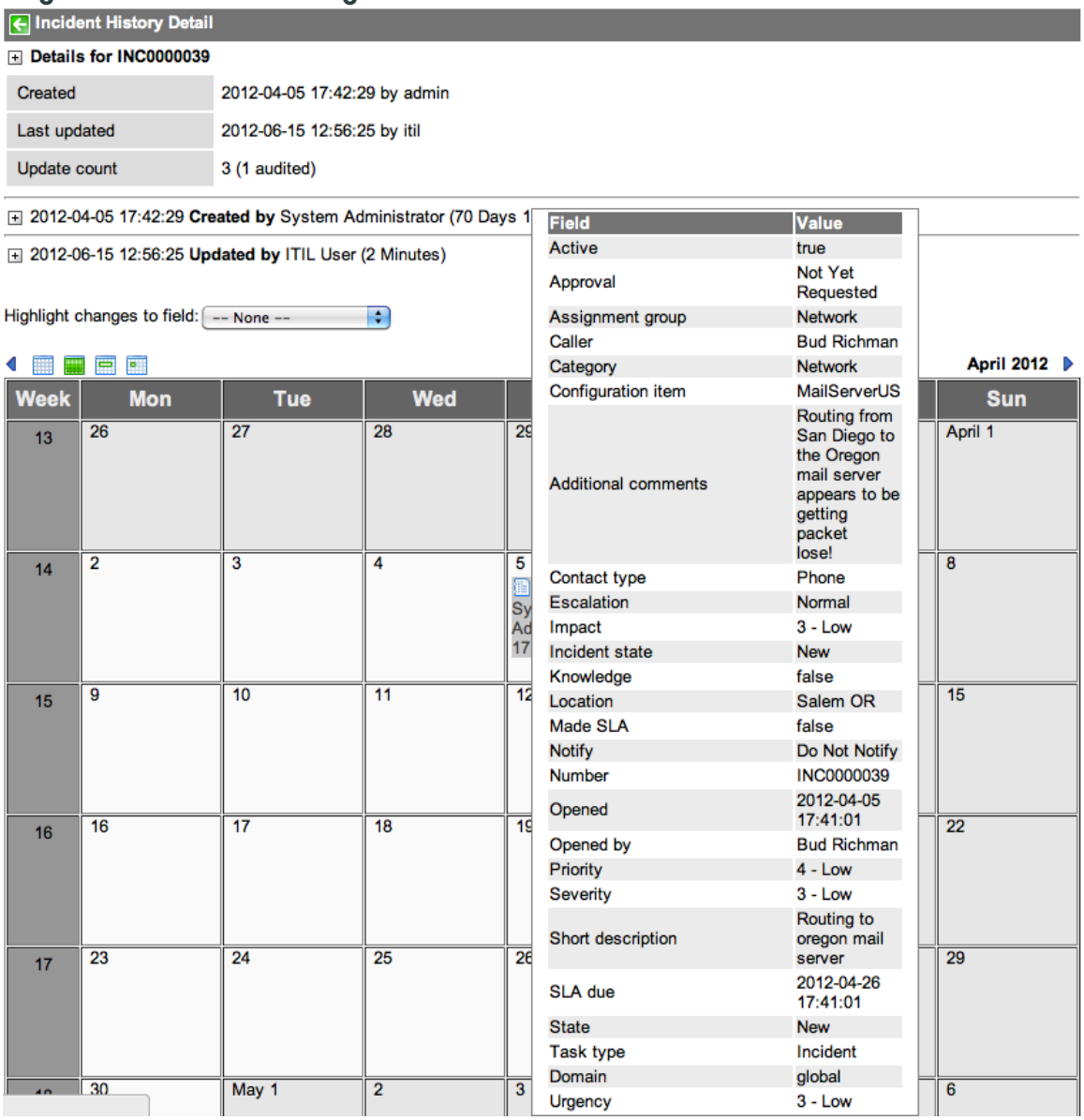
Hervorgehobene Änderungen anzeigen



Wenn Sie den Mauszeiger über das Symbol innerhalb eines Eintrags bewegen, werden in einem Popup alle Wertänderungen angezeigt. Dies sind die gleichen Informationen, die im oberen Teil des Formulars angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Kalenderänderungen an



Sie können auf die Tagesnummer klicken, um eine Ansicht der Änderungen für diesen Tag zu erhalten. Sie können auch auf die Wochennummer links klicken, um die Wochenansicht anzuzeigen. Sie können zu und von Monat zu Monat scrollen, um Änderungen anzuzeigen.

Verlaufszeitleiste

Sie können eine Zeitleiste der Änderungen für ein CI und die zugehörigen Datensätze, Beziehungen, Baselines und vorgeschlagenen Änderungen für das CI anzeigen. Zeitleisten sind für CIs in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle verfügbar, wenn Auditing für die Tabellen aktiviert ist.

Erforderliche Rolle: Die ACL für diese Ansicht basiert auf den Rollen, die in der Systemeigenschaft `glide.history.role` definiert sind, die standardmäßig auf itil festgelegtist. Außerdem muss der Benutzer Lesezugriff auf die Tabelle „Verlaufssatz“ [sys_history_set] haben, die standardmäßig dem Administrator gewährt wird.

Sie können eine Zeitleiste öffnen, wenn Sie den Verlauf eines CI anzeigen. Sie können den Zeitraum, den Zeitraum und die Eigenschaften angeben, die in der Zeitleiste angezeigt werden. Sie können entweder anzeigen, was sich in einem bestimmten Change Set geändert hat, oder das gesamte CI anzeigen, um Probleme besser beheben zu können. Sie können

Automatische Übersetzung

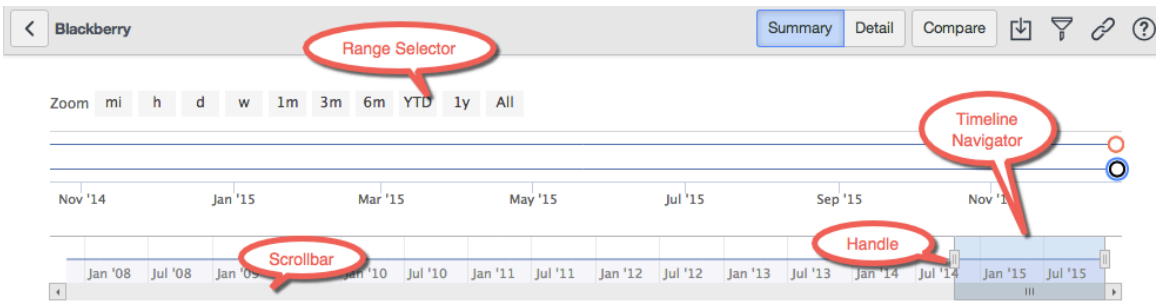
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auch eine Zeitleiste der Änderungen an den zugehörigen Datensätzen des CI anzeigen und jederzeit Snapshots des CI exportieren und vergleichen.

CI-Changes werden durch Blasen in verschiedenen Formen und Farben entlang der Zeitleiste dargestellt. Die Form jeder Blase stellt eine andere Art von Change dar, und die Farbe jeder Blase gibt an, ob die Änderung gültig oder ungültig ist. CI-Baselines werden durch schwarze Kreise dargestellt, über die Sie den Mauszeiger bewegen können, um weitere Details anzuzeigen. Klicken Sie auf das **?** Symbol, um Form- und Farbdefinitionen der Blase anzuzeigen, und auf eine Blase zeigen, um Details zum Change Set anzuzeigen.

Eine Änderung an einer Beziehung wird nur dann als gültig betrachtet, wenn sie über Change Management angewendet wurde. Wenn die Änderung über das Framework „Vorgeschlagene Änderungen“ angewendet wurde, ist sie gültig. Weitere Validierungsschritte finden Sie unter Erstellen oder bearbeiten Sie ein geplantes Validierungsskript .

Verlaufszeitleistenansicht



Zeitleistenblasen

Hinweis:
Vorgeschlagene Changes, die kein geplantes Startdatum haben, werden in der Zukunft platziert.

Zeitleistennavigator

Verwenden Sie die Ziehpunkte an beiden Enden des Zeitleistennavigators, um den angezeigten Zeitraum zu verlängern oder zu verkürzen.

Sie können zu einem anderen Zeitraum scrollen, indem Sie auf den unteren Teil des Zeitleistennavigators klicken und dann den Navigator nach links oder rechts ziehen.

Zoom

Standardmäßig wird die Zeitleiste für den letzten Monat angezeigt. Neben der Bezeichnung **Zoom** über der Zeitleiste können Sie ein anderes Zeitintervall auswählen. Sie können Intervalle von einer Minute bis zum gesamten Datenzeitraum auswählen.

Wenn sich das CI während des Zeitraums häufig ändert, werden die angezeigten Blasen möglicherweise zu voll. Sie können die Blasen auf eine der folgenden Arten vergrößern oder verkleinern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ändern Sie das Zeitintervall auf der Zeitleiste. Wenn Sie das Zeitintervall verkürzen, vergrößern Sie die Ansicht, und wenn Sie das Zeitintervall verlängern, verkleinern Sie die Ansicht.
- Wählen Sie den Abschnitt der Zeitleiste aus, den Sie vergrößern möchten.

Eigenschaftenfilter

Sie können die angezeigten Blasen filtern. Standardmäßig werden alle Blasen angezeigt, die Änderungen an allen Eigenschaften des CI darstellen. Sie können die Ansicht so beschränken, dass nur die Blasen angezeigt werden, in denen sich ausgewählte Eigenschaften geändert haben, und Blasen ausschließen, in denen sich nur nicht ausgewählte Eigenschaften geändert haben.

In den Ansichten „ **Detail“** und „ **Zusammenfassung** “ werden Eigenschaften innerhalb Ihres Filterbereichs hervorgehoben, die sich geändert haben. Die geänderten Eigenschaften werden hellblau hervorgehoben.

In der **Zusammenfassungsansicht** können Sie alle Eigenschaften des CI oder nur geänderte Eigenschaften einbeziehen. Wenn Sie alle Eigenschaften in der Zusammenfassungsansicht anzeigen, werden geänderte Eigenschaften vor unveränderten Eigenschaften aufgelistet.

Zusammenfassungsansicht

In der **Zusammenfassungsansicht** werden Snapshots der von jeder Blase dargestellten CIs angezeigt. Jeder Snapshot zeigt die Änderungen an den Feldern und Beziehungen des CI gemäß dem Change Set an. Zeigt alte und neue Werte vor und nach der Änderung sowie alle Beziehungen an, die hinzugefügt oder gelöscht wurden.

Verwenden Sie die Schaltflächen **>** und **<** auf beiden Seiten der Snapshot-Anzeige, um in chronologischer Reihenfolge durch die nächsten und vorherigen Change Set-Datensätze zu scrollen.

Detailansicht

In der **Detailansicht** werden Snapshots des CI angezeigt, die den Blasen entsprechen. Jeder Snapshot enthält die Felder, die sich innerhalb des Eigenschaftsfilterbereichs befinden, und zeigt die geänderten Eigenschaften mit einem hellblauen Hintergrund an. Klicken Sie auf eine Blase, um den entsprechenden Snapshot des CI anzuzeigen. Die angezeigten Daten sind schreibgeschützt.

Verwenden Sie die Schaltflächen **>** und **<** auf beiden Seiten, um in chronologischer Reihenfolge durch die nächsten und vorherigen Change Set-Datensätze zu blättern.

Zeigen Sie die Zeitleiste der Änderungen an zugehörigen Datensätzen an

In der Zeitleiste der Changes für einen CI-Datensatz können Sie auch eine Zeitleiste der Changes für die zugehörigen Datensätze des CI anzeigen.

Vorbereitungen

Erforderliche Rolle : admin

- Zieltabelle: Der CI-Datensatz muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden.
- Auditing: muss für die Tabelle aktiviert sein, die das CI enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Klicken Sie auf das Symbol „ **Zugehörige Datensätze** “, und wählen Sie zugehörige Datensätze aus der **Liste der** anzuzeigenden zugehörigen Datensätze aus.
   Klicken Sie erneut auf das Symbol Zugehörige Datensätze, um die Zeitleiste der zugehörigen Datensätze anzuzeigen.

Ergebnisse

Die Zeitleiste der Änderungen an den zugehörigen Datensätzen des CI wird direkt über der Zeitleiste des CI angezeigt. Wenn Sie alle zugehörigen Datensätze deaktivieren, wird die Zeitleiste der zugehörigen Datensätze ausgeblendet.

Nächste Maßnahme

Bewegen Sie den Mauszeiger über eine Change-Blase in der Zeitleiste der zugehörigen Datensätze, um Details zur Änderung anzuzeigen, z. B. Datum und Anzahl der geänderten Eigenschaften. Wenn Sie das Zeitintervall im Fokus ändern oder vergrößern oder verkleinern, wirkt sich dies gleichzeitig auf die CI-Zeitleiste und die Zeitleiste der zugehörigen Datensätze aus.

Exportieren Sie einen Snapshot eines CI

Sie können einen Snapshot eines CI aus seiner Zeitleiste exportieren.

Vorbereitungen

Das CI muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden. Auditing muss für die Tabelle aktiviert sein, die das CI enthält.
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Snapshot des CI in ein XML-, PDF- (Portal) oder PDF-Format (Querformat) exportieren.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Wählen Sie die Blase aus, die die Zeit darstellt, für die Sie einen Snapshot des CI exportieren möchten.
3. Klicken Sie auf das Exportsymbol ( ).
4. Wählen Sie das Dateiformat aus, das für den Export verwendet werden soll.
   Sie können die Datei zur Anzeige auf Ihr System herunterladen.

CI-Snapshots vergleichen

Sie können die Eigenschaften und Beziehungen eines CI an zwei verschiedenen Punkten in seiner Zeitleiste vergleichen.

Vorbereitungen

Das CI muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden. Auditing muss für die Tabelle aktiviert sein, die das CI enthält.
Erforderliche Rolle: admin.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Klicken Sie auf **Vergleichen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie ein **Startdatum** und ein **Enddatum** aus.
4. Klicken Sie auf **Vergleichen**.

Nachverfolgung von Änderungen an Referenzfeldern

Administratoren können Änderungen an Anzeigewerten von Referenzfeldern nachverfolgen.

Da Referenzfelder nur einen ID-Wert speichern, kann das System normalerweise nur Änderungen prüfen, wenn sich der ID-Wert ändert. Standardmäßig prüft das System keine Änderungen, wenn sich der Anzeigewert eines Referenzfelds ändert.

Betrachten Sie die folgende Situation. Eine Benutzerin ändert ihren Namen von Jane Smith in Jane Miller. Da der Benutzername der Anzeigewert für die Benutzertabelle ist, verweist jeder vorherige Verweis auf Jane Smith stattdessen auf Jane Miller. Wenn der Administrator nur den Namen des vorhandenen Benutzerdatensatzes aktualisiert, wird in Audit- und Verlaufsdatensätzen nur der neue Name „Jane Miller“ angezeigt. Standardmäßig bietet das System keine Möglichkeit, zwischen Änderungen zu unterscheiden, die unter dem ursprünglichen Benutzernamen vorgenommen wurden, und denen, die mit dem neuen Benutzernamen vorgenommen wurden.

Wenn Ihre Audit-Richtlinie die Nachverfolgung von Benutzernamenänderungen erfordert, können Sie:

- Erstellen Sie einen neuen Benutzerdatensatz für den neuen Namen, und deaktivieren Sie den vorherigen Benutzerdatensatz. Das System behält Audit-Datensätze für den alten Benutzernamen bei und erstellt zukünftige Audit-Datensätze mit dem neuen Benutzernamen.
- Erstellen Sie benutzerdefinierte Felder und eine Geschäftsregel, um den vorherigen Namen und das Datum der Namensänderung zu speichern. Das System kann diese Informationen verwenden, um die richtigen Namen in Audit- und Verlaufsdatensätzen zu erstellen.

