ServiceNow Security Best Practices Guide

Key considerations for securing Now Platform instances
Introduction

This document gives guidance on some of the main areas customers should consider when securing their Now Platform instance under the Shared Security Model.

*Please note: all information in this white paper is related to the standard Now Platform commercial environment.*

For information related to other globally located ServiceNow in-country cloud offerings and how these offerings may differ, please contact your ServiceNow account representative.
Table of contents

Introduction .................................................. 2
Overall security responsibilities .......................... 4
Certifications and accreditations .......................... 5
Securing the Now Platform instance ..................... 5
  Security contact details .................................. 5
  ServiceNow High Security plugin ....................... 6
  Instance hardening ...................................... 6
  Secure Coding ........................................... 7
  Email security .......................................... 7
  Logging and monitoring .................................. 9
Access control ............................................... 11
  Authentication ........................................... 11
  MID server security ..................................... 14
Encryption .................................................. 15
  Data in transit .......................................... 15
  Edge Encryption ........................................ 15
  Data at rest ............................................. 16
  Platform Encryption ..................................... 16
    Column Level Encryption Enterprise (CLEE) ........ 16
    Cloud Encryption ...................................... 16
    Key Management Framework (KMF) ................. 16
Software updates ......................................... 17
  Full Disk Encryption (FDE) ............................. 17
Mobile application security .............................. 18
Vulnerability assessment and penetration testing .... 19
Summary ..................................................... 20
Resources ..................................................... 20
Appendix A — Critical Security Settings ................. 21
Overall security responsibilities

Security is a partnership between the provider and customer, both with specific responsibilities.

ServiceNow provides its customers with extensive capabilities to configure their instances to meet their own security policies and requirements. However, overall security responsibilities are shared between customers, ServiceNow, and the data center provider.

The areas of responsibility are shown in the table below. For more information about security responsibilities with respect to customer data, please review Safeguarding Your Data and the Shared Responsibility Model overview.

There are several topics to consider when securing a Now Platform instance.

Some of these are configuration parameters within the product, and others relate to the customer’s own infrastructure, technologies, and how they are integrated.

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure configuration of instance</td>
<td>●</td>
</tr>
<tr>
<td>Authentication and authorization</td>
<td>●</td>
</tr>
<tr>
<td>Data management (classification and retention)</td>
<td>●</td>
</tr>
<tr>
<td>Data encryption at rest</td>
<td>●</td>
</tr>
<tr>
<td>Data encryption in flight</td>
<td>● ●</td>
</tr>
<tr>
<td>Encryption key management</td>
<td>● ●</td>
</tr>
<tr>
<td>Security logging and monitoring</td>
<td>● ●</td>
</tr>
<tr>
<td>Secure SDLC processes</td>
<td>● ●</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>● ●</td>
</tr>
<tr>
<td>Vulnerability management</td>
<td>● ●</td>
</tr>
<tr>
<td>Privacy</td>
<td>● ●</td>
</tr>
<tr>
<td>Compliance: regulatory and legal</td>
<td>● ● ●</td>
</tr>
<tr>
<td>Employee Vetting or Screening</td>
<td>● ● ●</td>
</tr>
<tr>
<td>Physical Security &amp; Environment Controls</td>
<td>● ● ●</td>
</tr>
<tr>
<td>Cloud infrastructure security management</td>
<td>●</td>
</tr>
<tr>
<td>Infrastructure management</td>
<td>●</td>
</tr>
<tr>
<td>Media disposal and destruction</td>
<td>●</td>
</tr>
<tr>
<td>Backup and restore</td>
<td>●</td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td>●</td>
</tr>
</tbody>
</table>
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 must be demonstrated consistently both to maintain customer trust and for regulatory and compliance reasons. ServiceNow maintains accreditation with many common standards.

A full list of the ServiceNow security-related certifications are publicly available on the Compliance page of the ServiceNow Trust site. They include the ISO 27001 series (27017, 27018, and 27701), as well as other global, regional, and industry specific certifications such as FedRAMP.

Securing the Now Platform instance

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

Best Practices: If customers make any configuration changes to their instance based on the information provided, ServiceNow strongly recommends that they first test those changes on a non-production instance.

Security contact details

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

- The security contact record within the customer account (located in Now Support) should be completed as soon as possible with details of at least two appropriate information security personnel.
- Security contacts should be capable of understanding and acting on the information they receive, since it may be critically important.
- If a customer specifies a distribution list, then they should also add a named individual.

