ServiceNow Security Best Practices Guide

Key considerations for securing your instance
Table of Contents

Introduction ........................................................................................................ 3
Overall security responsibilities ................................................................. 3
Certifications and accreditations ................................................................. 4
Securing your ServiceNow instance ......................................................... 4
Security contact details ................................................................................ 4
ServiceNow High Security plugin ............................................................... 4
Instance hardening ....................................................................................... 4
Email security .................................................................................................. 5
Logging and monitoring ............................................................................... 6
Access control .................................................................................................. 8
MID server security ....................................................................................... 10
Encryption ...................................................................................................... 11
Software updates ............................................................................................ 13
Mobile application security ........................................................................... 14
Vulnerability assessment and penetration testing ....................................... 14
Summary ........................................................................................................ 15
Additional Resources .................................................................................... 16
Appendix A: Additional critical security settings ....................................... 16
## Introduction

This document gives guidance on some of the main areas which should be considered when securing your ServiceNow instance under the shared security model. **Please note, all information in this eBook is related to the standard Now Platform commercial environment.** For information related to ServiceNow’s in-country cloud offerings around the globe and how they may differ, please contact your ServiceNow account representative. This document refers to resources found in the ServiceNow CORE Compliance Portal. Find out how to access CORE [here](#).

### 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.

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Customer</th>
<th>ServiceNow</th>
<th>Colocation (Data center providers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure configuration of instance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication and authorization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data management (classification and retention)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data encryption at rest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data encryption in flight</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption key management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security logging and monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure SDLC processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penetration testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance: regulatory and legal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee vetting or screening</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security and environment controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud infrastructure security management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media disposal and destruction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup and restore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td></td>
<td></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 ServiceNow’s 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 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.

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.

- The security contact record within your customer account (located in Now Support) 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.

**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.
- 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 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 Security Hardening Settings content 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 usage context, which is why they are not enabled by default.
- The Instance Security Center described below can greatly assist with assessing and working towards compliance with the Instance Security Hardening Settings.

**Instance Security Center (ISC)**

We provide the **Instance Security Center** to help you understand your instance’s security posture, letting you evaluate and harden specific security settings, monitor activity, and identify any areas for improvement. This displays security activity and configuration in a simple overview. We have produced some additional resources on how to work with ISC.

- The dashboard includes statistics, trends and an overall Compliance Score representing the level of correlation with the settings in the Instance Hardening Guide. This score can be refreshed at any time by users with an admin role.
- You can enable notifications via the Now Mobile App and third-party integrations like email, Slack or MS Teams for security events such as Admin logins, login failures, privilege escalation and others.

**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 Practices:** Consult the Instance Security Center frequently to assess and monitor your 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 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.
- If SPF is not an option, another approach is to add the ServiceNow mail server IP addresses to your ‘allow’ list, but this needs 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 should be used with care. Only activate if necessary for your use-case and ensure that you define a list of trusted domains from which accounts can be created. You can **control how passwords are assigned** to new accounts created this way.

**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.

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.

Best Practice: 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, 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 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.

Logs are a valuable source of security information that help highlight suspicious or malicious activity, so it is essential that they are adequately monitored. You can feed selected log activity to your SIEM (or any syslog server), using the syslog probe. The syslog probe is enabled via a management, instrumentation, and discovery (MID) server deployed in your network. Options are also available for direct customer SIEM integration which facilitate real-time logging as part of the Vault security bundle.

The Instance 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

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.

**Import logs**
You can view detailed information related to data import activity into your 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 you to keep track of the volume and destination of connections to external services.

**API Analytics**
You can track and analyze inbound REST and SOAP activity with API Analytics. This will help you understand which APIs are being used, by whom and to what degree.

**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.

Your 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**
You can monitor any ServiceNow access to your instance and the actions performed.

**Quarantined Files**
The ServiceNow Antivirus Protection detects potentially malicious files uploaded to your 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.
Access control

Every user must have an associated unique 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

Account and password control

- 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 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 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 unsecure endpoint, e.g. from a shared computer. The Instance Hardening Guide recommends disabling this feature.

- Remove credentials from the Welcome page, and disable password-less authentication.

- 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 knowledge base article.

- Activating the System for Cross-Domain Identity Management (SCIM) plugin allows you to easily provision and manage user identities, group membership and other properties from sources external to your instance using an industry-standard protocol. These typically include cloud-based services like Active Directory, Amazon Web Services, Okta and others. ServiceNow’s SCIM features free you 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, you 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.

- 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 will be denied. If using this approach, consider where all your users access the instance from, e.g. remote users. You 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 you have problems with, or failure of, your external authentication system, you can use Side Door access which allows users with local accounts 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 strongly encourage you to notify Customer Support of the modified name.

- When Multi-provider SSO is active, you 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 your 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. We recommend you 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.

- You can view Metrics for MFA use in the Instance Security Center.

- You can use Adaptive Authentication to enforce contextual authentication controls to the right users at the right time.