Nachverfolgung von Einfügungen

Standardmäßig erstellt das System keine Audit-Datensätze für Einfügungen, da Einfügungen in einer typischen Instanz mehr als 80 % der Größe der Audit-Tabelle ausmachen können.

Das Nichtverfolgen von Einfügungen ermöglicht eine bessere Leistung und eine viel kleinere Audit-Tabelle. Administratoren können die Überwachung von Einfügungen aktivieren, indem sie die Eigenschaft `glide.sys.audit_inserts` auf *true* setzen.

Nachverfolgung von CI-Beziehungen

Änderungen an einer CI-Beziehung (CI-Beziehungen, CI/Benutzer-Beziehungen oder CI/Gruppen-Beziehungen) werden im Verlauf der Elemente auf beiden Seiten der geänderten Beziehung angezeigt, unabhängig davon, ob die Änderung manuell war oder ein Ergebnis von Discovery war.

Beispiel: Wenn für Computer-Alpha eine von CI-Beziehung mit Computer-Beta verwendet wird, enthält der Verlauf für Alpha einen Datensatz, wann die Beziehung mit Beta hergestellt wurde, und ebenso enthält der Verlauf für Beta einen Datensatz, wann die Beziehung zu Alpha wurde eingerichtet. Dieses Beispiel zeigt den Verlauf, der angezeigt wird, wenn einige CI-Beziehungen hergestellt werden und dann eine der Beziehungen entfernt wird:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungsverlauf

⊟ 2008-12-03 10:49:37 **Updated by** Guest (19 Hours 54 minutes ago) - CI Relationship Change

- created 2 Days 2 Hours 51 minutes earlier

Relationship	Before	After
Runs	(relationship added)	Tomcat@tomdmac
Runs	(relationship added)	MySQL Server@tomdmac

⊞ 2008-12-03 10:49:38 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Disks

⊞ 2008-12-03 10:49:43 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Active Connections

⊞ 2008-12-03 10:50:02 **Updated by** Guest (19 Hours 53 minutes ago)

⊟ 2008-12-04 06:43:39 **Updated by** Glide Maintenance (just now) - CI Relationship Change

- last activity was 19 Hours 53 minutes earlier
- created 2 Days 22 Hours 45 minutes earlier

Relationship	Before	After
Runs	MySQL Server@tomdmac	(relationship removed)

Das erstellte Aufzählungszeichen gibt das Datum an, an dem das CI, der Benutzer oder die Gruppe erstellt wurde. Das Aufzählungszeichen der letzten Aktivität bezieht sich darauf, wann die Beziehungen zuletzt geändert wurden. Wenn Sie den CI-Beziehungsverlauf für einen oder alle CI-Beziehungstypen nicht anzeigen möchten, können Sie ihn deaktivieren, indem Sie die Überwachung in den CI-Beziehungstabellen (CI-Beziehung [cmdb_rel_ci], CI/Benutzer-Beziehungstyp [cmdb_rel_user_type]) oder Gruppe deaktivieren Beziehung [cmdb_rel_group]).

Strenge Sicherheitseinstellungen

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

Erkunden Sie die Einstellung für hohe Sicherheit

Aktivieren Sie Strenge Sicherheitseinstellungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Machen Sie sich mit den Funktionen und Geschäftsnutzen von Einstellungen für hohe Sicherheit vertraut.

Aktivieren Sie die strengen Sicherheitseinstellungen.

Konfigurieren Sie strenge Sicherheitseinstellungen

Machen Sie sich damit vertraut, wie Sie strenge Sicherheitseinstellungen konfigurieren.

Strenge Sicherheitseinstellungen erkunden

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

Das Modul „Strenge Sicherheitseinstellungen“ wird mit dem Plugin „Strenge Sicherheitseinstellungen“ aktiviert, das standardmäßig in neuen Instanzen aktiv ist. Wenn die strengen Sicherheitseinstellungen in Ihrer Instanz nicht aktiv sind, lesen Sie die Aktivierung von strengen Sicherheitseinstellungen anfordern. Weitere Informationen zu diesem Plugin finden Sie unter Hochsicherheits-Plugin in den Härtungseinstellungen für die Instanzsicherheit. Eigenschaften für die folgenden Arten von Hochsicherheitseinstellungen sind verfügbar:

- Standardeigenschaftswerte: Zur Erhöhung der Sicherheit auf Ihrer Plattform durch Zentralisierung aller kritischen Sicherheitseinstellungen an einem Ort für Verwaltung und Überwachung.
- Standardverweigerungseigenschaft: Stellt eine Sicherheitsmanagereigenschaft bereit, um das Standardsicherheitsverhalten für den Tabellenzugriff zu steuern.
- Rolle „Sicherheitsadministrator“: Stellt eine Rolle bereit, um die Änderung wichtiger Sicherheitseinstellungen und -ressourcen zu verhindern. Die Sicherheitsadministratorrolle wird nicht von der Administratorrolle geerbt und muss explizit zugewiesen werden.
- Erweiterte Berechtigungen: Ermöglicht Benutzern mit der Sicherheitsadministratorrolle, im Kontext eines normalen Benutzers zu agieren und bei Bedarf auf eine höhere Sicherheitsrolle aufzusteigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zugriffskontrollen für Eigenschaften: Ermöglicht Sicherheitsadministratoren das Festlegen der Rollen, die zum Lesen und Schreiben von Eigenschaften erforderlich sind.
- Systemprotokolle: Sind schreibgeschützt.
- Zugriffskontrollregeln: Steuern Sie, auf welche Daten Benutzer zugreifen können und wie sie darauf zugreifen können.

Hinweis:

- Strenge Sicherheitseinstellungen aktivieren auch automatisch das Plugin „Contextual Security“, wenn es nicht bereits aktiv ist. Darüber hinaus bietet Platform Security Settings - High Einstellungen und Funktionen im Zusammenhang mit der Erhöhung der Sicherheit Ihrer Instanz.
- Der Inhalt „Härtungseinstellungen für Instanzsicherheit“ enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform. Weitere Informationen zu diesen Eigenschaften finden Sie unter Härtungseinstellungen für die Instanzsicherheit.
- Weitere Informationen zu diesen Eigenschaften finden Sie unter Härtungseinstellungen für die Instanzsicherheit.

Es gibt zwei Möglichkeiten, die Eigenschaften von „Strenge Sicherheitseinstellungen“ festzulegen oder zu ändern.

- Navigieren zu **Systemsicherheit** > **Strenge Sicherheitseinstellungen**.

  Optionen auf der Seite „Strenge Sicherheitseigenschaften“ sind **Ja** oder **Nein**.

- Navigieren Sie zu **sys_properties.list**, und suchen Sie nach der Eigenschaft, die Sie festlegen oder ändern möchten.

  Optionen in der Tabelle „Systemeigenschaften“ [sys_properties.list] lauten **true** oder **false**.

Zugriffssteuerung für Eigenschaften

Zwei zusätzliche Spalten werden in der Tabelle „Eigenschaften“ [sys_properties] erstellt, wenn die Einstellungen für hohe Sicherheit aktiv sind:

- **read_roles**: Eine durch Kommas getrennte Liste von Rollennamen, die alle Felder dieser Eigenschaft lesen dürfen.
- **write_roles**: Eine durch Kommas getrennte Liste von Rollennamen, die alle Felder dieser Eigenschaft schreiben/ändern dürfen.

Eigenschaften, die in der Tabelle „Eigenschaften“ aufgeführt sind, haben **„read_roles“** von „admin“ und **„write_roles“** von „security_admin“. Benutzer mit der Administratorrolle können die Eigenschaftswerte anzeigen und lesen, müssen jedoch auf die Rolle security_admin hochstufen, um sie zu ändern.

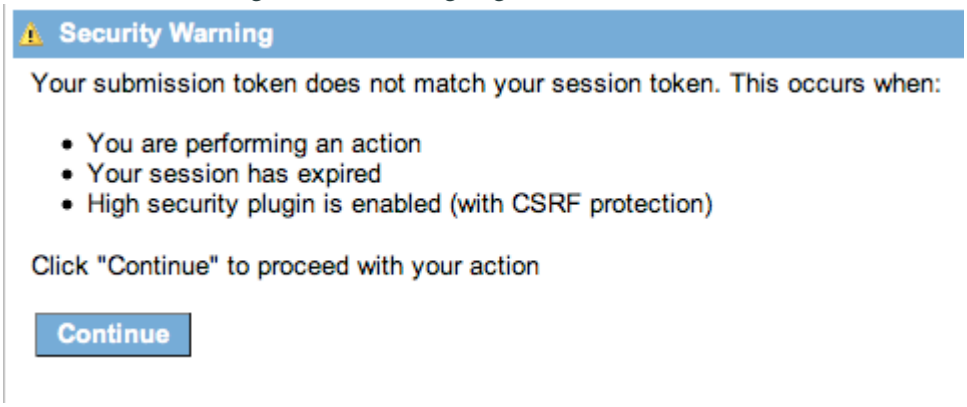
Benachrichtigungen

Durch die Aktivierung hoher Sicherheitseinstellungen werden auch Sicherheitswarnmeldungen aktiviert. Das Folgende ist ein Beispiel für eine Nachricht, die nach einer Genehmigung angezeigt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitswarnungsbenachrichtigung



Eigenschaften der strengen Sicherheitseinstellungen

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
glide.ui.escape_text	XML-Werte auf Parser-Ebene für die Benutzeroberfläche mit Escape-Zeichen versehen. Verhindert reflektierte und gespeicherte websiteübergreifende Skripting-Angriffe. Diese Eigenschaft ist im Service Portal nicht anwendbar. **Hinweis:** Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.	Ja	XML
glide.ui.escape_all_script	Erzwingt alle Ausdrücke in Jelly-JavaScript	Ja in neuen Instanzen	Escape Jelly

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	<![CDATA[<script type="text/javascript">]]> -Tags, die standardmäßig mit Escape-Zeichen versehen werden sollen. Erzwingt Escaping nur, wenn das Typ-Attribut in der <![CDATA[<script> Das Tag]]> ist leer oder der Wert ist text/javascript, text/ecmascript, application/javascript, application/ecmascriptoder application/x-javascript.		
glide.ui.rotate_sessions	Rotieren Sie HTTP-Sitzungsbezeichner, um Sicherheitsschwachstel zu reduzieren. Siehe: http://www.owasp.org/index.php/Session_Management#Rota .	Ja **Hinweis:** Wenn Sie das SAML 2.0-Plugin für die Single Sign-on-Authentifizierung verwenden, legen Sie diese Eigenschaft auf Nein fest. Andernfalls wird die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigt.	HTTP-Sitzungsbezeichner rotieren
glide.ui.secure_cookies	Sichere Sitzungscookies aktivieren: Aktivieren Sie zusätzliche Cookie-Sicherheit. Wenn **Ja**, wird eine strikte Validierung	Ja	Sichere Sitzungscookies

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	des Sitzungscookies erzwungen.		
glide.security.password_reset.uri	Für Mobilgeräte Passwortzurücksetzung: URL, zu der der Benutzer weitergeleitet wird, wenn er auf **Passwort vergessen?** klickt. Schaltfläche.		Keine
glide.security.strict.updates	Überprüfen Sie die Sicherheit eingehender Transaktionen während der Formularübermittlung noch einmal (Rechte werden immer bei der Formulargenerierung überprüft). **Hinweis:** Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.	Ja	Überprüfen Sie eingehende Transaktionen noch einmal
glide.security.strict.actions	Überprüfen Sie die Bedingungen für UI-Aktionen vor der Ausführung. Normalerweise werden Bedingungen nur beim Rendern	Ja	Überprüfen Sie die UI-Aktion vor der Ausführung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	des Formulars überprüft.		
glide.security.use_csrf_token	Aktivieren Sie die Verwendung eines sicheren Tokens, um eingehende Anforderungen zu identifizieren und zu validieren. Dieses Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.	Ja	Anti-CSRF-Token
glide.ui.escape_html_list_field	Escape-HTML für HTML-Felder in einer Listenansicht.	Ja	Escape-Zeichen für HTML
glide.html.escape_script	JavaScript-Tags in HTML-Feldern mit Escape-Zeichen versehen.	Ja	Escape-Zeichen für Javascript
glide.ui.forgetme	Entfernen Sie das Kontrollkästchen Benutzernamen speichern von der **Anmeldeseite**.	Ja	„Benutzernamen speichern“ entfernen
glide.smtp.auth	Authentifizieren Sie sich beim SMTP-Server anhand der Eigenschaften Benutzername und Passwort. **Hinweis:** Diese Eigenschaft ist veraltet.	Ja	SMTP-Authentifizierung (veraltet)
glide.script.verwenden.sandbox	Führen Sie vom Client generierte Skripts (AJAXEvaluate und Abfragebedingungen) in einer Sandbox mit eingeschränkten	Ja	Vom Client generierte Skripts in der Sandbox

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Rechten aus. Wenn **Ja**, sind nur die Business Rules und Skripteinbindungen verfügbar, bei denen das Kontrollkästchen **Vom Client aufrufbar** auf **Ja** festgelegt ist, und bestimmte Backend-API-Aufrufe werden nicht zugelassen. Weitere Informationen finden Sie unter Konfigurieren der Skript-Sandbox-Eigenschaft.		
glide.soap.strict_security	Erzwingen Sie strikte Sicherheit für eingehende SOAP-Anforderungen. Erfordert, dass eingehende SOAP-Anforderungen den Sicherheitsmanager für Tabellen- und Feldzugriff durchlaufen, und überprüft SOAP-Benutzer auf die richtigen Rollen für die Verwendung des Webservices.	Ja	Strikte Sicherheit für SOAP-Anforderungen
glide.basisauth.erforderlich.wsdl	Berechtigung für eingehende WSDL-Anforderungen anfordern.	Ja	WSDL-Anforderungsautorisierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Hinweis: Wenn Sie keine Autorisierung für eingehende WSDL-Anforderungen anfordern möchten, müssen Sie die Zugriffskontrollregeln (ACL) ändern, damit Gastbenutzer auf den WSDL-Inhalt zugreifen können.		
glide.basisauth.erforderlich.csv	Standardautorisierung für eingehende CSV-Anforderungen anfordern .	Ja	CSV-Anforderungsautorisierung
glide.basisauth.erforderlich.excel	Basic Authorization für eingehende Excel-Anforderungen anfordern.	Ja	Autorisierung von Excel-Anforderungen
glide.basisauth.erforderlich.importprozessor	Standardautorisierung für eingehende Importanforderungen anfordern.	Ja	Autorisierung der Importanforderung
glide.basisauth.erforderlich.pdf	Standardautorisierung für eingehende PDF-Anforderungen anfordern.	Ja	Autorisierung von PDF-Anforderungen
glide.basisauth.erforderlich.rss	Standardautorisierung für eingehende RSS-Anforderungen anfordern.	Ja	Autorisierung von RSS-Anforderungen
glide.basicauth.required.scriptedprocessor	Standardautorisierung für eingehende Skriptanforderungen anfordern.	Ja	Autorisierung von Skriptanforderungen
glide.basisauth.erforderlich.soap	Standard-Berechtigung für eingehende SOAP-Requests anfordern.	Ja	Standardauthentifizierung: SOAP-Anforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
glide.basisauth.erforderlich.unl	Basic Authorization für eingehende Entladeanforderungen anfordern.	Ja	Autorisierung der Entladeanforderung
glide.basisauth.erforderlich.xml	Standardautorisierung für eingehende XML-Anforderungen anfordern.	Ja	XML-Anforderungsautorisierung
glide.basisauth.erforderlich.xsd	Basic Authorization für eingehende XSD-Anforderungen anfordern.	Ja	Autorisierung von XSD-Anforderungen
glide.cms.catalog_uri_relative	Erzwingen Sie relative Links über den URI-Parameter in /ess/catalog.do. Bei **Ja**werden nur relative URLs über die Seite /ess/catalog.do mit dem Parameter *uri* zugelassen. Wenn **Nein**, sind alle URLs zulässig, was die Verknüpfung mit externen, nicht autorisierten Inhalten ermöglichen kann.	Ja	Erzwingen Sie relative Links
glide.set_x_frame_options	Aktivieren Sie diese Eigenschaft, um den X-Frame-Options-Antwortheader für alle UI-Seiten auf SAMEORIGIN festzulegen. Der X-Frame-Options HTTP Response Header kann verwendet werden, um anzugeben, ob der Browser eine Seite in einem <frame> oder <iframe> rendern kann. Websites können diese Eigenschaft	Ja	X-Frame-Options: SAMEORIGIN