Best Practices: Make sure the security contact details are accurate and always kept up to date, bearing in mind personnel and process changes within their organization.
ServiceNow High Security plugin

To help customers secure their instance easily and efficiently, ServiceNow provides 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 a customer’s instance 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: Customers 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, this property sets 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 control section later in this document for more details on authorization and ACLs.

Self-privilege elevation: Users with Security Admin privileges can elevate themselves when they need to perform operations requiring a higher privilege level. This action modifies ServiceNow system logs to be read-only and allows for controls to authorize access of properties.

Best Practices: Ensure that the High Security plugin is installed and activated where possible and enable the “default deny” property.

Instance hardening

In order to make a customer instance as secure and resistant to unauthorized access as possible, they will need to examine configuration, coding practices, and wider aspects of the deployment such as integrations or policies.

Guidance

The Hardening Settings content describes ways to make a customer 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 the usage context, which is why those settings are not enabled by default.
- The ServiceNow Security Center (SSC), described on the next page, can greatly assist with assessing and working towards compliance with the Instance Security Hardening Settings.
ServiceNow Security Center (SSC)

The ServiceNow Security Center is an application with a set of tools designed to help customers easily improve the security and compliance of their Now Platform instances.

The SSC Security Hardening tool allows customers to view their compliance with the ServiceNow recommended settings as a percentage score, identify the top non-compliant hardening settings that improve compliance, and allows for easy changes of the settings to strengthen their security posture.

In addition, the SSC Security Metrics tool provides over 60 different security KPIs that can be monitored, and it also creates notification alerts to help identify potential security issues, and insecure user behaviors.

Secure Coding

Development of code or applications on a customer 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 Practices: Customers should consult the ServiceNow Security Center frequently to assess and monitor their instance’s overall security level.

- Use the Hardening tile to research, test, and identify areas of noncompliance in a sub-production instance to assess impact to your environment. Ideally, the score should be as close to 100% as possible with a minimum score of 83%, without affecting product functionality.
- Enable the weekly digest notification to alert you to potential issues.
- Refer ServiceNow developers to the Secure Coding Guide to ensure that 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. Customers can choose which of these to enable as appropriate to enforce their 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 a customer instance for inspection by their 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. Customers can use these as criteria for the Email Filters Plugin to act on, if desired.

Email domain restriction

Customers can control the domains and users their instance can send email to and receive from by using system address filters. These can be customized to meet customer requirements.

- An organization may control inbound email with anti-spam technology using Sender Policy Framework (SPF). If so, their email systems need to accept email originating from their Now Platform instance. This is best achieved by configuring them to dynamically query the ServiceNow SPF records.
• If SPF is not an option, another approach is to add the ServiceNow mail server IP addresses to the “allow” list. This does need to be monitored, as the addresses could be subject to change.

**Automatic user account creation**

This feature allows user accounts to be [created dynamically by email](#), so it should be used with care. Only activate this feature if necessary for a specific use case.

Customers should ensure that they define a list of trusted domains from which accounts can be created. Customer admins can [control how passwords are assigned](#) to new accounts when they are created this way.

**Email monitoring**

Customers can monitor email and anti-malware activity in the [ServiceNow Security Center](#) to highlight potential issues and to guide any corrective actions that may need to be taken.

**Email encryption**

Now Platform instances have a built-in feature allowing it to send and receive email using opportunistic TLS. If a customer’s 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.

ServiceNow also supports the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. S/MIME is an end-to-end encryption protocol for sending digitally signed and encrypted emails that support data confidentiality, authenticity, and integrity.

**Customers using their own servers**

Customers can use their own SMTP, POP3, or IMAP servers for more control over how mail is filtered and received before being ingested by a Now Platform instance.

This is considered an advanced email configuration, and can optionally use a third-party email infrastructure via [OAuth 2.0](#) email authentication.

**Best Practices:** Use the email filters feature set to deal with suspect inbound messages, and limit accepted sender domains. Ensure automatic account creation is configured securely or disabled if not needed. Ideally, customers should configure their email systems to accept mail from their instance by using SPF.

If a customer already has a mature email security environment, they may consider using their own (or third-party) infrastructure to send and receive instance-related email and benefit from more precise perimeter email control.
Logging and monitoring

A Now Platform 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 a customer’s permission.

