servicenow

ServiceNow Security Best Practice Guide

Key considerations for securing your instance

servicenow

Table of contents

servicenow

Introduction

As a new customer of ServiceNow, you will be keen to get started with the Now Platform® and use its capabilities to enhance your organization's business processes. The ServiceNow infrastructure and Now Platform are intentionally built and operated with high levels of baseline security; however, as a customer you must make some decisions about the way in which your instance is configured to comply with your organization's security policies. You may have examined the security of the Now Platform during the procurement cycle, but now you need to know how to go about actually securing your instance and your data.

This document gives guidance on some of the main areas which should be considered, links to comprehensive resources, and best practice recommendations for each topic. You can ensure your instance has a good security foundation by understanding and acting on the recommendations in this guide.

Some customers may require assistance in addressing some of the content in this guide, due to resource or skills constraints. ServiceNow has introduced the TuneUp your Security service to help address this. You can find out more by watching this webinar.

Overall security responsibilities

ServiceNow provides its customers with extensive capabilities to configure their instances to meet their own security policies and requirements. The partnership of customer, ServiceNow, and colocation data center provider enables coverage across the entire application and infrastructure stack. The areas of responsibility are shown in the table below.

Responsibility	Owner		
	Customer	ServiceNow	Colocation Provider
Customer data management (classification and retention)	●		
Media disposal and destruction		●	
Backup and restore		●	
Authentication and authorization	●		
Data encryption at rest	●		
Encryption key management	●	●	
Security logging and monitoring	●	●	
Vulnerability management	●	●	
Business continuity and disaster recovery		●	
Secure SDLC processes	●	●	
Penetration testing	●	●	
Privacy	●	●	
Compliance: regulatory and legal	●	●	●

Infrastructure management		●	
Security management		●	
Secure configuration of instance	●		
Employee vetting or screening	●	●	●
Environment controls		●	●
Physical security		●	●

More details of ServiceNow's security program are available in the ServiceNow Assurance Pack (SNAP), which covers specifics of compliance, data security, technical controls, and other topics. This is available on CORE, the compliance area of our community site. Registration is required to access these resources.

Certifications and accreditations

ServiceNow provides highly resilient and secure cloud-based services to customers all over the world. The security of the infrastructure and data is paramount - a foundational requirement. This has to be demonstrated consistently both to maintain customer trust and for regulatory and compliance reasons. ServiceNow maintains accreditation with many common standards such as those shown in the table below. Further details are available in our Securing the Now Platform eBook.

Certification	Description	Industry	Geography
ISO/IEC 27001:2013	Specifies information security management best practices and controls	All industries	International
ISO/IEC 27017:2015	Implementation of cloud-specific information security controls	All industries	International
ISO/IEC 27018:2014	Securing personally identifiable information (PII) in the cloud	All industries	International
SSAE 18 SOC 1 Type 2 Report	Protecting the confidentiality and privacy of information in the cloud that affects the financial reports of customers	All industries	International
SOC 2 Type 2 Report	Focuses on controls that are relevant to security, availability, processing integrity, confidentiality, or privacy	All industries	International
FedRAMP High JAB ATO	US government-wide program that provides a standardized approach for assessing, monitoring, and authorizing cloud computing products and services	US Federal Government	United States Federal

DoD Impact Level 4	US government baseline for security requirements for cloud service providers that host DoD/IC information	US Department of Defense/Intelligence Community	United States Federal
Privacy Shield Frameworks	Sets out standards regarding the safe transfer of data between the EU/Switzerland and the US	All industries	International
Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3	Certifies the adoption of sound risk management and security practices for cloud companies	All industries	Singapore
ASD IRAP Certified Cloud Service	Helps Australian government agencies effectively engage and consume cloud-based solutions.	Australian Federal Government	Australia
Cloud Computing Compliance Controls Catalog (C5)	Cloud-specific compliance controls catalog developed by the German Federal Office for Information Security (BSI).	All industries	Germany

Securing your ServiceNow instance

There are several topics to consider when securing a ServiceNow instance. Some of these are configuration parameters within the product, and others relate to your own infrastructure and technologies and how they are integrated.

Best Practice: If you make any configuration changes to your instance based on the information provided, we strongly recommend that you first test those changes on a non-production instance.

The rest of this document describes the main areas of concern, along with links to documentation, and suggested points to address.

Security contact details

The ServiceNow Security Office (SSO) occasionally needs to relay security-related information directly to appropriate Information Security contacts within your organization. This could be to inform you of security issues, alerts or details of important software updates, etc.