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihr Inhalt nicht in andere Websites eingebettet wird. https://developer.mozilla.org/en/the_x-frame-options_response_header		
glide.ui.attachment.download_mime_types	Eine Liste von durch Kommas getrennten MIME-Typen für Anhänge, die im Browser nicht inline dargestellt werden. Verhindert websiteübergreifende Skripting-Angriffe. Beispielsweise erzwingt `text/html`, dass HTML-Dateien als Anhänge auf den Client heruntergeladen und nicht inline im Browser angezeigt werden.	`text/html,image/svg,image/svg+xml`	Download von MIME-Typen erzwingen
glide.security.groupby_acl_check	Wenn diese Eigenschaft aktiviert ist, werden ACL-Prüfungen für GroupBy-Vorgänge für die Gruppennamen basierend auf den tatsächlichen Daten aus den Gruppen ausgeführt.	Ja	Keine
glide.security.diag_txns_acl	Bei **Ja** kann nur der Administrator oder der Benutzer mit der zulässigen IP-Adresse auf `stats.do`, `threads.do` und `replication.do` zugreifen.	Nein	Leistungsüberwachung (ACL)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
glide.ui.security.codetag.allow_script	Zulassen, dass eingebetteter HTML-Code (mit [code]-Tags) JavaScript-Tags enthält. **Hinweis:** Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.	Nein	Lassen Sie eingebetteten HTML-Code zu
glide.script.allow.ajaxevaluieren	Aktivieren Sie den AJAXEvaluate-Prozessor. Mit dem API-Aufruf `AJAXEvaluate` kann der Client beliebige Skripts senden und auf dem Server ausführen.	Nein	Aktivieren Sie AJAXEvaluate
glide.login.autocomplete	Browsern die Verwendung der automatischen Vervollständigung für Passwortfelder in Anmeldeformularen erlauben.	Nein	Automatisches Ausfüllen des Passwortfelds

Die folgenden Eigenschaften werden in der Tabelle „sys_properties“ definiert, sind jedoch auf der Seite „Strenge Sicherheitseinstellungen“ nicht sichtbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
com.glide.communications.httpclient.verify_hostname	Überprüfen Sie den Hostnamen und die Zertifikatkette, die von Remote-SSL-Hosts angegeben werden. Schützen Sie sich vor MITM-Angriffen (Man-In-The-Middle). Weitere Informationen finden Sie unter Kubernetes-Spoke einrichten **Hinweis:** Diese Eigenschaft überschreibt die Eigenschaft com.glide.communications.trustmanager_trust_all.	Wahr	Keine
glide.basisauth.erforderlich.schema	Basic Authentication für eingehende Tabellenschema-Anforderungen anfordern.	Wahr	Keine
glide.security.csrf_previous.allow	Verwendung eines abgelaufenen sicheren Tokens zum Identifizieren und Validieren eingehender Anforderungen zulassen. Dieses Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.	false	Keine
glide.security.csrf_previous.time_limit	Zeit in Sekunden, bis ein sicheres Token abläuft. Ermöglicht die Kontrolle über die Gültigkeitsdauer des vorherigen CSRF-	86400 **Hinweis:** Wert in Sekunden. Entspricht 1 Tag.	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Tokens. Wenn die Benutzersitzung abläuft, läuft das sichere Token ab, es sei denn, die Eigenschaft *glide.security.csrf_previous.allow* ist aktiviert und sie liegt innerhalb des von dieser Eigenschaft beschriebenen Zeitrahmens. Dieses Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.		
glide.security.csrf.strict.validation.mode	Erzwingt die strikte Überprüfung von CSRF-Token, wobei das erneute Übermitteln der Anforderung durch Benutzer nicht erlaubt ist, wenn das CSRF-Token nicht übereinstimmt.	false	Strenge CSRF-Validierung
com.glide.security.check_unsanitized_html	Erzwingt das Bereinigungsverhalten von „translated_html“-Feldern auf globaler Ebene für Feldzuweisungen.	erzwingen	Keine

Konfigurieren der Skript-Sandbox-Eigenschaft

Aktivieren Sie die Skript-Sandbox-Eigenschaft (*glide.script.use.sandbox*), um vom Client generierte Skripts in einer Sandbox mit eingeschränkten Rechten auszuführen.

Es gibt zwei Fälle im System, in denen der Client Skripts zur Auswertung an den Server senden kann.

- Filter und/oder Abfragen: Es ist zulässig, einen Filter an den Server zu senden, z. B. `assigned_to=javascript:getMyGroups()`.
- System-API: Der API-Aufruf *AJAXEvaluate* ermöglicht es dem Client, beliebige Skripts auf dem Server auszuführen und eine Antwort zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Skript-Sandbox-Eigenschaft (`glide.script.use.sandbox`) aktivieren, wird das über einen dieser beiden Einstiegspunkte ausgewertete Skript in einer Sandbox mit eingeschränkten Rechten mit den folgenden Eigenschaften ausgeführt:

- Nur die Business Rules, die als vom **Client aufrufbar** markiert sind, sind in der Sandbox verfügbar.
- In der Sandbox sind nur Skripteinbindungen verfügbar, die als vom **Client aufrufbar** markiert sind.
- Bestimmte API-Aufrufe (hauptsächlich, aber nicht vollständig beschränkt auf Aufrufe mit direktem DB-Zugriff) sind nicht zulässig.
- Daten können in der Sandbox nicht eingefügt, aktualisiert oder gelöscht werden. Alle Aufrufe von `current.update()`werden beispielsweise ignoriert.

Hinweis:
Weitere Informationen zu dieser Eigenschaft finden Sie unter Vom Client generierte Skripts in der Sandbox in Härtungseinstellungen für Instanzsicherheit.

Diese Methoden sind in vom Client generierten Skripts nicht zulässig, wenn Skript-Sandboxing aktiviert ist.

Eingeschränkte Methoden

Klasse	Methode
GlideRecord	• `deleteMultiple()` • `löschenDatensatz()` • `getRowCount()` • `einfügen ()` • `aktualisieren ()` • `updateMultiple ()`
GlideSystem (gs)	• `addErrorMessage()` • `addInfoMessage()` • `addMessage()` • `eventQueue()` • `FlushMessages ()` • `getEscapedProperty()` • `getProperty()` • `Protokoll ()` • `logError ()` • `logWarning()` • `setProperty()` • `setRedirect()`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte Methoden (Fortsetzung)

Klasse	Methode
	• `setReturn()` • `workflowFlush()`
ScopedGlideRecord	• `deleteMultiple()` • `löschenDatensatz()` • `einfügen ()` • `aktualisieren ()` • `updateMultiple ()`
ScopedGlideSystem (gs)	• `addErrorMessage()` • `addInfoMessage()` • `debuggen ()` • `eventQueue()` • `ausführenNow()` • `getProperty()` • `getSessionToken()` • `Info ()` • `setRedirect()`
GlideDate GlideDateTime GlideTime	• `add()` • `addDays()` • `addDaysLocalTime()` • `addDaysUTC()` • `addMonthsLocalTime()` • `addMonths()` • `addSeconds()` • `addWeeks()` • `addYears()` • `vergleichenMit()` • `getByFormat ()` • `getDate()` • `getDayOfWeek ()` • `getDayOfWeekUTC` • `getDayOfWeekLocalTime()`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte Methoden (Fortsetzung)

Klasse	Methode
	• `getDayOfMonth ()` • `getDayOfMonthLocalTime()` • `getDayOfMonthNoTZ()` • `getDayOfWeek ()` • `getDayOfWeekLocalTime()` • `getDayOfWeekUTC()` • `getHourOfDayLocalTime()` • `getHourOfDayUTC()` • `getDaysInMonth ()` • `getDaysInMonthUTC()` • `getDaysInMonthLocalTime()` • `getDisplayValueInternal()` • `getDisplayValue ()` • `getHourLocalTime()` • `getLocalDate()` • `getLocalTime()` • `getMinutesLocalTime()` • `getMinutenUTC()` • `getMonthLocalTime()` • `getMonthNoTZ()` • `getMonthUTC()` • `getNumericValue()` • `getSeconds()` • `getTime ()` • `getTZOffset()` • `getValue ()` • `getYear()` • `getUserTimeZone()` • `getWeekOfYearLocalTime()` • `getWeekOfYearUTC()` • `getYearUTC()` • `getYearLocalTime()` • `istDST()` • `onOrAfter()`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte Methoden (Fortsetzung)

Klasse	Methode
	• `onOrBefore()` • `setDayOfMonthUTC()` • `setDisplayValue()` • `setMonth()` • `setNumericValue()` • `setTZ()` • `setValue()` • `setValueUTC()` • `subtract()` • `toString()`
GlideSchedule	• `add()` • `isInZeitplan()` • `Laden ()` • `wannNext()`

Hinweis:
Die GlideSystem (gs)-Methoden `log()`, `logError()`und `logWarning()` können mit Skript-Sandboxing aktiviert werden, indem die Systemeigenschaft `glide.security.sandbox_no_logging` auf falsegesetzt wird.

Wenn Sie das System ohne aktiviertes Skript-Sandboxing ausführen, gilt keine dieser Einschränkungen.

Hinweis:
Diese Eigenschaft ist standardmäßig aktiviert, wenn Sie das Plugin „Strenge Sicherheitseinstellungen“ aktivieren. Aktivieren Sie diese Eigenschaft nicht außerhalb des Plugins.

Strenge Sicherheitseinstellungen werden aktiviert

Das Plugin „High Security Settings“ ist standardmäßig in allen neuen Instanzen aktiv. Wenn es in Ihrer Instanz nicht aktiv ist, können Sie das Plugin anfordern.

Vorbereitungen
Erforderliche Rolle: keine

Bevor Sie die strengen Sicherheitseinstellungen für eine vorhandene Instanz aktivieren :

1. Überprüfen Sie die folgenden Informationen, um das neue Verhalten zu verstehen:
   - Zugriffskontrolllistenregeln
   - Strenge Sicherheitseinstellungen
   - Standardmäßige Deny-Eigenschaft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

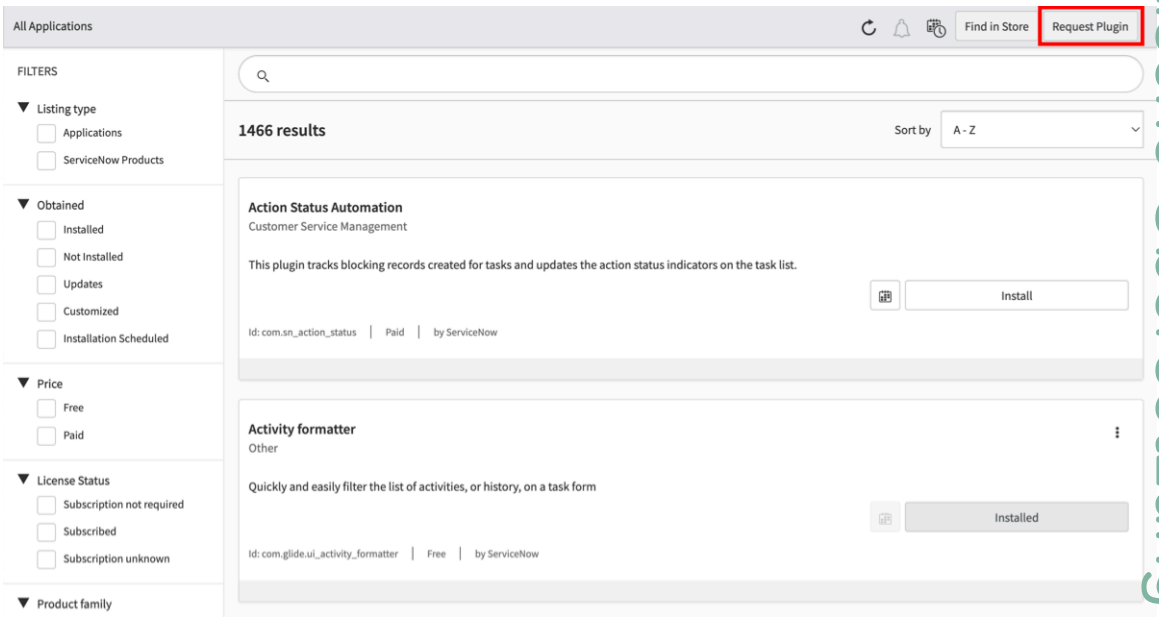
2. Aktivieren Sie das Plugin in einer Nicht-Produktionsinstanz. Ein aktueller Klon der Produktion ist vorzuziehen.
3. Testen Sie die überarbeitete Funktionalität, insbesondere die hinzugefügten ACLs und die Standardverweigerungs-Funktionalität. Setzen Sie die Tests fort, bis das System wie erwartet funktioniert. Wenn Benutzer nicht auf erwartete Ressourcen zugreifen können, stellen Sie sicher, dass sie über die entsprechenden Rollen und ACL-Regeln verfügen, um ihnen den Zugriff zu gewähren.
4. Erstellen Sie Update Sets aller erforderlichen Änderungen, damit Sie sie auf die Produktion anwenden können.

Hinweis:
Weitere Informationen zu diesem Plugin finden Sie unter Hochsicherheits-Plugin in den Härtungseinstellungen für die Instanzsicherheit.

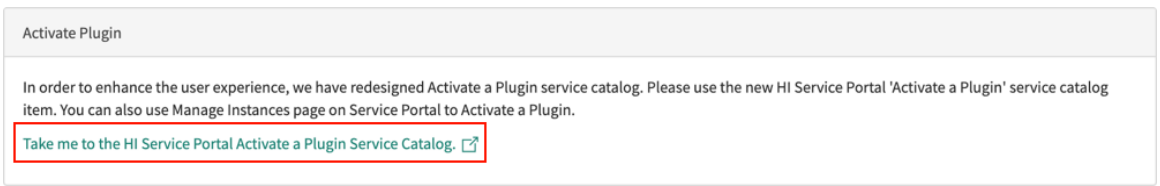
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“

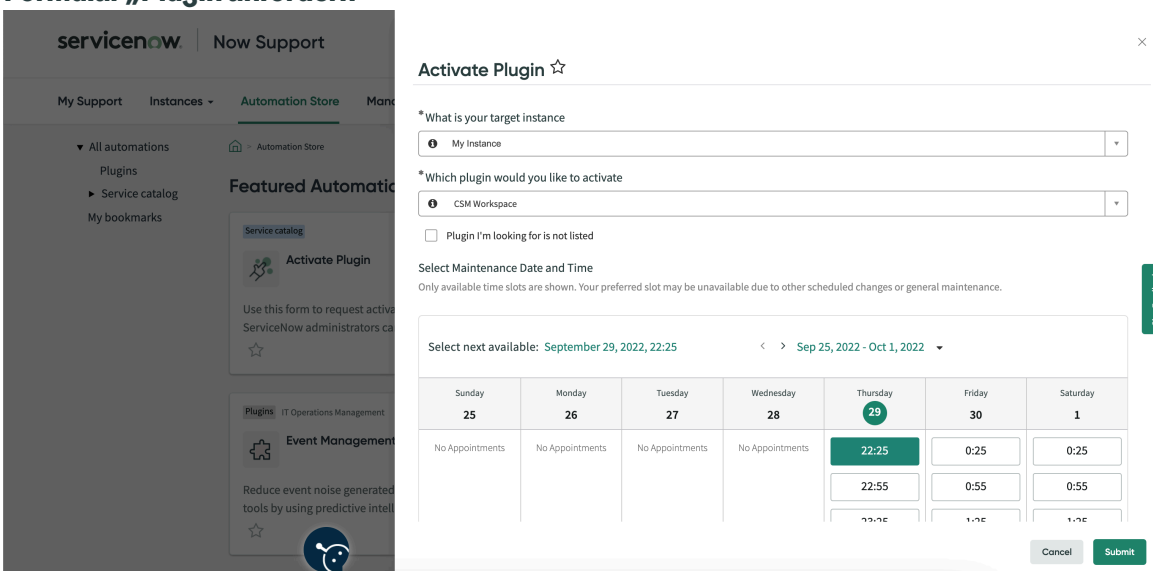
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
Weitere Informationen zum Anfordern eines Plugins finden Sie unter Plugins aus dem Servicekatalog anfordern [KB0751715] im Now Support Knowledge Base.