Logs are a valuable source of security information that help highlight suspicious or malicious activity, so it is essential that they are adequately monitored. Customers can feed selected log activity to their SIEM (or any syslog server), using the syslog probe.

The syslog probe is enabled via a Management, Instrumentation, and Discovery (MID) server deployed in their network. Options are also available for direct customer SIEM integration which facilitate real-time logging as part of the Vault security bundle.

The ServiceNow Security Center can also provide valuable insights. There is more information about this in the instance Hardening section of this document.

Event logs

Event logs reveal much about system activity, including login events (successful or otherwise), and privilege escalation.

System logs

System logs contain extensive information about general activity, including configuration changes, system errors, workflows, and inbound/outbound data connections.

Audit logs

The Event and System logs can also be used to provide an audit trail of any activity by ServiceNow personnel.

Transaction logs

These logs 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

Customers can enable auditing for database tables. Record history is perpetual and allows customers 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.

Import logs

Customers can view detailed information related to data import activity into their instance by checking the import logs. This includes information about source and status, time etc.

Outbound web services logs

These show REST and SOAP request activity and can help customers keep track of the volume and destination of connections to external services.
API Analytics
Customers can track and analyze inbound REST and SOAP activity with API Analytics. This will help the customer to understand which APIs are being used, by whom, and to what degree.

Log archival
Customers may wish to transfer log data from the instance to their environment for archival beyond the default log rotation period. The log rotation period varies depending on the log type.

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. Customers can add a system property to disable these messages.

An organization’s information security policy can provide guidance on which types of events are of interest and should generate alerts. Here are some examples of notable activity:

- **Privilege escalation**
  Unexpected modifications made to privileged roles, such as Admin, ITIL_Admin, and any other roles with higher privileges could indicate suspicious actions.

- **Failed logins**
  Unusual numbers or patterns of failed logins can reveal potential brute force attempts or password spray attacks.

- **Admin users added**
  New admin account creation should always be checked for validity in case of attempts at unauthorized privileged access.

- **SNC Logins**
  Customers can monitor any ServiceNow access to their instance, and the actions performed.

- **Quarantined files**
  The ServiceNow Antivirus Protection detects potentially malicious files uploaded to a customer instance, and this should be monitored for sources and frequency.

- **Impersonations**
  Monitoring for elevated account impersonation helps highlight any potentially dangerous, unnecessary, or unauthorized privileged access.

**Best Practices:**
- 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 a customer’s 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 user must have an associated unique user account defined within the Now Platform instance, and their identity must be established before access is granted. Outbound IP access controls is configured using the IP Address Access Control feature in the Now Platform. Additionally, ServiceNow supports the System for Cross-domain Identity Management (SCIM) protocol, which allows customers to synchronize user and group data from an external identity providers.

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

Authentication

Account and password control

Now Platform instances come 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.

- Customers have full control over the password policies enforced for access to their instance. For native or local accounts, customers can specify length, complexity, expiration, uniqueness, lockout, etc. (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. Customers can of course retain their existing policies for any external authentication services they 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 their instance from an unsecure endpoint, e.g., from a shared computer. The Instance Hardening Guide recommends disabling this feature.
- Remove credentials from the Welcome page and password-less authentication (logging in to the Now Platform with blank passwords).
- Configuring account lockout after a number of failed logins within a certain time frame can help guard against brute force authentication attacks.
- ServiceNow provides further guidance on enhancing authentication security in the Defending Your Now Platform instance Against Password Spray Attacks knowledge base article.
- Activating the System for Cross-Domain Identity Management (SCIM) plugin allows customers to easily provision and manage user identities, group membership and other properties from sources external to their instance using an industry-standard protocol. These typically include cloud-based services like Active Directory, Amazon Web Services, Okta and others. The ServiceNow SCIM features frees customers from having to create and manage multiple customized SOAP APIs.

Authentication mechanisms

A selection of authentication mechanisms are available. Basic or native authentication uses local accounts defined within the instance, while SAML 2.0, LDAP, OAuth2.0, and certificate-based authentication enable integration with external services. SAML 2.0 is often preferred as an 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.