- Security contacts
    - ServiceNow provides the Now Support portal (formerly HI), from which you can manage your customer account, instance, upgrades, and users. The security contact record within your customer account should be completed as soon as possible with details of at least two appropriate information security personnel. These contacts should be capable of understanding and acting on the information they receive, since it may be critically important.
    - If you specify a distribution list, then you should also add a named individual.

Best Practice: Make sure the security contact details are accurate and always kept up to date, bearing in mind personnel and process changes within your organization.

ServiceNow High Security Plugin

To help you to secure your instance easily and efficiently, we provide the High Security Plugin (HSP). This is a tool for enhancing security management and applying appropriate settings. The plugin enables High Security Settings, and the resulting actions include centralizing critical security settings, creating a distinct security administrator role, a default deny property, and others. The HSP is a simple and effective way of enhancing your instance's security.

- *Automatic activation*: since it is such a powerful way of increasing security, the HSP is installed and enabled by default on all new instances. Older releases may require this to be explicitly activated.
- *Manual activation*: you can request activation for older instances that do not have high security settings enabled by default (including those that have had upgrades from an older version). However, this should not be done without careful testing in a non-production environment, because activation will change some fundamental properties and behaviors.
- *Default deny property*: if high security settings are enabled, you can choose to set a default deny posture, which prevents read, write, create and delete for all tables unless explicit permission is given for a user or role in an ACL rule. See the *Access controls* section later in this document for more details on authorization and ACLs.

Best Practice: Ensure that the High Security Plugin is installed and activated where possible and enable the default deny property.

Instance hardening

To make your instance as secure and resistant to unauthorized access as possible, you will need to examine configuration, coding practices, and wider aspects of the deployment such as integrations or policies.

- Guidance
    - The Instance Hardening Guide describes ways to make your instance more secure and resistant to malicious intrusion. It also provides details of which settings and configurations *must* be applied (mandatory) and *should* be applied where possible (recommended). Some of these settings require an understanding of your particular usage context, which is why they are not enabled by default.
    - The Instance Security Center described below can assist with assessing and working towards compliance with the Instance Hardening Guide.
- Instance Security Center
    - To help you understand your instance's security posture and identify any areas for improvement, we provide the Instance Security Center (formerly Instance Security Dashboard - now deprecated). This evaluates your instance configuration and displays a simple overview and Daily Compliance Score representing your overall security level. This score can be refreshed at any time on the Orlando release or newer by users with an admin role.
    - The Paris release introduces the Auditor which compares your instance's security configuration against a reference configuration and highlights any areas for improvement.
    - The Hardening tile helps you to access and adjust specific security configurations.
    - The ISC also enables you to monitor key metrics to help identify potential security concerns.

  - From the New York Release onwards, the Event Ribbon displays several security metrics such as login types, login failures and security elevations, and also trend information. This information can be very useful for identifying security issues, and you can select which charts to display.
- Secure Coding
  - Development of code or applications on your instance should follow good security practices. The Secure Coding Guide covers several topics in this area and gives recommendations on aspects such as input/output sanitization, session management, secure access and others.

Best Practice: Use the Instance Security Center to assess and monitor the overall security level of your instance. For the New York release onwards, use the Event Ribbon and Top Recommendations guidance to help improve your instance's security posture by addressing any areas that need attention. Refer your ServiceNow developers to the Secure Coding Guide, and ensure they follow the practices outlined within.

Email security

The Now Platform provides multiple capabilities for email security. These include controlling which inbound messages are accepted and from whom, encrypting the transmission of outbound messages, and scanning the contents of any attachments for malicious content. You can choose which of these to enable as appropriate to enforce your security policy.

- Anti-malware and SPAM filtering
  - Malware scanning is performed by ServiceNow Antivirus Protection. If a malicious email or attachment is detected, it is stored within an email quarantine area in your instance for inspection by your security personnel.
  - Additionally, all email inbound to the Now Platform is analyzed for malware and SPAM scoring and the results are reflected in x-headers added to the messages. You can use these as criteria for the Email Filters Plugin to act on if desired.
- Email domain restriction
  - You can control the domains and users your instance can send email to and receive from by using system address filters. These can be customized to your requirements.
  - Your organization may control inbound email with anti-spam technology using Sender Policy Framework (SPF). If so, your email systems need to accept email originating from your ServiceNow instance. This is best achieved by configuring them to dynamically query the ServiceNow SPF records.
  - Another approach is to whitelist the ServiceNow mail server IP addresses if SPF is not an option, but this needs to be monitored as the addresses could be subject to change.
- Monitoring
  - You can monitor email and anti-malware activity in the ISC to highlight potential issues and to guide any corrective actions you may need to take.
- Encryption
  - Your instance has a built-in feature allowing it to send and receive email using opportunistic TLS. If your email server accepts TLS, messages will be transferred over an encrypted session, using TLS 1.2. This greatly enhances the privacy and integrity of messages as they traverse the internet.
- Using your own servers

- For more control over how mail is filtered and received before being ingested by your instance, you may wish to use your own SMTP, POP3, or IMAP servers. This is considered an advanced email configuration, and can optionally use a third-party email infrastructure via OAuth 2.0 email authentication.