HTML-Bereinigung

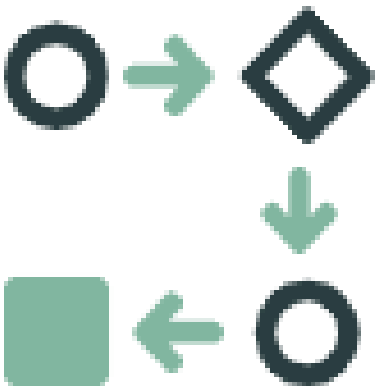
Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Erkunden Sie die HTML-Bereinigung

Erfahren Sie, wie die HTML-Bereinigung funktioniert.

Konfigurieren Sie die HTML-Bereinigung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Konfigurieren Sie die HTML-Bereinigung.
Aktivieren Sie die HTML-Bereinigung  Erfahren Sie, wie Sie die HTML-Bereinigung aktivieren.	

Durchsuchen der HTML-Bereinigung

Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Verwenden Sie die HTML-Bereinigung, um sicherzustellen, dass HTML-Inhalte in Ihrer Instanz keine potenziell schädlichen Inhalte enthalten. Bei der HTML-Bereinigung werden HTML-Tags entfernt, die dazu verwendet werden könnten, Ihre Instanz zu gefährden, z. B. <![CDATA[<script>]]>-, <link>- oder `<embed>` -Tags, die dazu verwendet werden können, unerwünschte Skripts in Ihrer Instanz auszuführen oder Benutzer zu unerwünschten Inhalten zu leiten. Sichere Tags, die die Formatierung Ihrer Inhalte steuern, bleiben erhalten. Als Administrator können Sie anpassen, welche Inhalte entfernt oder beibehalten werden. Sie können auch steuern, ob die Bereinigung für alle Inhalte oder nur für von Ihnen angegebene Felder gilt.

Die HTML-Bereinigung überprüft die integrierte Aufnahmeliste auf Markup, das Sie immer beibehalten möchten. Der Sanitizer stellt die `HTMLSanitizerConfig` -Skripteinbindung bereit, mit der Administratoren die integrierte Aufnahmeliste ändern können. Elemente können auch der Ausschlussliste hinzugefügt werden, um HTML-Markup zu entfernen. Der Inhalt der Ausschlussliste überschreibt die Aufnahmeliste.

Die folgenden Arten von Elementen können den Aufnahme- und Ausschlusslisten hinzugefügt werden:

- Globale Attribute
- Beliebige HTML-Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Standardmäßig unterstützen URL-Attribute wie `href` und `src` nur die folgenden Protokolle:

- `http`
- `https`
- `mailto`
- `Daten`

Beispiel:

```
<a href="https://community.servicenow.com/community">ServiceNow Community</a>
```

Hinweis:
Weitere Informationen zur Eigenschaft *`glide.html.sanitize_all_fields`*, die die Verwendung der HTML-Bereinigung steuert, finden Sie unter HTML-Bereinigung in den Härtungseinstellungen für die Instanzsicherheit.

Konfigurieren Sie urlAttributes und die Protokolle

Sie können urlAttributes und ihre Protokolle in der **HTMLSanitizer** -Skripteinbindung konfigurieren. Beispiel:

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
          - -
          - -
    }
```

Da sich `Notizen` in diesem Beispiel in der Aufnahmeliste befinden, wird diese URL nicht bereinigt:

```
<a title=“Lotus”
 href=“Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257EE
A003456FD”>Lotus</a></p>
```

Standardaufnahmeliste

Hinweis:
Die Standardaufnahmeliste ist eine Systemliste, auf die Benutzer in der Instanz nicht zugreifen können.

```
BUILTIN_HTML_WHITELIST :{

  globalAttributes:{ attribute:["id","class","lang","title","style"],

                     attributeValuePattern:{}},

  label:{ attribute:["for"]},

  font:{ attribute:["color","face","size"]},

  a:{ attribute:["href","nohref","name","shape"]},

  img:{ attribute:["src","name","alt","border","hspace","vspace","align","height","width"},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
   table:{ attribute:["border","cellpadding","cellspacing","bgcolor","background","align","no
 resize","height","width","summary","frame","rules"]},


 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},


 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},

   tr:{ attribute:["background","height","width","align","valign","char off","char"]},

   thead:{attribute:["align","valign","char off","char"]},

   tbody:{attribute:["align","valign","char off","char"]},

   tfoot:{attribute:["align","valign","char off","char"]},

   colgroup:{attribute:["align","valign","char off","char","span","width"]},

   col:{attribute:["align","valign","char off","char","span","width"]},

   p:{attribute:["align"]},

   style:{attributeValuePattern:{"type":"text/css"}}

   canvas:{ attribute:["height","width"]},

   details:{ attribute:["open"]},

   summary:{ attribute:["open","valign","char off","char"]},

   button:{ attribute:["disabled","accesskey","type"]},

   form:{},


 input:{ attribute:["size","maxlength","checked","alt","src","type","disabled","readonly","accessk
ey","border","usemap"]},

   select:{ attribute:["disabled","multiple","size"]},

   textarea:{ attribute:["rows","cols","disabled","readonly","accesskey"]},

   option:{ attribute:["disabled","label","selected"]},

   div:{ attribute:["align"]},

   ol:{ attribute:["start","type","square"]},

   ul:{ attribute:["type","square","itemscope","itemtype","itemref"]},

   li:{ attribute:["value","fb__id","itemprop"]},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
span:{ attribute:["color","size","data-mce-bogus","itemprop","face"]},

br:{ attribute:["clear"]},

h3:{ attribute:["itemprop"]},

html:{ attribute:["xmlns","lang","xml:lang"]},

link:{ attribute:["rel","type","href","charset"]},

meta:{ attribute:["name","content","scheme","charset","http-equiv"]},

pre:{ attribute:["xml:space"]},

noscript:{},  h1:{},  h2:{},  h4:{},  h5:{},  h6:{},

i:{},  b:{},  u:{},  strong:{},  em:{},  small:{},  big:{},

pre:{},  code:{},  cite:{},  samp:{},  sub:{},  sup:{},

strike:{},  center:{},  blockquote:{},  hr:{},  map:{},

dd:{},  dt:{},  dl:{},  fieldset:{},  legend:{}, figure:{},  tt:{},

body:{},  caption:{},  head:{},  title:{},  shape:{},},
```

Konfigurieren der HTML-Bereinigung

Sie müssen eine Skripteinbindung ändern, um Konfigurationsänderungen an der HTML-Bereinigung vorzunehmen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**.
2. Öffnen **Sie HTMLSanitizerConfig**.
3. Verwenden Sie die Klasse HTML_BLACKLIST, um der Ausschlussliste Elemente hinzuzufügen.

   Um der Aufnahmeliste Elemente hinzuzufügen, verwenden Sie die Klasse HTML_WHITELIST.

   Verwenden Sie dieses Format:

```
HTML_XXXXLIST :{
      globalAttributes :{

         attribute:[attribute-name1,...],
         attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,...}

      },<html-element-name>:{// Same as Above},----}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *globalAttributes* enthält Attribute- oder attributeValuePattern-Elemente, die global für alle HTML-Elemente gelten.
- *attribute* ist eine durch Kommas getrennte Liste von Attributen.
- *attributeValuePattern* ist ein Dictionary von Attribut-zu-Attribut-Wert-Regex-Muster-Paaren. „attribute-value-regex-pattern“ ist ein regulärer Ausdruck, der mit dem Attributwert übereinstimmen muss.

Example:
Betrachten Sie das folgende Beispiel:

```
HTML_WHITELIST:{
      globalAttributes:{
         attribute:["id","name"],},
      img:{
         attribute:["style","align"],
         attributeValuePattern:{src:".*jpeg"}},
      iframe:{},}
```

Sie fügt der Aufnahmeliste die folgenden Elemente hinzu:

- Die globalen Attribute id und name. Dies ist eine Liste von Zeichenfolgen, die global auf alle Elemente angewendet werden kann.
- Das img-Element, in dem die Attribute „style“ und „align“ lauten.
- Das img-Element, bei dem das Quellattribut des Bildes eine Datei mit der Erweiterung „.jpeg“ ist. Dies ist ein Beispiel für ein Muster eines regulären Ausdrucks, das einem Attributwert entspricht.
- Das iframe-Element.

Aktivieren der HTML-Bereinigung

Die HTML-Bereinigung bietet eine Eigenschaft zum Aktivieren oder Deaktivieren der Bereinigung für alle HTML-Felder im System.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig ist die Eigenschaft für neue Instanzen auf „true“ festgelegt.

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein.
2. Legen Sie die Eigenschaften *glide.html.sanitize_all_fields* und *glide.translated_html.sanitize_all_fields* auf **true fest**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Weitere Informationen zu dieser Eigenschaft finden Sie unter HTML-Bereinigung in Härtungseinstellungen für Instanzsicherheit.

Trouble?

Wenn die Eigenschaften in der Tabelle „Systemeigenschaften“ nicht vorhanden sind, können Sie sie hinzufügen.

Aktivieren der Bereinigung einzelner Felder

Sie können Feldattribute verwenden, um die Bereinigung für einzelne Felder zu aktivieren oder zu deaktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie müssen zuerst die Bereinigungseigenschaft auf „falsch“ festlegen und dann die Bereinigung für jedes Formular pro Feld aktivieren.

Prozedur

1. Navigieren Sie zur Tabelle sys_properties, und legen Sie `glide.html.sanitize_all_fields` auf **false**fest.
   Dadurch wird die Bereinigung für alle HTML-Felder im System deaktiviert.
2. Navigieren Sie zu dem Formular, das das HTML-Feld enthält.
3. Klicken Sie mit der rechten Maustaste auf die HTML-Feldbezeichnung, und wählen Sie **Dictionary konfigurieren**aus.
   Das Wörterbucheintragsformular wird für das Feld HTML geöffnet.
4. Geben Sie einen der folgenden Werte in das Feld Attribute ein:
   - Um die Bereinigung zu deaktivieren, geben Sie `html_sanitize=false`ein
   - Um die Bereinigung zu aktivieren, geben Sie `html_sanitize=true`ein
5. Klicken Sie auf **Aktualisieren**.
6. Um die HTML-Bereinigung für übersetzte HTML-Felder zu aktivieren, legen Sie die Eigenschaft `glide.translated_html.sanitize_all_fields`**auf true**fest.

Aktivieren der HTML-Bereinigungsprotokollierung

Wenn die HTML-Bereinigung Elemente oder Attribute entfernt, werden sie dem Systemprotokoll hinzugefügt.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können diese bereinigten Elemente überprüfen, indem Sie /syslog_list.do?sysparm_query=source%3DHTMLSanitizer zu Ihrer Instanz-URL hinzufügen.

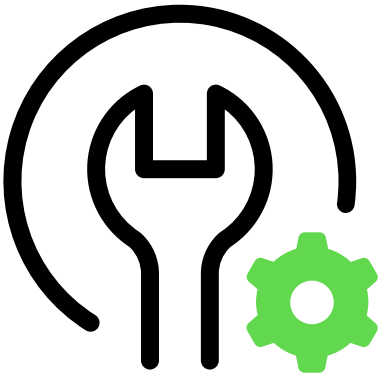
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um diese bereinigten Elemente zu überprüfen, fügen Sie `/syslog_list.do?sysparm_query=source%3DHTMLSanitizer` Ihrer Instanz-URL hinzu.
2. Um die Protokollierung zu aktivieren oder zu deaktivieren, fügen Sie den Systemeigenschaften die Eigenschaft `glide.html_sanitize.discarded_log.enable` hinzu, und legen Sie den Wert auf **true** (aktiviert) oder **false** (deaktiviert) fest.
   Diese Eigenschaft ist standardmäßig **true**.

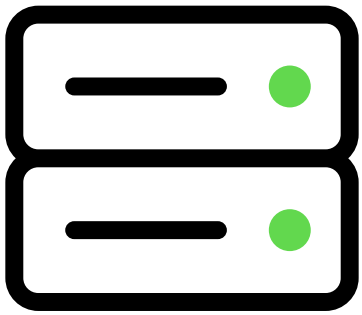
Andere Einstellungen und Sicherheitsressourcen

Dieser Abschnitt enthält Sicherheitseigenschaften, die Sie außerhalb des Instanz-Sicherheitszentrums festlegen, sowie andere sicherheitsbezogene Ressourcen.



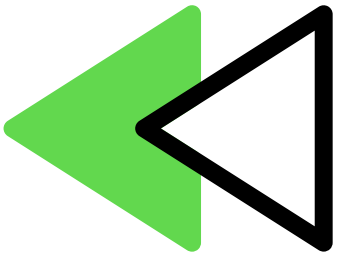
Eigenschaften des Sicherheitssystems

Sicherheitseinstellungen bieten mehrere Eigenschaften, um die Sicherheitsstufe in Ihrer Instanz zu steuern.



Leitfaden zur MID Server-Bereitstellung

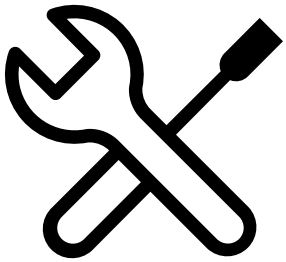
Der MID-Server (ServiceNow Management, Integration, and Discovery) ist eine schlanke Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf Standardhardware ausgeführt wird, einschließlich virtueller Computer.



Umkehrbares Verhalten

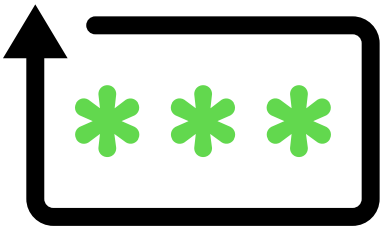
Es gibt Systemeigenschaften, die entweder als „safe_overrides“ oder „no_db_override“ kategorisiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



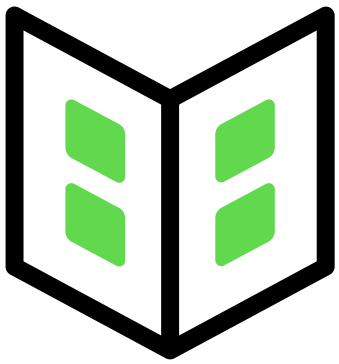
Veraltete Sicherheitseigenschaften

Diese Sicherheitseigenschaften waren in früheren Releases veraltet.



Verwenden der Javascript-Inhaltszugriffssteuerung

Sie können die JavaScript-Inhaltszugriffssteuerung verwenden, um die Liste der blockierten JavaScript-URLs von Drittanbietern in Ihrer Instanz zu ändern.



Andere Sicherheitshärtungsressourcen

Zusätzliche Informationsquellen zur Härtung von Sicherheitskontrollen im Zusammenhang mit der Now Platform.

Eigenschaften der Sicherheitseinstellungen

Sicherheitseinstellungen bieten mehrere Eigenschaften, um die Sicherheitsstufe in Ihrer Instanz zu steuern.