- Multi-provider Single Sign On (SSO) makes it possible to combine SSO with other authentication methods, including Open ID Connect (OIDC). OIDC allows users to authenticate using third party credentials such as from Google, Azure, Okta or others.
- For high-security environments, customers can use Personal Identity Verification (PIV) card or Common Access Card (CAC) authentication as an extension of certificate-based authentication, where certificates are stored on a smartcard.
- Customers can help prevent unauthorized access to their instance, unrelated to their organization, by setting an Inbound IP access restriction. For this access restriction ServiceNow recommends using Adaptive Auth, typically only allowing external addresses from the customer’s gateway or web proxy. Anyone trying to access the instance from an unauthorized range will be denied. If using this approach, consider where all users access the instance from, e.g., remote users. Customers can control outbound as well as inbound access by IP address.
- Adaptive Authentication allows a combination of criteria including IP address, role, and group membership to be used to create granular access control policies. These can be applied to Web Services/APIs as well as to normal user access.
Access via Side Door

If a customer has problems with, or failure of, their external authentication system, they can use Side Door access which allows users with local accounts to log in. Though ServiceNow advises against it, this feature can be disabled, or the login page can be renamed. In this case ServiceNow strongly encourages customers to notify Customer Support of the modified name.

- When Multi-provider SSO is active, customers can make SSO credentials mandatory for the main login page. In this case, Side Door access is still available.
- In the event of issues with SSO, Account Recovery (ACR) allows designated Administrator accounts to log in while bypassing SSO. If ACR and SSO are active on an instance, additional protections are placed on the main and Side Door login pages.

Multi-Factor Authentication

Third-party multi-factor authentication (MFA) can be integrated with a customer’s existing SAML IdP to provide additional login security. MFA provides a high level of security because authentication requires something the user knows (the password) as well as something they own (a one-time code produced by a MFA token or mobile phone, or physical attributes e.g., a fingerprint). Users logging into a system with MFA enabled must provide this additional credential along with their username and password.

- The Web Authentication integration, allowing physical keys and biometric data such as fingerprints or facial recognition to be used with MFA.
- The Now Platform supports direct MFA integration with local accounts, LDAP, and for SSO with SAML, OIDC, or Digest. The expansion of this feature allows conditional, rigorous authentication for e.g., remote users. Adaptive Authentication is a prerequisite for SSO with MFA.
- MFA can be enabled for specified users and specified roles, and configured for ease of use, e.g., to exempt recognized devices for a number of hours. ServiceNow recommends that customers enable MFA by default for all Admin users. MFA is supported for SSO integration, and ServiceNow offers built in MFA options, as well as email and SMS OTP.
- Customers can view Metrics for MFA use in the ServiceNow Security Center.
- Customers can use Adaptive Authentication to enforce contextual authentication controls to the right users at the right time. This included Step-Up or Step-Down MFA polices.

Monitoring

ServiceNow strongly recommends that customers monitor the event log for unusual activity such as high numbers of failed logins, especially within short time frames. Now Platform instances can create incident tickets or trigger workflows (e.g., notify a customer’s security response team) automatically when user-defined criteria and thresholds are met.

- Use the Session Management tile in the ServiceNow Security Center to view detailed information about all user sessions and lock out any that could present a risk.
- Optionally, customers can use a data filter to narrow the scope of their data filtration rule to apply only to specific records on a table as well as monitor high privileged users and get notified when new admins are created.

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, customers may want to limit concurrent sessions for the same account or role.
- If the HSP (described earlier) is enabled, customers can 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

Customers can place access 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 their instance. Customers 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.
- Attachments can be encrypted. See the Encryption section in this document for more details.

Access by ServiceNow employees

Generally, ServiceNow personnel cannot access a customer instance without their authorization, except for Customer Support employees assigned to an open case for that customer. 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. This is also tracked in the Instance's Security Center widget. There is more detail in the Securing the Now Platform white paper, including on controls such as the ServiceNow Access Control plugin (SNAC).

Customers may choose to activate the ServiceNow Access Control plugin to enforce a default deny posture for all users (including ServiceNow employees), except those that the customer specifies. Once this is activated, ServiceNow personnel must explicitly request access from the customer on an ad-hoc, and temporary, basis.

Auditing access permissions

Customers 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.

Customers can also use another ServiceNow tool to audit access permissions called Access Analyzer. Access Analyzer allows analyzation of the access control rules for a specific table or field, and allows customer admins to see which roles are required to perform read, write, create, or delete operations on that table or field.