Best Practice: Make use of the email filters feature-set to deal with suspect inbound messages, and where possible to limit accepted sender domains. Ideally, you should configure your email systems to accept mail from your instance by using SPF. If you already have a mature email security environment, consider using your own (or third-party) infrastructure to send and receive instance-related email and to benefit from more precise perimeter email control.

Logging and monitoring

Your ServiceNow instance performs detailed logging about various aspects of its operation. These logs are stored within the instance itself, and benefit from the same level of security as other data in the instance. This means application logs cannot be inspected by ServiceNow without your permission. Application and event logs can be a valuable source of security information, and can help highlight suspicious or malicious activity, so it is essential that you monitor these adequately.

- Event log
  - Event logs reveal a lot about system activity, including login events (successful or otherwise), and privilege escalation. You can feed selected activity from the event log to your SIEM (or any syslog server), using the syslog probe. This is enabled via a management, instrumentation, and discovery (MID) server deployed in your network. You can find more information about the MID server later in this document.
- System log
  - System logs contain extensive information about general activity, including configuration changes, system errors, workflows, and inbound/outbound data connections.
- Transaction logs
  - These record all web-browser related activity for an instance and can provide details of every request made. Transaction logs can be very useful for identifying unusual or malicious activity.
- Table auditing and record history
  - You can enable auditing for database tables. Record history is perpetual and allows you to track and view details of any changes made to the data since creation. By default, only the incident, problem, and change tables are tracked. For other tables, auditing needs to be enabled manually.
- Log archival
  - You may wish to transfer log data from the instance to your environment for archival beyond the default 21-day log rotation period. You can use web services requests, the data export feature, or the MID server to achieve this.
- Browser SQL Error Messages
  - Improper web queries can result in error messages from the database engine to be presented in the web browser. Though these can be useful to end users and developers, they can also be used by would-be attackers to glean information about the underlying system or to help guide their attempts to access the system. You can add a system property to disable these messages.

Best Practice: Enable table auditing for important or sensitive data. Monitor important logs to help identify any suspicious or malicious activity. Use the syslog probe to send logs to your SIEM to allow activity monitoring and help identify security events. Transfer log data from the instance for archival and reference. Disable browser SQL messages.

Access control

Every legitimate user must have an associated user account defined within your instance, and their identity must be established before access is granted. User accounts can be created manually or imported by the MID server from an existing directory service, along with groups and memberships.

The most important methods for controlling access to your instance are user authentication to verify identity, and authorization to control access levels and permissions. Some others are discussed here too.

- Authentication
    - Your instance comes with certain built-in accounts such as 'admin', 'ITIL' and 'employee' which are provisioned with default passwords, unique to the instance. These should be changed as soon as possible.
    - You can use several different authentication mechanisms to provide authentication to your instance. Basic or native authentication uses local accounts defined within the instance. SAML 2.0, LDAP, OAuth2.0 and others enable use of external services. Multi-provider SSO allows a combination of single sign-on (SSO) and other authentication methods.
    - When Multi-provider SSO is active, you can configure authentication to require SSO credentials for the main login page. In this case, Side Door access is still available.
    - If you experience a problem or failure of your external authentication system, you can make use of Side Door access which allows users with local account to log in. Though we *advise against it*, it is possible to disable this feature, or to rename the login page. In this case we encourage you to notify customer support of the modified name.
    - SAML 2.0 is often a preferred authentication method as it is very secure and widely used. Most customers will already have some form of SAML identity provider (IdP) such as ADFS, Ping, or others.
    - Third-party multi-factor authentication (MFA) can be integrated with your existing SAML IdP to provide additional login security. When a user logs in to a system with MFA enabled, they must submit an additional one-time verification code along with their user name and password. These one-time codes are usually generated on the user's hardware or software token. MFA provides a high level of security because authentication requires something the user knows (the password) as well something they own (the MFA token or mobile phone).
    - The Now Platform supports direct MFA integration with local accounts and LDAP only. MFA can be enabled for both specified users and specified roles, and configured for east of use, e.g. to exempt recognized devices for a number of hours.
    - You have full control over the password policies enforced for access to your instance. For native or local accounts, you can specify length, complexity, expiration, uniqueness, lockout, etc., and starting with the Orlando release, this can be set in the GUI. To maximize security, encourage the adoption of long passphrases and aim to eliminate the use of simple, 'common' passwords. You can of course retain your