Es gibt mehrere Möglichkeiten, die Eigenschaften der allgemeinen Sicherheitseinstellungen festzulegen oder zu ändern.

- Navigieren zu **Systemeigenschaften** > **Sicherheit**.

  Optionen auf der Seite „Sicherheit“ sind **Ja** oder **Nein**.

- Navigieren Sie zu **sys_properties.list**, und suchen Sie nach der Eigenschaft, die Sie festlegen oder ändern möchten.

  Optionen in der Tabelle „Systemeigenschaften“ [sys_properties.list] lauten **true** oder **false**.

- Navigieren zu **Systemsicherheit** > **Instanz-Sicherheitszentrum**, und klicken Sie dann auf **Härtung**.

  Sie können die Einstellungen für die wichtigsten und kritischsten Sicherheitseigenschaften konfigurieren. Der Inhalt „Härtungseinstellungen für Instanzsicherheit“ enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform. Weitere Informationen zu diesen Eigenschaften finden Sie unter Härtungseinstellungen für die Instanzsicherheit.

⚠ Warnung:
Wenn Sie eine dieser Sicherheitsfunktionen implementieren, müssen Sie die Funktionen gründlich testen, bevor Sie sie in einer Produktionsinstanz bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support für Codierung und eingebettete Skripts

glide.ui.security.allow_codetag	Unterstützt das Einbetten von HTML-Code mit dem [code]-Tag. Standardwert: Ja **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Lassen Sie eingebetteten HTML-Code zu
glide.ui.security.codetag.allow_script	Ermöglicht eingebettetem HTML (mit [code]-Tags), Javascript-Tags zu enthalten. **Hinweis:** Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport. Weitere Informationen finden Sie unter JavaScript-Tags in eingebettetem HTML zulassen.
glide.ui.escape_all_script	Erzwingt alle Ausdrücke in Jelly-JavaScript <![CDATA[<script type="text/javascript">]]> -Tags, die standardmäßig mit Escape-Zeichen versehen werden sollen. Erzwingt Escaping nur, wenn das Typ-Attribut in der <![CDATA[<script> Das Tag]]> ist leer oder der Wert ist text/javascript, text/ecmascript, application/javascript, application/ecmascriptoder application/x-javascript. • Standardwert: ◦ Neue/zbootete Instanzen: true ◦ Aktualisierte Instanzen: false • Empfohlener Wert: Ja **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Escape Jelly

Anhangbeschränkungen und Verhalten

com.glide.attachment.max_size	Legt die maximale Dateianlagengröße in Megabyte fest.
glide.attachment.role	Listet die Rollen (kommagetrennt) auf, die Anhänge erstellen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glide.attachment.extensions	Listet die Dateierweiterungen (kommagetrennt) auf, die über den Anhangsdialog an Dokumente angehängt werden können. Erweiterungen dürfen den Punkt (.) nicht enthalten. Beispiel: xls, xlsx, doc, docx. Lassen Sie das Feld leer, um alle Erweiterungen zuzulassen. **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Dateierweiterungen einschränken
glide.ui.attachment.force_download_all_mime_types	Erzwingt den Download aller MIME-Typ-Anhangdateien (Multifunktions-Internet-Mail-Erweiterungen). Standardwert: • Neue/zbootete Instanzen: Ja • Aktualisierte Instanzen: Nein **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Download von MIME-Typen erzwingen
glide.security.file.mime_type.validation	Aktiviert (**Ja**) oder deaktiviert (**Nein**) die MIME-Typvalidierung für Dateianhänge. Über `glide.attachment.extensions` konfigurierte Dateierweiterungen werden während des Uploads auf den MIME-Typ überprüft. Standardwert: • Neue/zbootete Instanzen: Ja • Aktualisierte Instanzen: Nein **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: MIME-Typeinschränkung für Uploads

Kunden-Uploads

Diese Eigenschaften wirken sich nur auf Kunden-Uploads aus. Sie wirken sich nicht auf Anhänge aus.

glide.ui.strict_customer_uploaded_static_content	Wenn Sie diese Eigenschaft auf **Ja**festlegen, wird die Möglichkeit aktiviert, die Dateitypen einzuschränken, die heruntergeladen werden können, wenn sie mit der Funktion „Datei hochladen“ von Now

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Platformhochgeladen wurden. Verwendet mit *glide.ui.strict_customer_uploaded_content_types* **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Aktivieren Sie Einschränkungen beim Dateidownload
glide.ui.strict_customer_uploaded_content_types	Wenn dieser Parameter eine Liste von durch Kommas getrennten Dateitypen enthält, können von den Dateien, die mit der Funktion „Datei hochladen“ von Now Platformhochgeladen wurden, nur diese Dateitypen von der Instanz heruntergeladen werden. **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Geben Sie herunterladbare Dateitypen an

Security Manager und Optionen

glide.security.manager	Sicherheitsmanager
glide.sm.default_mode	Standardverhalten des Sicherheitsmanagers, wenn keine ACLs in einer Tabelle vorhanden sind.
glide.security.strict.updates	Überprüft die Sicherheit eingehender Transaktionen während der Formularübermittlung doppelt. Rechte werden bei der Formulargenerierung immer überprüft. **Hinweis:** Diese Eigenschaft ist standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport. Weitere Informationen finden Sie unter Überprüfen Sie eingehende Transaktionen noch einmal.
glide.security.strict.actions	Überprüft Bedingungen für UI-Aktionen vor der Ausführung. Normalerweise werden Bedingungen nur beim Rendern des Formulars überprüft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Hinweis: Einstellungen zum Härten der Instanzsicherheit: Überprüfen Sie die UI-Aktion vor der Ausführung
glide.security.granular.create	Erzwingt die Erstellungsregeln für neue Datensätze (im Gegensatz zu den Schreibregeln, die das Erstellen und Aktualisieren umfassen können).
glide.security.explain.write.locks	Zeigt eine Erklärung zu gesperrten Formularelementen an.

Cookies

glide.ui.forgetme	**Entfernt** das Kontrollkästchen Benutzernamen speichern von der Anmeldeseite, wenn die Instanz entweder LDAP- oder DB-Anmeldungen verwendet. Die aktiven angemeldeten Sitzungen des Benutzers werden nach X Minuten Inaktivität abgebrochen, wobei X der Wert der **Systemeigenschaft glide.ui.session_timeout** ist. Standardwert: Ja (Neue und Z-gestartete Instanzen **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: „Benutzernamen speichern“ entfernen
glide.ui.secure_cookies	Aktiviert sichere Sitzungscookies, um zusätzliche Cookie-Sicherheit zu erzwingen. Wenn **Ja**, wird eine strikte Validierung des Sitzungscookies erzwungen. Wenn Versions-3-Cookies aktiviert sind, werden zusätzliche Sicherheitsanforderungen erzwungen. **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Sichere Sitzungscookies
glide.secure_cookie.debug	Debugging von sicheren Sitzungscookies. Wählen Sie diese Option aus, um die umfangreiche Debug-Protokollierung von Cookie-Vorgängen für sichere Sitzungen zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsbeschränkungen für die Ausführung von Skripts, die vom Client stammen

glide.script.verwenden.sandbox	Führen Sie vom Client generierte Skripts (AJAXEvaluate und Abfragebedingungen) in einer Sandbox mit eingeschränkten Rechten aus. Wenn diese Option aktiviert ist, sind nur die Geschäftsregeln und **Skripteinbindungen** verfügbar, für die das Kontrollkästchen Clientaufrufbar aktiviert ist, und bestimmte API-Aufrufe (Back-End-Anwendungsprogrammierschnittstelle) sind nicht zulässig. **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Vom Client generierte Skripts in der Sandbox
glide.script.allow.ajaxevaluieren	Aktiviert den AJAXEvaluate-Prozessor. **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Aktivieren Sie AJAXEvaluate
glide.script.secure.ajaxgliderecord	Wendet standardmäßige Sicherheits-Zugriffskontrolllisten (ACLs) auf AJAXGlideRecord-Aufrufe an. Standardwert: Ja, für neue und aktualisierte Instanzen. (Wenn **Ja**, kann dies nicht in **Nein**geändert werden.) **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Aktivieren der AJAXGlideRecord-ACL-Überprüfung

Verschiedenes

com.glide.communications.trustmanager_trust_all	Standardmäßig vertraut die Instanz der Zertifizierungsstelle (CA) eines Zertifikats. Stellt sicher, dass die Instanz selbst ausgestellte Zertifikate akzeptiert. Um die Zertifizierungsstelle eines Zertifikats zu validieren, legen Sie diese Eigenschaft auf **Nein**fest

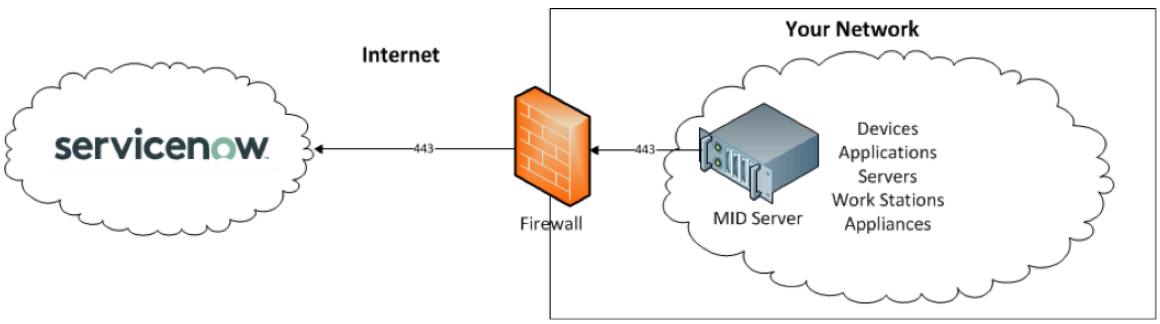
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Hinweis: Einstellungen zum Härten der Instanzsicherheit: Zertifikatvertrauen
glide.ausgehend.sslv3.deaktiviert	Wenn aktiv, erzwingt ausgehende Verbindungen von einer Instanz die Verwendung von Transport Layer Security (TLS) anstelle von Secure Sockets Layer (SSL). **Hinweis:** Einstellungen zum Härten der Instanzsicherheit: Deaktivieren von SSLv2/SSLv3

Zusätzliche Eigenschaften sind für Strenge Sicherheitseinstellungenverfügbar.

Leitfaden zur sicheren MID Server-Bereitstellung (Härtung der Instanzsicherheit)

Der MID-Server ServiceNow Management, Integration, and Discovery ist eine einfache Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf Standardhardware ausgeführt wird, einschließlich virtueller Computer.



Es authentifiziert sich sicher bei Ihrer Instanz in der ServiceNow Cloud mit seinen eigenen Anmeldeinformationen und erleichtert die Datenübertragung mit Ihren Anwendungen, Datenquellen und Services. Mehrere MID Server können in verschiedenen Netzwerksegmenten bereitgestellt werden, um zusätzliche Skalierbarkeit zu bieten.

Berücksichtigen Sie die folgenden Faktoren in Bezug auf die Sicherheit Ihres MID Servers:

Physische Sicherheit

Sichern Sie die physische Hardware, die den MID Server oder den Hypervisor für virtualisierte MID Server hostet.

- Bewahren Sie die Hardware an einem sicheren Ort auf, der die Hardware vor nicht autorisiertem Zugriff schützt.
- Schützen Sie den Zugang zu diesem Standort mit einem elektronischen Kartenleser und Videoüberwachung.
- Platzieren Sie die physische Hardware in einem abgeschlossenen Gehäuse oder einem Rack mit physischer Schlüsselzugriffskontrolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheit der virtuellen Infrastruktur

Verwenden Sie die Virtualisierung von vmit der Flexibilität, mehrere MID Server in virtualisierten Betriebssystemen und Netzwerken in gemeinsam genutzter physischer Hardware zu installieren.

Der Zugriff auf den Hypervisor und die Verwaltungskonsolen der virtuellen Infrastruktur muss geschützt werden, um ein nicht autorisiertes Klonen des virtualisierten MID Servers zu verhindern:

- Beschränken Sie den Zugriff auf den Hypervisor und die Verwaltungskonsolen der virtuellen Infrastruktur durch wenige vertrauenswürdige Administratoren.
- Lassen Sie nur Verbindungen zum internen vertrauenswürdigen Netzwerk für die Managementkonsole wie ESX Server und VirtualCenter zu.
- Verwenden Sie VLANs, um Netzwerkangriffe zu verhindern.
- Befolgen Sie die Sicherheitsrichtlinien, die in den Leitfäden zur Virtualisierungshärtung der Anbieter veröffentlicht wurden.

Betriebssystemsicherheit

Erfahren Sie, wie der MID Server seinen Now Platform -Benutzernamen und sein Passwort in seiner Konfigurationsdatei mit dem Namen `config.xml`für die sichere Authentifizierung bei der Instanz speichert.

Der MID Server muss in einem sicheren und gesicherten Betriebssystem bereitgestellt werden, um Schutz vor nicht autorisiertem Zugriff auf die Anmeldeinformationen zu bieten:

- Beschränken Sie den Zugriff auf das Betriebssystem auf wenige, vertrauenswürdige Administratoren.
- Überwachen Sie die Betriebssystemprotokolle, um nicht autorisierten Zugriff zu erkennen, insbesondere Versuche, auf die Datei config.xml zuzugreifen, da diese Datei wichtige MID Server-Konfigurationsinformationen enthält.
- Installieren Sie regelmäßig Sicherheitspatches für das Betriebssystem mit der neuesten Antivirensoftware, und aktualisieren Sie die Antivirus-Definitionen regelmäßig.
- Der MID Server benötigt ein aktuelles Java-Framework, um ausgeführt werden zu können. Halten Sie Java regelmäßig auf dem neuesten Stand.
- Entfernen oder deaktivieren Sie nicht benötigte Services und Anwendungen.
- Installieren Sie eine BS-Firewall, um den Zugriff auf nicht autorisierte Ports zu beschränken.
- Befolgen Sie die Sicherheitsrichtlinien, die in den Härtungsleitfäden für Betriebssysteme der Anbieter veröffentlicht wurden.

Netzwerksicherheit

Der MID Server kommuniziert über Port 443 über SSL mit der Instanz und erfordert keine eingehenden Verbindungen.

Gehen Sie wie folgt vor, um Ihren MID-Server in einem Netzwerk ordnungsgemäß zu sichern:

- Installieren Sie den MID Server auf einem gesicherten Server hinter einer Unternehmensfirewall, um sich vor nicht autorisiertem Zugriff aus dem Internet zu schützen.
- Konfigurieren Sie die Firewall auf dem MID Server so, dass keine anderen eingehenden Verbindungen akzeptiert werden als die, die für die Unternehmensverwaltung des Betriebssystems und der Hardware erforderlich sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das System, das den MID Server hostet, muss auf die Download-Site ServiceNow unter **install.servicenow.com**zugreifen können.

  Hinweis:
  Diese URL führt zur Download-Site ServiceNow, auf die über dieses Thema nicht zugegriffen werden kann.

  Der MID Server-Hostcomputer muss auf diese Site zugreifen können, um das Installationspaket herunterzuladen. Er kontaktiert **install.servicenow.com** alle 60 Minuten, um zu sehen, ob eine neuere Version verfügbar ist, und führt in diesem Fall ein automatisches Upgrade durch. Ein MID Server-Upgrade findet auch statt, wenn Sie eine Instanz aktualisieren.

Firewall

Konfigurieren Sie Ihre Firewall so, dass ausgehender Netzwerkverkehr vom MID Server zu Ihrer Instanz und dem Auto-Upgrade-Server zugelassen wird.

Verwenden Sie zum Konfigurieren Ihrer Firewall die folgenden Beispielsyntaxen:

- `<source IP> AN<instance_name> .service-now.com AN PORT 443`
- `<source IP> AN install.service-now.com AN PORT 443`

Administration und Management

In diesem Abschnitt werden die Sicherheitspraktiken und -richtlinien für die Verwaltung des MID Servers in Ihrer Umgebung beschrieben.