Instance identification

The way customers name and brand their instance can help with security. Customers may wish to avoid choosing a name for their instance that obviously associates it with their organization, e.g., acmeinstance or mycompanyprod.

- Customers can rename an instance if necessary.
- Customers should also carefully consider how they use branding and logos on the login page.

Best Practices:

- Change the default login credentials. If possible, use SAML authentication, and integrate with MFA.
- Enforce the use of strong passphrases and restrict access to a customer instance from unknown IP addresses.
- Review the ServiceNow guidance on password spray attacks and 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 modules, formerly 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 specified users at ServiceNow that have access to the Now Platform instance.


**MID server security**

The ServiceNow MID server is a Java application that runs as a service on one or more servers on a customer network, which is designated for that role. The MID server acts as a conduit to the customer’s infrastructure (and services) that need to communicate directly with the Now Platform instance. These services might be internal or external to the customer network and can 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 the customer’s existing internal IT security policy and operating procedures.

**Network connectivity**

Communication from the MID Server to a customer instance is only ever outbound; on their local network it is only to systems that they determine. All outbound connections are via HTTPS on port 443. Customers can explicitly disable SSL to ensure that only TLS 1.2 is used.

- 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. 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.
- The customer admin should ensure that they exclude (or disable) the MID server during any internal vulnerability scanning to avoid creating unnecessary traffic to their instance.

**Other considerations**

There are extensive options for protecting MID Server data with encryption.

- Customers can encrypt credentials stored within configuration files, supplying TLS certificates for mutual network authentication, enabling certificate validation, code signing and requiring authentication for web services API and SOAP connections.
- Customers should store the credentials the MID server uses for service connections in a secure external storage system for additional protection.
- ServiceNow recommends that customers enable the MID server command audit log, which records the commands run for the Discovery application. Customers should also regularly review the log to check for anomalies or errors.
• 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.

• Client-Side Secrets Management capability, included in the Vault bundle, allows customers to secure secrets at the MID server, so the private key is not housed in the Now Platform instance.

**Best Practices:**

- 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, customers can encrypt stored credentials, enforce certificate validation, and supply TLS certificates.
- 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 configured to be encrypted within the database and/or customers can elect to subscribe to functionality to encrypt the data volume transparently on the backend. The physical disks on which the instance runs can be encrypted in their entirety to guard data in case of their loss or theft.

Customers can use different types of encryption simultaneously for data stored in a Now Platform instance. Customers should select these according to their use case and the risks that they wish to mitigate. For example, a customer might choose to transparently encrypt their data at rest, data fields can be configured to be encrypted at the application layer, cloud encryption on the entire data volume, or leverage full disk hardware encryption – which also requires a dedicated environment to protect against drive or server theft.

Information transferred between a customer’s Now Platform instance and any external services customers 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 is transferred between a user’s web browser or mobile app and a Now Platform instance over HTTPS using TLS 1.2, with AES 128 or AES 256 cipher suites (SSL is not supported).

- All HTTP requests are redirected to HTTPS (secure HTTP).
- 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**

Edge Encryption enables an on-premises proxy application to encrypt (or tokenize) specified data with AES 128/256 before transmission to a customer instance over HTTPS.

In this case, data is already encrypted (or tokenized) when it enters the Now Platform instance, so the customer’s most sensitive data never leaves their premises in a vulnerable form.

Since the Now Platform customer 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 a Now Platform instance, including attachments, can be protected with column-level encryption using AES128, or AES 256. This allows encryption of specified database fields and attachments through use of cryptographic modules (formerly encryption contexts).

- These cryptographic modules provide role-based access control and enable customers to decide what is encrypted, what algorithm is used, and which encryption key is utilized.
- The key itself is stored within the instance and is protected via the Now Platform NIST 800-57 compliant Key Management Framework.
- The encryption key is also protected by a wrapping mechanism through several other keys stored within the customer instance and the ServiceNow Key Management System (KMS).
- The Password2 field type in ServiceNow is an out-of-the-box feature specifically designed for the secure storage of sensitive data. When data is entered into this field, it’s encrypted using a dedicated cryptographic module. This encrypted field is particularly useful in scenarios such as system integrations where authentication credentials, like API keys, are stored, or in custom ServiceNow applications where sensitive information needs to be safeguarded.