existing policies for any external authentication services you have integrated, such as LDAP, SAML, etc.
    - There are some security-related adjustments to the login page to consider. 'Remember Me' is a feature for caching user login page credentials in a browser. This can present security issues if users access your instance from an insecure endpoint, e.g. from a shared computer. The Instance Hardening Guide recommends disabling this feature.
    - Similarly, default credentials should be removed from the login page, and password-less authentication should be disabled.
    - You can help prevent unauthorized access to your instance by restricting access from IP addresses unrelated to your organization—typically only allowing your gateway or web proxy external addresses. Anyone trying to access the instance from an unauthorized range would be denied. If using this approach, consider where all your users access the instance from, e.g. remote users. From the Paris release, you can now control *outbound as well* as inbound access by IP address.
    - We strongly recommend that you monitor the event log for unusual activity such as high numbers of failed logins, especially within short timeframes. Your instance can create incident tickets or trigger workflows (e.g. notify your security response team) automatically when user-defined criteria and thresholds are met.
    - You can use the Session Management tile in the ISC to view detailed information about all user sessions and lock out any that could present a risk.
    - Configuring account lockout after a number of failed logins within a certain timeframe can help guard against brute force authentication attacks.
    - We provide further guidance on enhancing authentication security in the Defending Your ServiceNow Instance Against Password Spray Attacks knowledgebase article.
- Authorization
    - Once a user has successfully authenticated, access to parts of the instance interface, functions, and the data within it are controlled with access-control lists (ACLs) and role-based access control (RBAC). ACLs use the account ID and associated groups to determine what access should be granted to an object, e.g. read, write, delete, create, etc.
    - Role-based access control rules are ACLs assigned to roles defined within the instance. These might cater to different types of users or various job roles. User accounts and groups are assigned to roles, and permissions are applied to those roles.
    - To provide an extra level of protection, you may want to limit concurrent sessions for the same account or role.
    - If the HSP (described earlier), is enabled, you can choose to set a default deny property, which prevents read, write, create, and delete for all tables unless explicit permission is given for a user or role in an ACL rule.
    - All new instances have the Security Jump Start (ACL Rules) Plugin installed to provide a base level of access security for key system tables.
- File attachments
    - You can place controls on file attachments. Uploads can be restricted by role, file extension, MIME type, or size, to help prevent potentially malicious files being stored and subsequently delivered from your instance. You can also control which file types can be downloaded, including by MIME type, and prevent image access by unauthenticated users.

    - The ServiceNow Antivirus Protection plugin is installed and activated by default. This performs anti-virus (AV) scanning on all attachments.
- Access by ServiceNow employees
    - Generally, there can be no access to your instance by ServiceNow personnel without your authorization. The exception to this is customer support employees assigned to an open case for your organization. Any such access is strictly controlled and monitored, and customers can identify this activity at any time by tracking the occurrence of the identifier *name@snc* in the instance event logs. There is more detail in the Data Access Controls whitepaper, including on controls such as the ServiceNow Access Control plugin (SNAC).
    - You may choose to activate the ServiceNow Access Control plugin to enforce a default deny posture for all users (including ServiceNow employees), except those you specify. Once this is activated, ServiceNow personnel must explicitly request access from you on an ad-hoc and temporary basis.
- Auditing access permissions
    - You can check which users have access to which tables, and to what degree, using the Contextual Security Auditor plugin. This is an interactive tool which evaluates table access permissions and displays them in an easy to understand format. It can be installed by customer support on request.
- Instance identification
    - The way you name and brand your instance can help with security. You may wish to avoid choosing a name for your instance that obviously associates it with your organization, e.g. *acmeinstance* or *mycompanyprod*. You can rename an instance if necessary.
    - In a similar vein, you should carefully consider how you use branding and logos on the login page.