Erstellen Sie ein Konto mit einer mid_server-Rolle

Erstellen Sie ein Benutzerkonto in der Instanz, die eine mid_server-Rolle enthält.

Befolgen Sie beim Erstellen eines Benutzeraccounts die folgenden Richtlinien:

- Verwenden Sie in der Instanz für den MID Server kein Administratorkonto.
- Verwenden Sie für das MID Server-Konto eine ausreichende Länge und Komplexität des Passworts.
- Das Passwort muss aus mindestens 12 Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.
- Verwenden Sie verschiedene MID Server-Konten mit eindeutigen Passwörtern für verschiedene MID Server in einer Instanz.
- Verwenden Sie die strikte SOAP-Sicherheitsfunktion, um alle Tabellen mit Zugriffssteuerungslisten (ACL) zu schützen, indem Sie *`Enforce strict security on incoming SOAP requests`* in aktivieren **Systemeigenschaften** > **Webservices**.
- Ändern Sie die MID Server-Passwörter in einer Häufigkeit, die der Passwortrichtlinie Ihrer Organisation entspricht.

Hinweis:
Weitere Informationen finden Sie unter MID Server-Benutzer erstellen und Rolle gewähren .

Einrichten eines MID-Servers auf einem Windows-Host

Wenn Sie den MID Server auf einem Windows-Host installieren, wird ein Windows-Dienst erstellt. Standardmäßig wird dieser Service als lokales Windows-Systemkonto ausgeführt. Ändern Sie nach Abschluss der Installation den neu erstellten Windows-Dienst in ein Konto mit der geringsten Anzahl von Berechtigungen, die zum Ausführen des MID Servers auf dem Windows-Host erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Computerverwaltung** > **Services und Anwendungen** > **Services**.
2. Klicken Sie mit der rechten Maustaste auf **ServiceNow MID Server**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Popup-Fenster **auf die Registerkarte Anmelden**.
4. Klicken Sie auf das Optionsfeld neben **Dieser Account**.
5. Geben Sie den entsprechenden Benutzernamen und das Passwort des Kontos ein, unter dem der Service ausgeführt werden soll.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster Services mit der rechten Maustaste auf **ServiceNow MID Server**, und klicken Sie dann auf Neu **starten**.
8. Vergewissern Sie sich, dass der MID Server erfolgreich neu gestartet und eine Verbindung zur Instanz hergestellt werden konnte.

Anmeldeinformationen für Windows Discovery und Orchestration

Richten Sie auf den Zielsystemen mit der geringsten Anzahl erforderlicher Berechtigungen ein lokales Windows- oder Active Directory-Konto ein. Es ist möglicherweise nicht erforderlich, Anmeldeinformationen des Domänenadministrators zu verwenden.

Die folgenden Seiten der Produktdokumentation enthalten Anleitungen dazu, welcher Kontotyp verwendet werden soll und welche Berechtigungen erforderlich sind.

- Windows-Anmeldeinformationen
- Windows-Probes und -Berechtigungen
- Microsoft Just Enough Administration (JEA) für Discovery

Anmeldeinformationen für Linux Discovery und Orchestration

Verwenden Sie bei der Erkennung und Orchestrierung ein Nicht-Root-Konto mit eingeschränkten sudo-Berechtigungen auf Linux-Zielsystemen.

Verwenden Sie die folgenden Richtlinien:

- Verwenden Sie für das Linux-Konto eine ausreichende Länge und Komplexität des Passworts. Das Passwort muss aus mindestens 12 Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.
- Bei der Konfiguration von sudo-Berechtigungen können sich die lokalen Pfade zu ausführbaren Binärdateien je nach ausgeführter Linux-Distribution unterscheiden. Weitere Informationen finden Sie unter Berechtigte MID Server-Befehle .

Verschlüsseln Sie die Anmeldeinformationen für den MID-Server

Standardmäßig werden die Anmeldeinformationen für den MID Server in der Datei config.xml verschlüsselt.

Stellen Sie beim Bearbeiten der Datei config.xml und beim Angeben des Passworts sicher, dass das Attribut `encrypt="true"` vorhanden ist, indem Sie die folgende Syntax verwenden:

```
<parameter name="MID.instance.username" value="MIDsrvadmin" />
```

```
<parameter name="MID.instance.password" encrypt="true" value="$ECUREpassw0rd"/>
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Durch die Verschlüsselung von MID Server-Anmeldeinformationen wird kein unsicherer Serverhost durch schlechte physische Sicherheit und Netzwerksicherheit ersetzt. Das in der Datei config.xml gespeicherte Passwort wird beim ersten Start des MID Servers oder, falls es sich um einen vorhandenen MID Server handelt, beim Neustart verschlüsselt.

Legen Sie die Mindestgröße der DH-Gruppe auf 2048 Bit fest

Das National Standard Institute of Technology (NIST) hat die Verwendung des Diffie-Hellman (DH) 1024-Bit-Schlüssels nach dem Jahr 2013 verboten. Legen Sie stattdessen die Mindestgröße der DH-Gruppe auf 2048 Bit fest.

1. Navigieren Sie in der -Instanz zu **MID-Server** > **Server**.
2. Klicken Sie auf den Namen des MID Servers, für den Sie diese Funktionalität deaktivieren möchten.
3. Klicken Sie in der MID Server-Konfiguration auf die Schaltfläche **Neu** neben Konfigurationsparameter.
4. Konfigurieren Sie unter MID Server-Konfigurationsparameter die folgenden Parametereinstellungen:
   - **Parametername** `mid.ssh.dh_group_length_min`
   - **Wert** 2048

Deaktivieren Sie ausgehende SSL

Sie können SSLv2 und SSLv3 im Now Platformdeaktivieren. Durch das Festlegen dieser Eigenschaft wird der MID Server gezwungen, TLS zu verwenden und die erhöhte Sicherheit bei ausgehenden Verbindungen wie REST- und SOAP-Anforderungen zu nutzen.

1. Navigieren Sie in der -Instanz zu **MID-Server** > **Eigenschaften**.
2. Fügen Sie einen Konfigurationsparameter hinzu, und legen Sie seinen Wert wie folgt fest:
   - **Nennen** Sie `glide.outbound.sslv3.disabled`
   - **Wert „** `true`“.

Deaktivieren Sie schwächere Algorithmen

Sie können die schwächeren Algorithmen deaktivieren, sodass Anforderungen an einen nicht TLS 1.2-konformen HTTP-Server dort fehlschlagen, wo sie früher funktionierten.

Bearbeiten Sie die Datei jre/lib/security/java.security im Agent-Ordner mit der folgenden Syntax:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, [other schwache Algorithmen…]
```

Hinweis:
Beachten Sie, dass diese Datei beim Upgrade überschrieben wird. Daher sollten Sie über einen Prozess verfügen, um diese Datei nach jedem Upgrade erneut zu aktualisieren.

PowerShell-Benutzer sollten ihren Windows -Administrator konsultieren, um niedrigere Versionen von TLS zu deaktivieren. Um Details dazu zu erhalten, welche Versionen von TLS in PowerShell verwendet werden, verwenden Sie den Befehl `[enum]::GetNames([Net.SecurityProtocolType])`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Umkehrbares Verhalten

Es gibt Systemeigenschaften, die entweder als „safe_overrides“ oder „no_db_override“ kategorisiert sind.

Sichere Überschreibung

Die Werte für diese Eigenschaften können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden).

Hinweis:
Administratoren können die Eigenschaft „Sichere Überschreibung“ nicht umbenennen oder löschen.

Attribut	Kategorie
Standardmäßig verweigern	Zugriffssteuerung
Aktivieren der AJAXGlideRecord-ACL-Überprüfung	Zugriffssteuerung
Datenschutz für vom Client aufrufbare Skripteinbindungen	Zugriffssteuerung
Vom Client generierte Skripts in der Sandbox	Eingabevalidierung
Überschreibung des Sammlungsmodus (veraltet)	Sicherheitsaufnahmeliste

Keine DB-Überschreibung

Die vorhandenen Werte für diese Eigenschaften können nicht geändert oder überschrieben werden.

Attribut	Kategorie
Aktivieren Sie Einschränkungen beim Dateidownload	Anlagen

Veraltete Sicherheitseigenschaften

Diese Sicherheitseigenschaften waren in früheren Releases veraltet.

Überschreibung des Sammlungsmodus (veraltet)

Die Eigenschaft `glide.whitelist.manager.collection_mode.override` wurde entwickelt, um die Abwärtskompatibilität für stark angepasste Instanzen zu gewährleisten. Es wurden Paketaufrufe verwendet, die in einer Version vor Calgary erstellt wurden, und sind seitdem veraltet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.whitelist.manager.collection_mode.override
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Durch Deaktivieren der Eigenschaft „Sammlungsmodus“ wird die Sicherheitslücke geschlossen, die beim Importieren von Java-Paketaufrufen in eine Instanz vorhanden ist.
Empfohlener Wert	false
Funktionale Auswirkung	(Niedrig) Es sollte keine Auswirkungen geben, solange die Ergebnisse aus Abschnitt 10.6 überprüft und genehmigt werden. Um sicherzustellen, dass die Instanz ordnungsgemäß funktioniert, testen Sie die Änderungen in einer Nicht-Produktionsumgebung, bevor Sie sie in der Produktionsumgebung bereitstellen
Sicherheitsrisiko	(Hoch) Clientseitige API-Aufrufe, die zum Datenabruf oder Objektzugriff auf dem Server führen, gelten aus Sicherheitsgründen als gefährlich. Validieren Sie sie auf Autorisierung und Einschränkung für den Zugriff auf vertrauliche Objekte.
Referenzen	https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483

SMTP-Authentifizierung (veraltet)

Die Eigenschaft `glide.smtp.auth` gibt an, ob für einen SMTP-Server Benutzernamen- und Passwortauthentifizierungseinträge erforderlich sein sollen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.smtp.auth
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Erzwingt die SMTP-Authentifizierung
Empfohlener Wert	Wahr
Funktionale Auswirkung	(Hoch) Diese Fehlerkorrektur erzwingt die Authentifizierung beim externen E-Mail-Server, bevor der Inhalt in Form einer E-Mail übermittelt wird. Wenn die Automatisierung für die Bereitstellung von E-Mail-Inhalten eingerichtet ist, kann dies Auswirkungen haben, bis Sie die Eigenschaft festlegen und einen relevanten Benutzernamen/ein relevantes Passwort für den E-Mail-Serverzugriff angeben.
Sicherheitsrisiko	(Niedrig) Aktivieren Sie die SMTP-Authentifizierung, bevor der Inhalt an den externen E-Mail-Server gesendet wird. Die Authentifizierung sollte immer erfolgen, bevor Transaktionen an/von der Instanz stattfinden.
Referenzen	E-Mail-Eigenschaften

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden der JavaScript-Inhaltszugriffssteuerung

Wenn Sie ein Upgrade-Kunde sind, können Sie die JavaScript-Inhaltszugriffssteuerung verwenden, um die Liste der blockierten JavaScript-URLs von Drittanbietern in Ihrer Instanz zu ändern.

Vorbereitungen

Wenn Sie ein Upgrade-Kunde sind, haben Sie Lese- und Schreibzugriff auf die Tabelle.

Wenn Sie ein neuer Kunde sind, werden alle Datensätze ausgeblendet. Wenden Sie sich an den Support von ServiceNow®, um Unterstützung zu erhalten.

Erforderliche Rolle: admin

Prozedur

1. Suchen Sie im Anwendungsnavigator nach `sys_js_content_provider_rule.list`.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Regel für JavaScript-Inhaltsanbieter

Feld	Beschreibung
Aktiv	Option, bei der die Regel aktiv wird, wenn sie ausgewählt wird. Wenn diese Option deaktiviert ist und keine anderen Regeln übereinstimmen, wird die **Pfad** -URL zugelassen.
Pfad	Absolute URL zu einer JavaScript-Datei. **Hinweis:** Jeder Pfad hat vier Variationen. Zum Beispiel blockiert der Pfad `/scripts/lib/jquery/jquery-1.8.2.min.js` die folgenden URLs: ○ /scripts/lib/jquery/jquery-1.8.2.min.js ○ /scripts/lib/jquery/jquery-1.8.2.min.jsx ○ /lib/jquery/jquery-1.8.2.min.js ○ /lib/jquery/jquery-1.8.2.min.jsx
Aktion	Option zu ○ **Verweigern**: Der Server gibt die Antwort **404 Nicht gefunden** für die **Pfad** -URL oder eine ihrer Variationen zurück. ○ **Zulassen**: Der Server gibt den Inhalt der Datei für die **Pfad** -URL oder eine ihrer Variationen zurück. ○ **Umleiten**: Der Server gibt den Inhalt einer alternativen Datei zurück, wie im Feld Umleitungspfad angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Option, die den Umfang der Regel angibt. **Global** ist die Standardeinstellung. **Hinweis:** Diese Funktionalität ist nicht bereichs-/anwendungs- oder domänenabhängig.
Umleitungspfad	Feld, das den Pfad für die Umleitung angibt. Wenn **Aktion** auf **Umleiten**festgelegt ist, wird einer Anforderung für die **Pfad** -URL stattdessen der Inhalt von dieser URL zugestellt.

4. Klicken Sie auf **Absenden**.

Andere Sicherheitshärtungsressourcen

Im Folgenden finden Sie zusätzliche Informationsquellen zur Härtung von Sicherheitskontrollen im Zusammenhang mit Now Platform.

Ressource	Beschreibung
Sicherheitstestportal	Sicherheitsservices-Portfolio auf HI
KB0538598	Penetrationstests für Kundenanwendungen | Richtlinie und Verfahren
KB0546756	Deaktivieren des Zugriffs auf das öffentliche Content Management System (CMS).
KB0550071	ServiceNow, Inc. Überprüfung der Instanzzugriffskontrolle
KB0550613	IP-Adressbeschränkungen erkennen und aktivieren
KB0550828	Audit und Überprüfung von GlideAjax-Transaktionen
KB0550837	Skript-Sandboxing-Korrektur
KB0551031	Sicherheitskorrektur für die Passwortzurücksetzungs-UI
KB0552835	Fehlerkorrektur für Demo-Benutzerkonten
KB0529232	ServiceNow, Inc. Monitoring – Übersicht und Einblick
KB0564232	Verwenden der Mobile-App ServiceNow, Inc. mit externer Authentifizierung
Sicherheit und Risiko	ServiceNow, Inc. Community

ServiceNow®-Zugriffssteuerung

Mit dem Plugin „SNC Access Control“ (com.snc.snc_access_control) können Sie steuern, welche Kundenservice und Support Mitarbeiter wann auf Ihre Instanz zugreifen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie die ServiceNow-Zugriffssteuerung

Erfahren Sie mehr über die Funktionen der Zugriffssteuerung ServiceNow®.

Aktivieren Sie die ServiceNow-Zugriffssteuerung

Aktive ServiceNow® Zugriffssteuerung.

Konfigurieren Sie die ServiceNow-Zugriffssteuerung

Machen Sie sich damit vertraut, wie die Zugriffssteuerung ServiceNow® konfiguriert wird.

Audit-Protokollierung

Lernen und überprüfen Sie die Audit-Protokollierung der ServiceNow® Zugriffskontrolle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow® Zugriffssteuerung erkunden

Mit dem Plugin „SNC Access Control“ (com.snc.snc_access_control) können Sie steuern, welche Kundenservice und Support Mitarbeiter wann auf Ihre Instanz zugreifen können.

Wenn Sie das Plugin zum ersten Mal aktivieren, können sich Kundenservice und Support Mitarbeiter nicht bei der Instanz anmelden. Alle derzeit angemeldeten Kundenservice und Support Mitarbeiter bleiben angemeldet. Sie erstellen Datensätze in der SNC-Zugriffssteuerungstabelle, die bestimmten SNC-Mitarbeitern oder allen Mitarbeitern Zugriff gewähren.