Platform Encryption

Platform Encryption brings together Column Level Encryption Enterprise with the new Cloud Encryption capabilities.

Column Level Encryption Enterprise (CLEE)

Column Level Encryption Enterprise is available as an additional licensable as part of the Platform Encryption bundle. This encryption option is similar to the "legacy" column-level encryption, but with multiple additional capabilities, such as API support, system-level access.

API support enables automated processes and workflows to function on encrypted data and enhanced key management with the option of customer-supplied keys (Bring Your Own Key, BYOK).

CLEE employs Cryptographic Modules in which an encryption key, scheme, and policy are combined to allow flexible and granular cryptography for instance data.

Cloud Encryption

Cloud Encryption encryption is an additional cost option available with the Platform Encryption bundle. Cloud Encryption enables encryption of the database storage volume at rest and ensures compatibility with database technology enhancements that ServiceNow may introduce in the future.

Cloud encryption provides protection in the unlikely event of physical disk loss or theft.

Cloud encryption also uses the KMF, therefore also benefits from NIST 800–57 compliant key lifecycle management, including segregation of duties, rotation of ServiceNow–managed keys and the option of Customer Managed Keys (CMK).

Withdraw and Resupply capability allows customers to withdraw their CMK and leverage Quorum control for approval operations to trigger a shutdown of their instance until a restore operation is performed to resupply the withdrawn key.

If the withdrawn CMK is not restored within 30 days, instance DB backups will no longer be accessible. Backup data lost in this way is not recoverable.

Key Management Framework (KMF)

Now Platform Key Management Framework is the foundation of Column Level Encryption Enterprise and Cloud Encryption. KMF enables FIPS 140-2-L3 compliant key storage, Bring Your Own Key (BYOK), improved key management throughout the NIST 800–57 based key lifecycle, and many other benefits, including the ability to transfer keys securely between instances.
Full Disk Encryption (FDE)

Full Disk Encryption is available at an additional cost allowing the disks used to store customer instance data include self-encryption capabilities.

FDE requires customers to purchase a dedicated environment to encrypt all information when the system is offline and therefore provides protection in the unlikely event of physical disk loss or theft.

Integration traffic

Single sign-on (SSO): With SSO, authentication can be performed using SAML integrations to the customer IdP using TLS. Secure Lightweight Directory Access Protocol (LDAPS) is also available for authentication and user object synchronization.

File transfers: Files can be made outbound from a customer's 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 over HTTPS using TLS, and can make use of certificate-based mutual authentication. In addition, inbound REST APIs can be protected with adaptive authentication access policies, and SOAP requests can be digitally signed.

Outbound JDBC queries: These outbound queries be made from a customer instance. This traffic is not encrypted but can be securely proxied via the MID server discussed elsewhere in this document.

Best Practices:

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

Software updates

As with any software product, a Now Platform 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.

Upgrades

Periodically upgrading the software version allows customers to benefit from enhanced functionality, performance, security, and usability. There will typically be two major platform upgrades released every year. Upgrades can be installed at the customer's convenience, within the bounds of the ServiceNow end-of-life (EOL) policy.

- The Upgrade Center helps customers plan and manage their upgrades by previewing changes, monitoring the process, and viewing historical information.
- ServiceNow strongly advises customers to upgrade at least once per year. Customers 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, ServiceNow requires customers to keep up to date with platform releases, our EOL policy reflects this. ServiceNow usually releases 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 the customer instance, and those of all other customers. After this date the customer instance will be automatically upgraded, if necessary.

Best Practices: Aim to install patches and platform updates as soon as possible to ensure the highest levels of security for both the customer's own instance and those of other customers. This also enables customers to maintain continuous support by conforming to the EOL policy. Use Upgrade Center to help manage the process.

Mobile application security
Customers may want to take advantage of native ServiceNow mobile applications for iOS and Android, which enable use of a customer 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. Customers can enable re-authentication to re-validate user credentials as a prerequisite to performing certain actions within the app.

Data security
All data in transit is protected with TLS 1.2, 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 can be enabled. The record data will be encrypted in storage.

Application distribution
The mobile applications can be distributed with common Enterprise Mobility Management (EMM)/Mobile Device Management (MDM) platforms.

Customers can use Mobile Application Management (MAM) to control, secure, and enforce policies for ServiceNow mobile apps. These tools provide a central point of control for securing customer data on mobile apps, even in scenarios where they are not the owner of the mobile device. ServiceNow only supports Microsoft Intune and BlackBerry SDKs.