Best Practice: Change the default login credentials. If possible, use SAML authentication, and integrate with MFA. Enforce the use of strong passphrases and restrict access to your instance from unknown IP addresses. Review ServiceNow's guidance on password spray attacks, and also disable password-less authentication. Remove the 'Remember Me' checkbox and default credentials from the login page. Monitor the logs for high numbers of login failures and create alerts accordingly. Enable the default deny table access policy and add granular control with RBAC. Use encryption contexts (discussed later in this document) with RBAC to further enhance data access control. Consider limiting file attachments, uploads and downloads. Consider using the ServiceNow Access Control plugin to control ServiceNow's access to your instance.

MID server security

The ServiceNow MID server is a Java application that runs as a service on one or more servers on your network, which you have designated for that role. The MID server acts as a conduit for any of your infrastructure and services that need to communicate with your instance. These might be internal or external to your network, and could include directory services, logging, or infrastructure management systems.

- Physical security
    - The MID server is a critical piece of infrastructure and may contain sensitive information. As with any other important infrastructure, it should be located within a

secured environment, e.g. a data center or server room, with good physical security and controlled access.

- Server platform
  - The MID server Java application runs on supported Windows or Linux Servers with a Java Runtime Environment. Installation packages are digitally signed for security. The server operating system and runtime environment should be deployed, secured, and hardened in line with your existing internal IT security policy and operating procedures.
- Network connectivity
  - Communication from the MID Server to your instance is only ever outbound; on your local network it is only to systems that you determine. All outbound connections are via HTTPS on port 443. You can explicitly disable SSL to ensure that only TLS 1.2 is used. Other versions of TLS are not supported.
  - MID servers must be able to connect to https://install.service-now.com for automatic updates, and can use a web proxy for outbound connections. For releases after London, MID servers can upgrade directly from the instance itself.
  - On the internal network, the MID server uses a variety of ports and protocols according to the resources it is connecting to, e.g. SSH, WMI, SNMP, etc.
  - Ensure that you exclude (or disable) the MID server during any internal vulnerability scanning to avoid creating unnecessary traffic to your instance.
- Other considerations
  - You can increase the operational security of the MID server by encrypting credentials stored within configuration files, supplying SSL/TLS certificates, enabling certificate validation and requiring authentication for web services connections.
  - You should store the credentials the MID server uses for service connections in a secure external storage system for additional protection.
  - From the Orlando release onwards, the MID server supports Microsoft Just Enough Administration (JEA) for basic discovery. This uses role-based administration through PowerShell Remoting and removes the need for discovery accounts to have full Admin privileges.

Best Practice: Ensure the MID server is in a physically secure, controlled location and that the operating environment has been secured and hardened. Enable only the minimum connectivity necessary between the MID server and the internal and external network, allowing for required services and infrastructure. Disable the use of SSLv3. For additional security, you can encrypt stored credentials, enforce certificate validation and supply SSL certificates, and you should protect service credentials in a secure storage system.

Encryption

The Now Platform can encrypt data to maintain its confidentiality and integrity. While in transit, data is secured with TLS 1.2; while at rest, data fields can be encrypted within the database. The physical disks on which the instance runs can be encrypted in their entirety to guard data in case of their loss or theft.

You can use different types of encryption simultaneously for data stored in your instance. You should select these according to the risks you wish to mitigate. For example, you might choose full disk encryption for a base level of protection against drive or server theft. You can protect sensitive database fields or attachments with platform encryption. Database encryption allows you to ensure all data stored in the system remains encrypted while your instances are in use. For

extremely sensitive data that should not leave your premises, Edge Encryption or tokenization provides the ideal solution.

Information transferred between your ServiceNow instance and any external services you have integrated with, e.g. authentication, file transfers, or web services extensions, can also be encrypted. This is also true of traffic to and from the MID server.