Das Plugin verhindert, dass Mitarbeiter von Kundenservice und Support ohne Ihre ausdrückliche Genehmigung auf die Instanzen zugreifen. Andere autorisierte ServiceNow Betriebsmitarbeiter müssen jedoch in ihrer Kapazität für den Support und die Verwaltung des Produkts und die Überprüfung der Nutzung administrative Aktionen für die zugrunde liegende Infrastruktur durchführen. Diese Infrastruktur umfasst Server und Datenbanken sowie andere Infrastrukturkomponenten, aus denen die SaaS-Lösung besteht. Diese Zugriffsmethode ist vollständig überprüfbar und nachverfolgt.

Mit diesem Plugin können Sie den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Genehmigung einschränken, sodass sich dies auf die Servicelevel des Supports und die Verfügbarkeits-SLA auswirken kann. Die Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeitern Zugriff auf Ihre Instanz gewährt wird.

Anmeldesicherheit

Die Sicherheit für autorisierte Kundenservice und Support Mitarbeiteranmeldungen bei -Instanzen verwendet verschlüsselte Token, die von einem sicheren Server generiert werden. Nur ordnungsgemäß authentifizierte Kundenservice und Support Mitarbeiter erhalten Zugriff auf eine Instanz. Ohne das Plugin „SNC Access Control“ stellt der Sicherheitsserver sicher, dass Zugriffsrechte für hi.service-now.com erzwungen werden. Wenn das Plugin aktiviert ist, müssen die verschlüsselten Anmeldetoken mit den Namen in der vom Plugin bereitgestellten Zugriffsliste übereinstimmen, wobei die in diesen Datensätzen definierten Kriterien verwendet werden. Mit dieser Methode der Authentifizierung können Sie genau bestimmen, welche Kundenservice und Support Mitarbeiter auf ihre Instanzen zugreifen dürfen und wann diese Mitarbeiter dies tun dürfen.

Die für dieses System ausgewählte Architektur verfügt über mehrere Funktionen, die die Sicherheit für Ihre Instanzen verbessern sollen:

Sicherheitsserver

Der Sicherheitsserver ist ein gesperrter Linux-Host, auf den nur ServiceNow Sicherheitspersonal zugreifen kann. Dieser Server ist das einzige System, das Zugriff auf den kritischen privaten Verschlüsselungsschlüssel hat, der zum Erstellen der Anmeldetoken erforderlich ist. Durch diese Aufteilung (eine standardmäßige Sicherheitspraxis) wird der private Schlüssel auch für den unwahrscheinlichen Fall geschützt, dass ein Angreifer die HI-Instanz gefährdet.

Synthetic-Benutzer

Die Funktion in Instanzen, die es autorisierten Kundenservice und Support Mitarbeitern ermöglicht, sich bei ihrer Instanz anzumelden, erfordert keine Bereitstellung eines -Kontos in dieser Instanz. Es wird kein Benutzerdatensatz bereitgestellt, und es werden keine permanenten oder persistenten Anmeldeinformationen bereitgestellt. Stattdessen wird für jede Kundenservice und Support Mitarbeiteranmeldung ein künstlicher Benutzer erstellt. Dieser Benutzer ist nur im Arbeitsspeicher vorhanden und bietet keine dauerhaften Berechtigungen. Wenn das Plugin „SNC Access Control“ aktiviert ist, können Sie die Autorisierung eines Kundenservice und Support Mitarbeiters jederzeit aufheben.

Token

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Sicherheitstoken sind spezifisch für eine Instanz und einen bestimmten Kundenservice und Support Mitarbeiter. Darüber hinaus funktioniert der Mechanismus, der die Token generiert, nur bei tatsächlichen Kundenservice und Support Mitarbeiteranmeldungen bei HI, nicht bei Benutzern, deren Identität angenommen wird. Sobald ein Sicherheitstoken generiert wurde, kann sich nur ein bestimmter Kundenservice und Support Mitarbeiter damit bei einer Instanz anmelden.

Zeitbegrenzung

Sicherheitstoken laufen vier Stunden nach ihrer Generierung ab. Dieser Ablauf schränkt den Nutzen von gekaperten Token ein, die nur während dieses kurzen Zeitfensters verwendet werden können.

Protokollierung

Anmeldungen von Kundenservice und Support Mitarbeitern bei -Instanzen werden als Anmeldeereignis aufgezeichnet.

- Jede Aktion des angemeldeten Mitarbeiters Kundenservice und Support wird dem Transaktionsprotokoll in der -Datenbank hinzugefügt.
- Sie wird auch dem Instanzprotokoll im Dateisystem hinzugefügt, auf das die meisten Mitarbeiter von ServiceNow nicht zugreifen können.
- Kundenservice und Support Mitarbeiteranmeldungen und -aktionen sind leicht erkennbar, da die Benutzernamen alle auf @snc enden (z. B. frodo.baggins@snc).

Diese Aktionen bieten Ihnen eine benutzerfreundliche, robuste und zuverlässige Sicherheitsprotokollierung für den Zugriff durch Nicht-Mitarbeiter.

Sicherheitsverarbeitungs-Flow

Wenn sich ein Kundenservice und Support -Mitarbeiter bei einer -Instanz anmelden möchte, sieht der Sicherheitsverarbeitungs-Flow wie folgt aus:

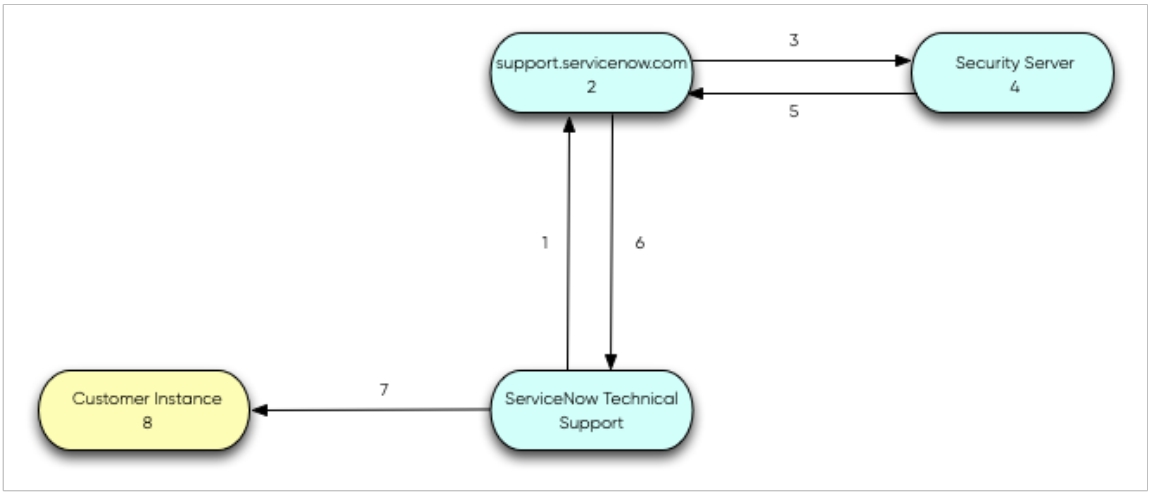
1. Ein Kundenservice und Support -Techniker fordert eine Anmeldung für die Instanz über hi.service-now.com an.
2. HI überprüft, ob der Techniker über die richtige Rolle verfügt, die den Zugriff auf Instanzen autorisiert.
3. Wenn der Benutzer über die richtige Rolle verfügt, sendet HI die Zugriffsanforderung an den Sicherheitsserver.
4. Der Sicherheitsserver überprüft, ob die Anforderung von der HI-IP-Adresse stammt, und wertet die Anforderung aus (Benutzer, Rolle und IP-Adresse der anfordernden Person). Wenn die Anforderung gültig ist, genehmigt sie der Sicherheitsserver und erstellt ein Token. Dieses Token enthält den Benutzernamen, die Rollen, die Instanz-ID und die Uhrzeit (Beginn der vierstündigen Lebensdauer des Tokens). Schließlich verschlüsselt der Sicherheitsserver das Token mit dem privaten Verschlüsselungsschlüssel.
5. Der Sicherheitsserver sendet das verschlüsselte Token an HI.
6. Hi sendet das Token an den Browser des Support-Technikers.
7. Der Browser des Support-Technikers initiiert eine Anmeldung bei der Instanz mit dem speziellen Benutzernamen, der auf @sncendet.
8. Die Instanz verwendet den öffentlichen Schlüssel, um das Token zu entschlüsseln. Um das Token zu überprüfen, gleicht die Instanz es mit dem im vorherigen Schritt angegebenen Benutzernamen, der Instanz-ID und dem autorisierten Zeitfenster ab. Wenn das Plugin „SNC Access Control“ aktiviert ist, überprüft die Instanz, ob der Benutzer:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aufgeführt
- Aktiv
- Konfiguriert für den Zugriff auf die Instanz im aktuellen Zeitfenster

9. Wenn der Benutzer authentifiziert ist, erstellt die Instanz im Speicher einen *künstlichen Benutzer* mit den angegebenen Rollen. Dieser Benutzer bleibt nicht erhalten, nachdem das Zeitlimit abgelaufen ist, sich der Benutzer abmeldet oder die Instanz neu gestartet wurde.

ServiceNow Prozess-Flow für Sicherheitszugriff



Audit-Protokollierung

Mit der folgenden Protokollierung werden Anmeldungen und Aktivitäten von Kundenservice und Support Mitarbeitern nachverfolgt:

- Ereignisprotokolle: Die Ereignisprotokolle zeigen alle Kundenservice und Support Anmeldungen bei einer Instanz.
- Transaktionsprotokolle: Die Transaktionsprotokolle zeigen alle Aktivitäten in der Instanz, einschließlich aller Löschversuche.

Hinweis:
Weitere Informationen zu diesem Plugin finden Sie unter Plugin „SNC Access Control“. in den Härtungseinstellungen für die Instanzsicherheit.

ServiceNow® Zugriffssteuerung wird aktiviert

Sie fordern die Aktivierung des Plugins „SNC Access Control“ (com.snc.snc_access_control) an.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Es gibt zwei Möglichkeiten, ein Plugin anzufordern:

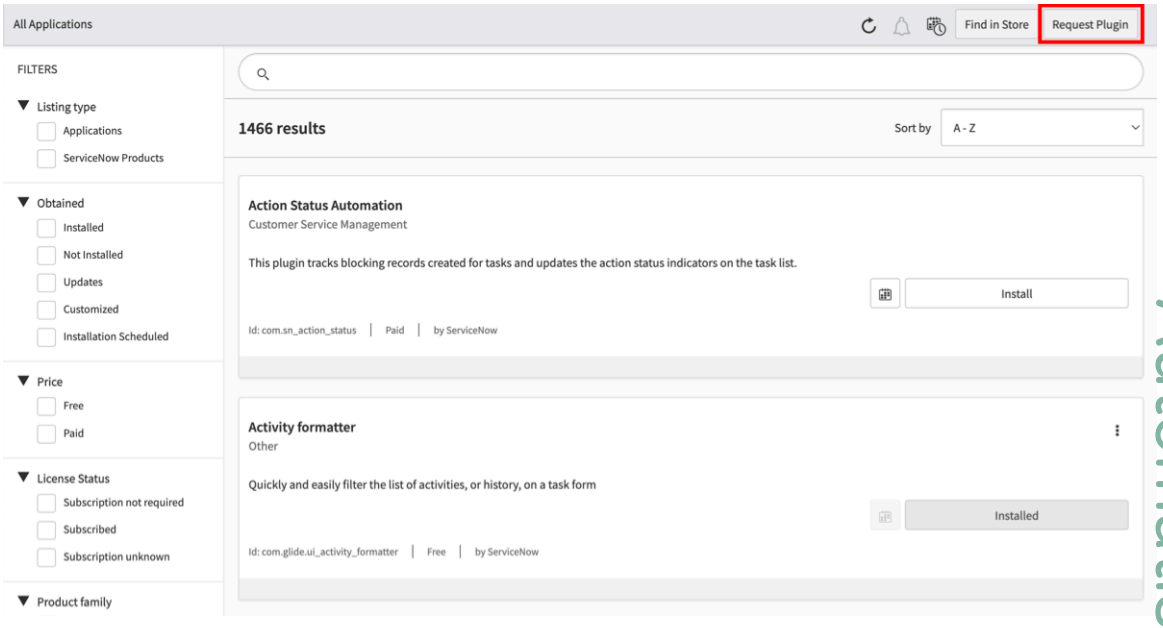
- Greifen Sie direkt auf den Servicekatalog Now Support zu, indem Sie auswählen **Alle** > **Servicekatalog** > **Plugin aktivieren** auf Now Support.
- Greifen Sie über die Seite „Alle Anwendungen“ in Ihrer Instanz auf den Now Support-Servicekatalog zu, indem Sie die folgenden Schritte ausführen.

Automatische Übersetzung

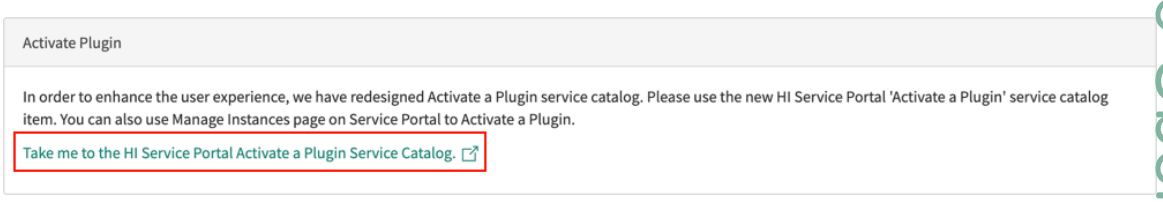
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins

Automatische Übersetzung

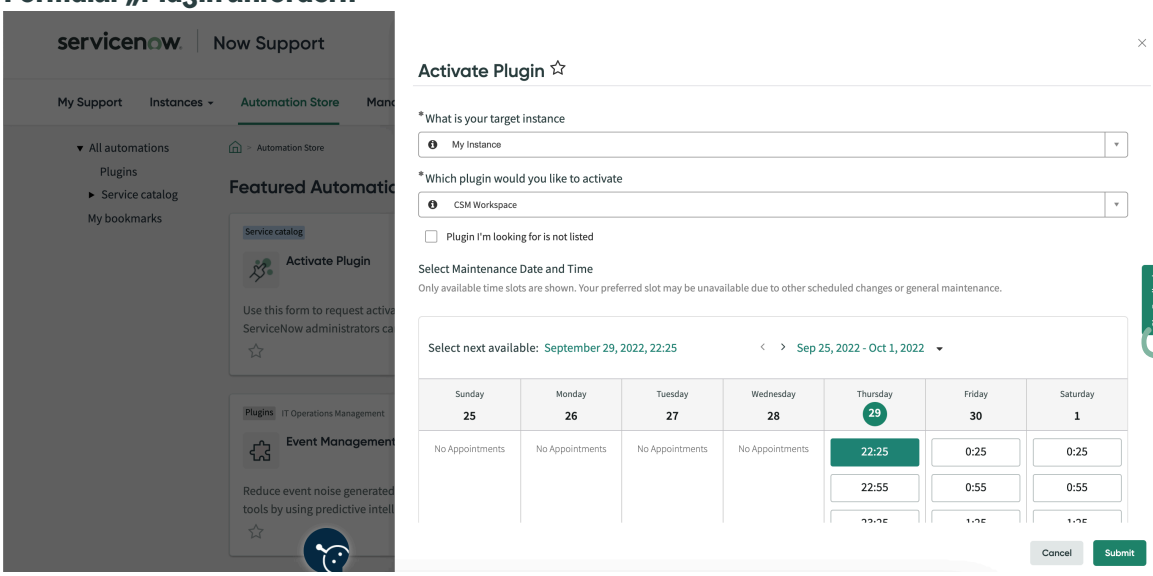
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Plugins aus dem Servicekatalog anfordern [KB0751715] im Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow® Zugriffssteuerung konfigurieren

Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere Kundenservice und Support Mitarbeiter anzugeben, die berechtigt sind, sich bei Ihrer Instanz anzumelden.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:

Das Plugin „SNC Access Control“ (com.snc.snc_access_control) verhindert, dass Mitarbeiter von Kundenservice und Support ohne Ihre ausdrückliche Genehmigung auf die Instanzen zugreifen. Andere autorisierte ServiceNow Betriebsmitarbeiter müssen jedoch in ihrer Kapazität für den Support und die Verwaltung des Produkts administrative Aktionen für die zugrunde liegende Infrastruktur durchführen. Diese Infrastruktur umfasst Server und Datenbanken sowie andere Infrastrukturkomponenten, aus denen die SaaS-Lösung besteht. Diese Zugriffsmethode ist vollständig überprüfbar und nachverfolgt.