Monitoring

- 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.

- Use the Session Management tile in the Instance Security Center to view detailed information about all user sessions and lock out any that could present a risk.

- Optionally, you can use a data filter to narrow the scope of your 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, you may want to limit concurrent sessions for the same account or role.

- If the HSP (described earlier), is enabled, you 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

- You 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 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.
- Attachments can be encrypted. See the Encryption section in this document for more details.

Access by ServiceNow employees

Generally, ServiceNow personnel cannot access your instance without your authorization, except for 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. This is also tracked in the Instance’s Security Center widget. 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. You should also carefully consider how you 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 your instance from unknown IP addresses.
- Review ServiceNow’s 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 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.

- MID servers must be able to connect to [https://install.service-now.com](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.
- Ensure that you exclude (or disable) the MID server during any internal vulnerability scanning to avoid creating unnecessary traffic to your instance.

**Other considerations**

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

- You 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.
- You should store the credentials the MID server uses for service connections in a secure external storage system for additional protection.
- We recommend you enable the MID server command audit log, which records the commands run for the Discovery application and 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 ServiceNow 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, you 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.

You can use different types of encryption simultaneously for data stored in your instance. You should select these according to your use case and the risks you wish to mitigate. For example, you might choose to transparently encrypt your data at rest using database encryption on most of the database tables, 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 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 is transferred between a user's web browser or mobile app and a ServiceNow 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** 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 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, 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 you to decide what is encrypted, select the algorithm used, and supply the encryption key. The key itself is stored within the instance and is protected via ServiceNow’s NIST 800-57 compliant Key Management Framework and is protected by a wrapping mechanism through several other keys stored within the customer instance and the ServiceNow Hardware Security Module (HSM).
- **Platform Encryption** brings together Column Level Encryption Enterprise with the new Cloud Encryption capabilities or Database Encryption.
- **Column Level Encryption Enterprise** is available as an additional licensable feature. This is like the ‘legacy’ column-level encryption, but with multiple additional capabilities, such as API support, system-level access – which enables automated processes and workflows to function on encrypted data – and enhanced key management with the option of customer-supplied keys. It employs Cryptographic Modules in which an encryption key, scheme and policy are combined to allow flexible and granular cryptography for instance data.
- ServiceNow’s **Key Management Framework (KMF)** is the foundation of Column Level Encryption Enterprise. It 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.
- **Cloud encryption** is an additional cost option available with the Platform Encryption bundle. It 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, and 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)**. A 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 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.
- **Database encryption** is an additional cost option that allows you to encrypt data tables 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 (specifically, it would provide encrypted database tables within a separately encrypted backup). Database encryption provides protection in the unlikely event of physical disk loss or theft.
- You have the option of using your own encryption key with database encryption. This feature – **Customer Controlled Switch (CCS)** – requires you to implement an endpoint on your own premises or work with a technology partner who has an endpoint integration with CCS.
- **Full disk encryption (FDE)** is an additional cost option where the disks used to store your instance and data include self-encryption capabilities. FDE requires customers to purchase a dedicated environment. This encrypts all your 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) 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 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 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 Practices:
• 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 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.

Upgrades
Periodically upgrading the software version allows you 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 your convenience within the bounds of the ServiceNow end-of-life (EOL) policy.
• The Upgrade Center helps you to plan and manage your upgrades by previewing changes, monitoring the process, and viewing historical information.
• 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. Use Upgrade Center to help manage the process.

**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. You can enable re-authentication to re-validate user credentials as a pre-requisite 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. 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 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 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. 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 several factors, including overall risk and possible impact. Customers may request a summary of the results from these tests.

• We rotate 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 ServiceNow’s 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.

• You must report your findings to us within 30 days.

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 the CORE Compliance Portal. Find out how to access CORE here.

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 the Now Support Portal. ServiceNow will respond to findings in accordance with the process described in the Customer Instance Security 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 greatly affects 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 product documentation site for further reading.
## Additional Resources

- ServiceNow Trust Site
- ServiceNow Product Documentation
- Customer Success Center
- Securing the Now Platform eBook
- ServiceNow Data Access Controls
- Cloud Security, Trust and Compliance Center
- CORE Compliance Portal
- Defending your Instance against Password Spray Attacks

## Appendix A: Additional 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>glide.script.use.sandbox</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>glide.sm.default_mode</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>glide.script.secure.ajaxgliderecord</td>
<td>True (perform GlideAjax ACL evaluation)</td>
<td>This enforces ACL evaluation for GlideAjax API calls e.g. from scripts. If set to &quot;False&quot; users could bypass any ACLs in place, and access or modify data in any table via GlideAjax calls.</td>
</tr>
<tr>
<td>glide.pop3readerjob.create_caller</td>
<td>False (do not automatically create users)</td>
<td>If set to &quot;True&quot;, user accounts can be automatically created by sending an email to the instance.</td>
</tr>
<tr>
<td>glide.script.allow.ajaxevaluate</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>glide.basicauth.required.scriptedprocessor</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>