- Data in transit
  - Data transferred between a user's web browser or mobile app and a ServiceNow instance is transferred over HTTPS using TLS, with AES 128 or AES 256 cipher suites (SSL is not supported) and all HTTP requests are redirected to HTTPS. The data is decrypted again at the ServiceNow perimeter before being entered into the database.
  - Outbound email can also be sent over TLS, as described in the email security section of this document.
  - Edge Encryption enables an on-premises proxy application to encrypt or tokenize specified data with AES 128/256 before transmission to your instance over HTTPS. In this case, data is already encrypted or tokenized when it enters the instance, so in effect, your most sensitive data need never leave your premises in a vulnerable form. Since your organization holds the encryption keys, the data cannot be decrypted by anyone without the proper authorization and is always inaccessible to ServiceNow.
- Data at rest
  - Data stored within an instance can be protected with column-level encryption using TDEA, AES128, or AES256. This allows encryption of specified database fields and stored files through use of encryption contexts. These enable you to decide what is encrypted, select the algorithm used, and supply the encryption key, which is stored within the instance. This key is itself encrypted by a unique AES128 key stored separately in the ServiceNow key management infrastructure. Encryption contexts are tied to defined user roles, and hence are used to control user access to data.
  - Full disk encryption is an additional cost option where the disks used to store your instance and data include self-encryption capabilities. This encrypts all your information when the system is offline and therefore provides protection in the unlikely case of physical disk loss or theft.
  - Database encryption is an additional cost option that allows you to encrypt all of the data stored within your database, with no loss of functionality. Data is encrypted with AES encryption and decrypted in real time as it is accessed. If enabled, this will also be applied to all sub-instances and backup data.
- Integration traffic
  - Single sign-on (SSO) authentication can be performed using SAML integrations to your IdP using TLS. Secure Lightweight Directory Access Protocol (LDAPS) is also available for authentication and user object synchronization.
  - File transfers can be made outbound from your instance with SFTP, FTPS, or SCP. Outbound clear text protocols such as FTP and HTTP are also supported, but not recommended. Inbound transfers such as web uploads are conducted exclusively over HTTPS. In each case, TLS is supported. Email attachments are discussed in the section on email security.
  - Inbound and outbound web-based connections to external REST/SOAP services are also over HTTPS using TLS. Outbound connections can also benefit from certificate-based mutual authentication. SOAP requests can also be digitally signed.
  - Outbound JDBC queries can be made from your instance. This traffic is not encrypted but can be securely proxied via the MID server discussed elsewhere in this document.

Best Practice: Configure web browsers to use only TLS 1.2 or higher when connecting to your instance. This can be done on the browser itself or enforced by your web proxy or other gateway. Encrypt data at rest within the instance using the method that best suits your needs. Traffic to your integration providers should be configured to use TLS wherever possible, with outbound REST/SOAP connections making use of certificate-based authentication.

Software updates

As with any software product, a ServiceNow instance requires maintenance and updates from time to time. This is achieved by applying the patches and upgrades made available by our Patching and Upgrades Program.

- ServiceNow Patching Program
  - The ServiceNow Patching Program updates customer instances to required patch versions throughout the year. With this program, instances receive the latest security, performance, and functional fixes. Most importantly, patching remediates known security vulnerabilities and is an essential component of any patch management process.
  - More detailed information about the program is available to customers in the ServiceNow Patching Program FAQs knowledgebase article.
- Upgrades
  - Periodically upgrading the software version allows you to benefit from enhanced functionality, performance and usability. There will typically be two major platform upgrades released every year. Upgrades can be installed at your convenience within the bounds of the ServiceNow end-of-life (EOL) policy.
  - We *strongly advise* customers to upgrade at least once per year. You can find more guidance and best practices on upgrading and many other topics in the Customer Success Center.
- EOL policy
  - To help ensure the highest levels of security, we require you to keep up to date with platform releases, and our EOL policy reflects this. We usually release two major version updates per year and in general will only support the current version (N) and one prior release (N-1). Older versions are considered 'end-of-life', are no longer supported, and must be upgraded by a specified date to ensure the security of both your instance and those of all other customers. After this date your instance will be automatically upgraded if necessary.

Best Practice: Aim to install patches and platform updates as soon as possible to ensure the highest levels of security for both your own instance and those of other customers. This also enables you to maintain continuous support by conforming to the EOL policy.

Mobile application security

You may want to take advantage of ServiceNow's native mobile applications for iOS and Android, which enable use of your instance from mobile devices. These utilize OAuth 2.0 and benefit from the robust authentication mechanisms previously explored, which can be augmented with MFA along with AppAuth. Once authenticated, mobile users are subject to the same access controls as any other users.

- Mobile application security controls

  - Mobile-specific security controls are available to provide additional security functions. These include restricting clipboard operations, requiring a PIN for access, disabling attachments, and obscuring the app screen when in the background.
- Data security
  - All data in transit is protected with TLS, and application preference information is encrypted with AES128.
  - By default, only application preferences are stored locally; no record data is stored on the mobile device, though this is configurable.
- Application distribution
  - The mobile applications can be distributed with common Enterprise Mobility Management (EMM)/Mobile Device Management (MDM) platforms.
  - Mobile application security can be further managed with Microsoft Intune or Blackberry Dynamics

Best Practice: Employ MFA along with your preferred authentication mechanism. Use the built-in controls for application access, clipboard, screen shots, etc. Avoid storing record data on the mobile device. Utilize an EMM to ensure secure management of mobile devices and applications.