Mit diesem Plugin können Sie den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Genehmigung einschränken, sodass sich dies auf die Servicelevel des Supports und die Verfügbarkeits-SLA auswirken kann. Die Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeitern Zugriff auf Ihre Instanz gewährt wird.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **SNC-Zugriffssteuerung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.

SNC-Zugriffssteuerung

Formularfelder	Beschreibung
Name	Benennt jeden Kundenservice und Support Mitarbeiter, der berechtigt ist, sich bei dieser Instanz anzumelden. ○ Drücken Sie die Namen als firstname.lastname in Kleinbuchstaben aus, getrennt durch einen Punkt (z. B. john.smith). Jeder Name muss einen entsprechenden Benutzerdatensatz in *support.servicenow.com*haben. ○ Wenn mehr als ein Kundenservice und Support Mitarbeiter berechtigt ist, sich bei dieser Instanz anzumelden, geben Sie mehrere Namen ein, und trennen Sie sie durch Kommas. ○ Um allen Kundenservice und Support Mitarbeitern Anmelderechte für den Zugriff auf die Instanz zu gewähren, geben Sie anstelle des Namens ein Sternchen (*) ein. ○ Wenn Sie den Zugriff von Mitarbeitern Kundenservice und Support auf die Instanz einschränken möchten, dürfen die Werte im Feld **Name** kein Sternchen (*) enthalten.
Grund	Visuell lesbares Feld, das beschreibt, warum Sie die Zugriffsberechtigung erteilen. Dieses Feld ist optional.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder	Beschreibung
Starten	Gibt das Startdatum und die Startzeit des Zeitraums an, in dem die angegebenen Kundenservice und Support Mitarbeiter Anmeldezugriff haben. Dieses Feld ist ein Pflichtfeld.
Ende	Gibt das Enddatum und die Endzeit des Zeitraums an, in dem die angegebenen Kundenservice und Support Mitarbeiter Anmeldezugriff haben. Dieses Feld ist ein Pflichtfeld.
Aktiv	Steuert, ob dieser Berechtigungsdatensatz aktiv ist. Der Standardwert ist Aktiv.

Audit-Protokollierung

Die folgende Protokollierung verfolgt Anmeldungen und Aktivitäten von ServiceNow Mitarbeitern.

Ereignisprotokolle	Die Event-Protokolle zeigen alle ServiceNow Anmeldungen bei einer Kundeninstanz.
Transaktionsprotokolle	Die Transaktionsprotokolle zeigen alle Aktivitäten in der Instanz, einschließlich aller Versuche zum Löschen von Protokollen.

Virtuelles privates Netzwerk (VPN)

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Erkunden

Lernen Sie die Funktionen und Geschäftsvorteile von Virtual Private Network kennen.

Aktivieren

Aktivieren Sie das virtuelle private Netzwerk.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren

Machen Sie sich damit vertraut, wie Sie ein virtuelles privates Netzwerk konfigurieren.

Virtual Private Network (VPN) erkunden

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Meine IP-Informationen

Bei der Konfiguration einer Integration, die ein verschlüsseltes Protokoll verwendet, z. B. Lightweight Directory Access Protocol (LDAP) oder HTTPS, empfiehlt es sich, das Internet als Transportmechanismus zu verwenden.

Es können jedoch Sicherheits- oder Netzwerkarchitekturanforderungen bestehen, die die Verwendung einer Site-to-Site-IPSEC-VPN-Verbindung (Virtual Private Network) zwischen den Rechenzentren und Ihren Geschäftsnetzwerken vorschreiben. Das VPN unterstützt die erforderliche verschlüsselte Kommunikation zwischen der Instanz und Ihrem Netzwerk.

VPN-Verbindungen

Die ServiceNow VPN-Infrastruktur verwendet Paare von ASA-Geräten (Adaptive Security Appliance) von Cisco, die als VPN-Beendigungspunkte dienen.

Das VPN zwischen der Instanz und Ihrem Netzwerk nutzt Ihre vorhandene Netzwerkhardware, um die Kommunikation zu unterstützen. Es ist nicht erforderlich, Hardware zu installieren. Da jeder Kunde eine eindeutige Konfiguration hat, verfügt die Instanz über eine flexible VPN-Lösung. Die Instanz hat Tunnel zu Checkpoint-, Juniper-, Normal- und anderen IPSEC-VPN-fähigen Geräten erstellt.

Die VPN-Verbindungen zwischen der -Instanz und Ihrem Netzwerk werden erstellt, um den verschlüsselten Datenverkehr in Ihr Netzwerk zu unterstützen. Integrationen, die das VPN verwenden, weisen häufig keine Verschlüsselung als Teil des zugrunde liegenden Protokolls

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf. Zum Beispiel LDAP über das VPN im Vergleich zu LDAPS über das Internet und HTTP über das VPN im Vergleich zu HTTPS über das Internet.

Das Netzwerk lässt keinen eingehenden Datenverkehr zur ServiceNow-Integration oder Endbenutzer-zu-ServiceNow-Datenverkehr über eine VPN-Verbindung zu. Diese eingeschränkte Kommunikation umfasst den Endbenutzerzugriff auf die Plattform, die Verwaltung der Plattform, Webservices-Integrationen und andere Integrationen, die für die Verwendung eines MID Servers konfiguriert sind. Die gesamte eingehende Kommunikation an die Instanz muss über das Internet mit HTTPS erfolgen. Diese Konfiguration stellt einen verschlüsselten Kommunikationskanal bereit. Der Verschlüsselungskanal erfüllt zusammen mit der IP-Zugriffssteuerung die Sicherheitsanforderungen für diesen Datenverkehrsfluss.

Adressen für die VPN-Kommunikation

Um Konflikte oder Überschneidungen mit internen ServiceNow -Netzwerken oder mit anderen internen IP-Adressschemas in Ihrem Netzwerk zu vermeiden, muss der gesamte Datenverkehr in der Verschlüsselungsdomäne Nicht-RFC-1918-Adressen auf beiden Seiten des Tunnels verwenden.

ServiceNow stellt eine einzelne IP-Adresse für die Quelle von Abfragen in Ihrem Netzwerk bereit. Sie müssen NAT-Nicht-RFC-1918-Adressen (Network Address Translation) für jeden Host angeben, der in Ihre Instanz integriert wird. Diese öffentlichen Adressen müssen Ihrer Organisation gehören. Drittparteiadressen können nicht in Tunneln verwendet werden. Darüber hinaus darf die Verschlüsselungsdomäne nicht die IP-Adresse des VPN-Peers enthalten.

Redundante Tunnel

Es gibt zwei Möglichkeiten, Redundanz für Ihre Tunnel zu erstellen:

- Verwenden derselben Verschlüsselungsdomäne hinter beiden Peers. Dies ist die bevorzugte Methode.
- Verwenden einer anderen Verschlüsselungsdomäne hinter jedem Peer.

Bei der ersten Methode müssen Sie hinter jedem Ihrer Peers dieselbe NAT-Adresse angeben, um einen Verbindungspfad mit dieser Adresse zu Ihrem Server zu erstellen. Der Pfad zu Ihrem Server kann derselbe physische Computer oder ein Spiegel sein, der identische Services bereitstellt. Mit dieser Methode verwendet Ihre Instanz dieselbe IP-Adresse, um eine Verbindung zu Ihren Servern herzustellen, unabhängig davon, ob Ihr primärer oder sekundärer Tunnel aktiv ist. Wenn Sie mehr als einen Server haben, folgen Sie demselben Schema für weitere Server. Diese Methode bietet Ihren Benutzern die meiste Transparenz und wird empfohlen.

Die zweite Methode erfordert eine Konfiguration in Ihrer Instanz, um die Redundanz bereitzustellen. Wenn der Tunnel beispielsweise für LDAP verwendet wird, können Sie redundante LDAP-Server in Ihrer Instanz bereitstellen. Beachten Sie, dass diese Methode eine Zeitüberschreitung der Verbindung zum ersten konfigurierten LDAP-Server erfordert, bevor die Instanz versucht, eine Verbindung zum sekundären Server herzustellen. Aufgrund dieser zusätzlichen Zeitverzögerung sollte diese Lösung nur implementiert werden, wenn die erste Option nicht erreichbar ist. Beachten Sie auch, dass nicht alle Services in Ihrer Instanz redundant für konfiguriert werden können. Wenn Sie einen VPN-Tunnel für etwas anderes als LDAP verwenden und Redundanz erforderlich ist, überprüfen Sie, ob Ihre Konfiguration mehrere Adressen unterstützt, oder sehen Sie sich die erste Option oben an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alternativen zur Verwendung eines VPN

Diese Alternativen bieten eine einfachere Möglichkeit, Ihre Instanz mit den Ressourcen in den ServiceNow -Rechenzentren zu verbinden, und bieten eine bessere Verschlüsselung. Darüber hinaus können Sie Probleme vermeiden, die durch VPN-Ausfallzeiten verursacht werden können, z. B. wenn Ihre Instanz bei einem Problem mit dem VPN-Tunnel für Benutzer nicht verfügbar ist.

Single Sign-on und MID-Server

Erwägen Sie die Verwendung einer Kombination aus Single Sign-on (SSO) für die Authentifizierung und dem MID Server für die Synchronisierung von Benutzerdaten, anstatt ein VPN zu verwenden, um Ihren LDAP-Server mit Ihrer Instanz zu verbinden. Erwägen Sie für andere Integrationen als LDAP die Verwendung der zertifikatsbasierten Verschlüsselung.

Sie können den LDAP-Listener auf einem MID-Server verwenden, um Ihre Benutzertabelle nahezu in Echtzeit zu synchronisieren.

Der Vorteil dieses Ansatzes besteht darin, dass keine Firewall-Lücken, Routen, VPN-Tunnel oder andere spezielle Netzwerkeinstellungen konfiguriert und verwaltet werden müssen. Die SSO/MID-Server-Lösung ist die flexibelste, sicherste und kosteneffektivste Methode, um eine vollständige LDAP-Integration zu erreichen.

LDAP über SSL

Eine weitere Alternative zur Verwendung eines VPN-Tunnels besteht in der Konfiguration von LDAP Over SSL (LDAPS) direkt über das Internet. Sie können einen schreibgeschützten Domänencontroller konfigurieren und die Instanz in Ihrer DMZ sperren, indem Sie nur die Quelladressen der Instanz und die Zielports Ihrer Wahl verwenden. Da die Ports für LDAP in Ihrer Instanz konfigurierbar sind, können Sie bei Bedarf eine Portadressübersetzung (Port Address Translation, PAT) durchführen. Mit LDAPS steuern Sie das Zertifikat, das über einen verschlüsselten Kanal in die Instanz hochgeladen wird (siehe Ein Zertifikat wird in eine Instanz hochgeladen). Die Pakete können ohne das Zertifikat nicht verschlüsselt oder entschlüsselt werden.

Der Vorteil dieses Ansatzes besteht darin, dass er einen stärkeren Verschlüsselungs- und Entschlüsselungsmechanismus bietet. Ein VPN kann den Datenverkehr zwischen den beiden Partnern im Internet nur mit einem koordinierten vorinstallierten Schlüssel verschlüsseln und entschlüsseln, ähnlich einem Passwort. LDAPS bietet einen längeren verschlüsselten Pfad (End-to-End) auf Anwendungsebene und mit einem Zertifikat, das weitaus komplizierter ist als ein vorinstallierter Schlüssel, den der IPSec-Tunnel verwendet.

VPN-Setup

Ab dem Zeitpunkt, zu dem eine VPN-Anforderung gesendet wird, dauert es normalerweise maximal eine Woche, bis der VPN-Build abgeschlossen ist. Zur Unterstützung der Redundanzanforderungen Ihrer Instanz und Ihrer Organisation werden mindestens zwei und maximal vier VPNs bereitgestellt (vom aktiven Standort zu Ihrem aktiven Standort oder vom aktiven Standort zu Ihrem DR-Standort usw.).

Es wird empfohlen, die Verschlüsselungsdomäne so spezifisch wie möglich zu gestalten. Idealerweise enthält die Verschlüsselungsdomäne nur die spezifischen Hosts, die für die Integrationen erforderlich sind. Eine große Verschlüsselungsdomäne kann Möglichkeiten für Routing-Diskrepanzen schaffen (VPN vs. Internet).

Um das VPN zu erstellen, führt die Instanz folgende Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Stellt die VPN-Peer- und Hostadressen aus jedem Rechenzentrum bereit.
2. Erstellt die erforderliche VPN-Konnektivität von zwei Rechenzentren in Ihrem Netzwerk. Zur Unterstützung der Redundanz- und Notfallwiederherstellungsanforderungen (Disaster Recovery, DR) können die VPNs von zwei Rechenzentren in zwei Netzwerken bereitgestellt werden.

Die Instanz unterstützt nicht den Aufbau mehrerer VPN-Tunnel in einem Kundennetzwerk, um eine Verbindung zu mehreren geografischen Regionen oder Tochterunternehmen herzustellen. Sie sollten standortübergreifendes Routing, Datenverkehrsverteilung oder Datenverkehrsformung in Ihrem eigenen internen Netzwerk durchführen, anstatt über mehrere VPN-Tunnel zu verfügen.

Aktivieren eines VPN-Service

Verwenden Sie für alle VPN-Anforderungen, einschließlich Bereitstellung, Änderungen oder allgemeine Fragen, das VPN-Anforderungsformular des Servicekatalogs.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu https://support.servicenow.com/now?draw=case.
2. Wählen Sie die Registerkarte **Automation Store** aus.
3. Verwenden Sie die Struktur auf der linken Seite, um zu zu navigieren **Alle Automatisierungen** > **Servicekatalog** > **Cloud-Infrastruktur**.
4. Wählen Sie **VPN-Anforderungen aus**
5. Wählen Sie den entsprechenden VPN-Anforderungstyp aus.
6. Beantworten Sie die Fragen.
   Die Fragen variieren je nach ausgewähltem Anforderungstyp.
7. Klicken Sie auf **Absenden**.

Ergebnisse
Sobald Ihre Anforderung übermittelt wurde, arbeitet ServiceNow mit Ihren Netzwerktechnikern zusammen, um zu testen und zu validieren, ob der Datenverkehr vom VPN erfolgreich weitergeleitet wird. Um sicherzustellen, dass Ihre Fragen zeitnah beantwortet werden, gehen Sie während dieses Prozesses auf VPN-bezogene Fragen ein.

Adresse für die VPN-Kommunikation konfigurieren

Um Konflikte oder Überschneidungen mit internen ServiceNow -Netzwerken oder internen IP-Adressschemata eines anderen Kunden zu vermeiden, erfordert die Instanz, dass der gesamte Datenverkehr in der Verschlüsselungsdomäne Nicht-RFC-1918-Adressen auf beiden Seiten des Tunnels verwendet.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Instanz stellt eine einzelne IP-Adresse für die Quelle von Abfragen in Ihrem Netzwerk bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Geben Sie NAT-Adressen (Network Address Translation) (Nicht-RFC-1918-Adressen) für jeden Host an, der in die Instanz integriert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.