Best Practices:
- Employ MFA along with a preferred authentication mechanism.
- Use the built-in controls for application access, clipboard, screen shots, etc.
- Avoid storing record data on the mobile device.
- Use an EMM or a MAM 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, ServiceNow has developed a sophisticated vulnerability testing and remediation program. ServiceNow understands that customers may also wish to carry out their own application penetration testing to learn more about the external security posture of their instances. Both processes are described here:

The ServiceNow testing program

ServiceNow uses a multi-layered testing program and SSDLC for developing our products. ServiceNow follows recognized industry best practice from organizations such as OWASP and NIST, among others. Throughout the development cycle, ServiceNow regularly tests 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. The ServiceNow vulnerability management SOP describing this process is available from the CORE Compliance Portal. Learn how to access CORE here.

- Code is statically tested for vulnerabilities using a related process when checked into the main ServiceNow branch. ServiceNow also performs 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 several factors, including overall risk and possible impact. Customers may request a summary of the results from these tests.

- ServiceNow rotates testing through several 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

ServiceNow customers may perform a penetration test against a sub-production instance in alignment with the ServiceNow Customer penetration testing policy. Any security testing outside of this process is not permitted.

At the conclusion of the authorized testing period, all findings that impact the platform must be reported to ServiceNow via the Security Findings application in Now Support. The process for submitting findings is detailed here.

- The target instance must be a non-production instance, running a supported update and hotfix combination.

- Customers must report their findings to ServiceNow within 30 days.

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

Best Practices: Review the most recent ServiceNow published penetration test reports in the CORE Compliance Portal. Find out how to access CORE here.

If a customer wishes to carry out their own annual application penetration test, they must ensure that they have first installed the latest updates, hardened the instance, and fulfilled the prerequisite conditions described above.

After this is completed customers can schedule a test in the Now Support Portal. ServiceNow will respond to findings in accordance with the process described in the Customer Penetration Testing Policy.
Summary

Though the Now Platform is designed with security as a priority, the way a customer sets up their instance to meet necessary security policies greatly affects the security of the data it contains.

Maintaining security is an ongoing process, it is always important to monitor activity, keep abreast of new developments, implement relevant changes, and verify the results at regular intervals.

This document has given an overview of the main areas to focus on to ensure the security of a customer’s Now Platform instance. There are also online links to a wide range of resources providing more details and guidance. By using the information provided, customers will be able to configure their instance to be as secure as possible, ensuring that it remains that way.

Please visit the ServiceNow product documentation site for further reading.

Resources

- ServiceNow Trust Site
- ServiceNow Product Documentation
- Customer Success Center
- Securing the Now Platform white paper
- Cloud Security, Trust, and Compliance Center
- Defending your Instance against Password Spray Attacks
- ServiceNow CORE Compliance Portal Directory (requires access)
- Appendix A: Additional critical security settings
- How to access the ServiceNow CORE Compliance Portal
Appendix A — Critical Security Settings

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.

<table>
<thead>
<tr>
<th>Property (Hyperlinked)</th>
<th>Default (recommended) value</th>
<th>Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.script.use.sandbox</code></td>
<td>• True (enable script sandboxing)</td>
<td>• 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.</td>
</tr>
<tr>
<td><code>glide.sm.default.mode</code></td>
<td>• Deny (default deny mode)</td>
<td>• 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.</td>
</tr>
<tr>
<td><code>glide.script.secure.ajaxgliderecord</code></td>
<td>• True (perform GlideAjax ACL evaluation)</td>
<td>• 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.</td>
</tr>
<tr>
<td><code>glide.pop3readerjob.create.caller</code></td>
<td>• False (do not automatically create users)</td>
<td>• If set to “True,” user accounts can be automatically created by sending an email to the instance.</td>
</tr>
<tr>
<td><code>glide.script.allow.ajaxevaluate</code></td>
<td>• False (do not allow client scripts on server)</td>
<td>• 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.</td>
</tr>
<tr>
<td><code>glide.basicauth.required.scriptedprocessor</code></td>
<td>• True (require authentication for script requests)</td>
<td>• If this property is set to false, incoming script requests are not authenticated. This could allow unauthorized access to data.</td>
</tr>
</tbody>
</table>