Vulnerability assessment and penetration testing

Vulnerability assessment and penetration testing are vital for confirming the security of an instance and to identify and address any potential weaknesses.

To ensure the highest levels of security for our customers, we have developed a sophisticated vulnerability testing and remediation program. We understand that you may also wish to carry out your own application penetration testing to learn more about the external security posture of your instances. Both of these processes are described here:

- The ServiceNow testing program
  - We use a multi-layered testing program and SSDLC for developing our products. We follow recognized industry best practice from organizations such as OWASP and NIST, among others. Throughout the development cycle, we regularly test against the most common web application threats, such as those specified in the OWASP top-ten, e.g. input validation, cross site scripting (XSS), and session management.
  - Our product security team regularly scans test instances of supported releases with a commercial web application scanner which has been configured and tuned specifically for the Now Platform. Scans are modified as necessary to cover new features or platform changes. Any validated findings feed into the development remediation process so that identified vulnerabilities are addresses prior to release. Our vulnerability management SOP describing this process is available to customers in CORE.
  - Code is statically tested for vulnerabilities using a related process when checked into the main ServiceNow branch. We also perform internal, manual testing of any new patches and hot fixes developed through the lifecycle of a release family. In both cases, any detected issues enter the remediation process to be addressed where necessary.
  - Cloud infrastructure is internally (weekly) and externally (daily) scanned for vulnerabilities using a third-party enterprise vulnerability scanner. Internal scanning is performed on an authenticated basis to ensure maximum coverage.

  - An independent third party performs application penetration testing on all major releases before they are made available to customers. Validated findings are taken forward for remediation based on a number of factors, including overall risk and possible impact. Customers may request a summary of the results from these tests.
  - We rotate testing through a number of qualified providers to deliberately expose the platform to different teams, processes, and techniques. This maximizes the possibility of gaining actionable results during this stage of the overall process.
- Customer testing
  - You are allowed to perform your own application penetration test against your instance once a year, provided you have first *met the pre-requisite conditions* listed below (so that security fundamentals are in place) and the that test has been correctly scheduled and authorized. You can make your request via the Security Center in the HI Service Catalog. Any security testing outside of this process is not permitted.
    - The target instance must be running the latest update and hotfix set for the supported version. Testing is not permitted on early access (EA) releases.
    - The instance must achieve an 'Excellent' rating after being hardened as outlined in the Instance Hardening Guide.
    - You must report your findings to us within 10 business days.
    - In the event that you discover a potential vulnerability, please follow our Responsible Disclosure Guidelines in all cases.

The HSP and Instance Hardening Guides described earlier in this document are important tools for securing your instance(s) and remediating against potential vulnerabilities.

Best Practice: Review ServiceNow's most current published penetration test reports in CORE. If you wish to carry out your own annual application penetration test, ensure that you have first installed the latest updates, hardened the instance, and fulfilled the pre-requisite conditions described above. You can then schedule your test in HI. ServiceNow will respond to findings in accordance with the process described in the Customer Application Penetration Testing document.

Summary

Though the Now Platform is designed with security as a priority, the way you set up your instance to meet your security policies has a large bearing on the security of the data it contains. Maintaining security is an ongoing process, so it's important to monitor activity, keep abreast of new developments, implement relevant changes, and verify the results in a regular cycle.

This document has given an overview of the main areas to focus on to ensure the security of your ServiceNow instance. There are also inline links to a wide range of resources providing more details and guidance. By using the information provided, you will be able to configure your instance to be as secure as possible and ensure that it remains that way.

Please visit the ServiceNow documentation site for further reading.

Some customers may require assistance in addressing some of the content in this guide due to resource or skills constraints. ServiceNow has introduced the TuneUp your Security service to help address this. You can find out more by watching this webinar.

servicenow

Appendix A: Additional critical security settings

The core content of this guide explains the main areas that should be examined and configured to maximize the security of your instance. This appendix lists a handful of critical low-level properties whose configuration should be checked and verified. They are usually set correctly when the High Security Plugin is activated, but if incorrectly configured, and without any other mitigation, they could have a significant security impact.

Some of these properties are covered elsewhere in this guide under other topics such as High Security Settings, but they are highlighted here for clarity and ease of reference.

Property (hyperlinked)	Default (recommended) value	Implications
glide.script.use.sandbox	**True** *(enable script sandboxing)*	The script sandbox limits the actions scripts can perform. Disabling this could allow a user to run JavaScript on the instance unrestricted with high-level privileges, which could result in negative consequences or instance compromise.
glide.sm.default_mode	**Deny** *(default deny mode)*	This sets the instance's default data access behavior. If set to "Allow" the ACL engine will allow read, write, create and delete access to any tables that don't have more restrictive ACLs set.
glide.script.secure.ajaxgliderecord	**True** *(perform GlideAjax ACL evaluation)*	This enforces ACL evaluation for GlideAjax API calls e.g. from scripts. If set to "False" users could bypass any ACLs in place, and access or modify data in any table via GlideAjax calls.
glide.pop3readerjob.create_caller	**False** *(do not automatically create users)*	If set to "True", user accounts can be automatically created by sending an email to the instance.
glide.script.allow.ajaxevaluate	**False** *(do not allow client scripts on server)*	This controls whether clients can run scripts on the server. Setting this value to False prevents client scripts being run on an instance via an AJAXEvaluate API call. This works in conjunction with the script sandbox.
lide.basicauth.required.scriptedprocessor	**True** *(require authentication for script requests)*	If this property is set to false, incoming script requests are not authenticated. This could allow unauthorized access to data.

Appendix B: HealthScan checks

The ServiceNow customer outcomes team can assess the security of your instance using a tool called HealthScan, which evaluates the overall configuration of your instance, including specific security properties. It produces several scores which help indicate any areas which could be improved. The Instance Security Center gives a similar evaluation, in line with the HealthScan analysis.

By following the advice in this guide, you can ensure your instance is configured to a high level of security. However, HealthScan examines some additional properties which are only covered in the Instance Hardening Guide. Those properties are listed here for completeness, and so that you can adjust them if required.

Security topic	Property (hyperlinked)	Recommended value	Description
Access controls	glide.live_profile.details	**ACL**	Enable ACLs to control live profile details
	glide.script.ccsi.ispublic	**False**	Privacy on client-callable script includes
	glide.soap.require_content_type_xml	**True**	SOAP content type checking
	glide.basicauth.required.jsonv2	**True**	Requiring basic authentication for incoming JSONv2 requests
Email security	glide.email.inbound.convert_html_inline_attachment_references	**False**	Convert inbound email HTML
	glide.user.default_password	**User defined**	Set complex 'default' password
Input validation	glide.export.escape_formulas	**True**	Escape Excel formulas
	glide.ui.jelly.js_interpolation.protect	**True**	Jelly/JS interpolation
	glide.ui.security.allow_codetag	**False**	Allow embedded HTML code
	glide.html.sanitize_all_fields	**True**	HTML sanitizer
Security whitelisting	sys_whitelist_packages	**Empty list**	Check whitelist package calls
	sys_whitelist_member	**Empty list**	Check whitelist member calls
	glide.security.url.whitelist	**Active**	URL whitelist for logout redirects
	glide.xml.entity.whitelist	**Active**	Enable XML entity whitelist

	glide.xml.entity.whitelist.enabled	**True**	Allow XML entity validation
	com.glide.script.packages_call_removal	**Active**	Packages call removal tool
Session management	glide.ui.session_timeout	**60 min**	Session activity timeout
	glide.cookies.http_only	**True**	Cookie access via HTTP only

servicenow

Appendix C: Resources

For more information

- Securing the Now Platform eBook
- ServiceNow Assurance Pack (SNAP)
- Defending your Instance against Password Spray Attacks
- ServiceNow Data Access Controls
- Cloud Security, Trust and Compliance Center
- Customer Success Center
- Integrate your Tenable.io and Tenable.sc with ServiceNow Vulnerability Response
- Implement ServiceNow Vulnerability Response
- How does my CMDB impact Vulnerability Response
- Trust Site
- CORE - Compliance Operations Readiness Evidence Portal
- How to contact ServiceNow
- www.servicenow.com

Acronyms used

Acronym	Term
TDEA	Triple Data Encryption Algorithm Keying option 1
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
CORE	ServiceNow Compliance and Operations Readiness Evidence portal
EOL	End of Life
HSP	High Security Plugin
IdP	Identity Provider
IMAP	Internet Message Access Protocol
LDAPS	Secure Lightweight Directory Access Protocol
MFA	Multi Factor Authentication
MID	Management, Instrumentation and Discovery Server
NIST	The National Institute of Standards and Technology
OAuth	Open Authorization standard
OWASP	The Open Web Application Security Project
POP3	Post Office Protocol, Version 3

SAML	Secure Assertion Markup Language
SMTP	Simple Mail Transfer Protocol
SSDLC	Secure Software Development Life Cycle
SSO	Single sign-on
SSO	ServiceNow Security Office
SSL	Secure Sockets Layer
TLS	Transport Layer Security