Encryption technical summary

SNAP deep dive
# Table of contents

- Introduction .......................................................................................................................... 3
- Encryption in transit ............................................................................................................... 3
  - Interactive end-user sessions .............................................................................................. 4
  - Email encryption .................................................................................................................. 4
  - File transfers ......................................................................................................................... 4
  - Direct database query ......................................................................................................... 4
  - Web services integrations ....................................................................................................... 4
  - Single sign-on (SSO) integrations ......................................................................................... 5
  - ServiceNow MID server ....................................................................................................... 5
- Encryption at rest .................................................................................................................... 5
  - Now Platform capabilities ..................................................................................................... 5
  - ServiceNow infrastructure encryption capability ................................................................. 8
- Summary ................................................................................................................................. 10
- Resources ............................................................................................................................... 11
  - Encryption-specific resources ............................................................................................. 11
  - Further reading ..................................................................................................................... 11
Introduction

ServiceNow provides its customers with a highly flexible system of action, known as the Now Platform®. This software platform, provided as a subscription service from a ServiceNow owned and managed private cloud, enables customers to automate business processes and build intuitive applications using a single data model. Customers can use the data they store within and across their assigned, individual, private instances of the Now Platform to meet their enterprise management requirements.

ServiceNow customers who have concerns about storing their information outside of their own physical premises or networks may opt to encrypt their data using one or more of the encryption options included in this document.

Encryption options in ServiceNow fall into either of two categories:
- **Encryption in transit**: information transmitted to or received from an instance of the Now platform, as well as relevant integrations
- **Encryption at rest**: information stored within an instance of ServiceNow

This document summarizes the relevant encryption capabilities and considerations for their use in ServiceNow.

Encryption in transit

By their nature, instances of the Now Platform are designed to be accessible via the internet. This provides maximum flexibility in how, when, and from where customers access their instances. The internet, however, is a public network and communications on it can be intercepted if they are not encrypted or otherwise protected.

ServiceNow provides transport layer encryption as standard within its Now Platform infrastructure. The Now Platform enables customers to use its encryption in transit capabilities when integrating with their own external systems, data sources, or services.

The following table summarizes encryption in transit features:

<table>
<thead>
<tr>
<th>Element</th>
<th>Encryption Method</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive end-user sessions</td>
<td>TLS 1.2†</td>
<td>Highest publicly-available ratified encryption.</td>
</tr>
<tr>
<td>Email</td>
<td>TLS 1.2* opportunistic TLS</td>
<td>Highest publicly-available ratified encryption where mutually supported, with cleartext</td>
</tr>
<tr>
<td>File transfers</td>
<td></td>
<td>Inbound to instance via HTTPS only Retrieved by instance, from external location: TLS 1.2* over FTPS (implicit or explicit), SFTP, SCP Highest publicly-available ratified encryption where mutually supported, with cleartext FTP option for legacy integrations</td>
</tr>
</tbody>
</table>

* Including proposed TLS1.3 suites, i.e. ECDHE-ECDSA (Forward Secrecy)
† ServiceNow is deprecating TLS versions 1.0/1.1 through Q1 2020
### Table 1 - Encryption in transit features

<table>
<thead>
<tr>
<th>Feature</th>
<th>TLS Support</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web services integration</td>
<td>TLS 1.2* supporting outbound certificate-based mutual authentication</td>
<td>Highest publicly-available ratified encryption when initiated from ServiceNow instance, but does not currently support inbound mutual authentication</td>
</tr>
<tr>
<td>Single Sign-On (SSO)</td>
<td>TLS 1.2*</td>
<td>Highest publicly-available ratified encryption.</td>
</tr>
<tr>
<td>MID server</td>
<td>TLS 1.2* plus additional application-level public key pair encryption between MID server and instance</td>
<td>Highest publicly-available ratified encryption, with double encryption of credentials used for discovery and orchestration</td>
</tr>
</tbody>
</table>

### Interactive end-user sessions

Customer end-user access to any of their assigned instances is always encrypted using TLS over HTTPS. It is not possible to connect to an instance over clear text, nor downgrade or redirect a secured end-user connection to an insecure one. The Now Platform offers AES-256 and AES-128 cipher suites, negotiated in accordance with the capabilities of a customer’s end-user’s browser or the customer’s internet-facing infrastructure. ServiceNow’s infrastructure uses TLS 1.2 cipher suites.

### Email encryption

Email is encrypted using opportunistic TLS where supported by client email infrastructure. ServiceNow will negotiate 1.2 encryption during the SMTP handshake and will fall back to plaintext SMTP where a secure channel cannot be negotiated.

### File transfers

ServiceNow supports a variety of file transfer protocols including FTPS, SFTP, and SCP. These are for instance-initiated communication out to external systems only and support TLS 1.2. There is no inbound file transfer facility beyond HTTPS/web services uploads.

### Direct database query

ServiceNow supports direct JDBC queries out to external systems. JDBC connections are not encrypted but can be securely proxied via a customer Management, Instrumentation, and Discovery (MID) server. The communication to the MID server in the customer environment is secured as described in the ServiceNow MID Server section below.

### Web services integrations

As is the case for end-user access, integrations by a customer to external SOAP or REST endpoints also use HTTPS with TLS 1.2.

In addition to the transport layer security offered by HTTPS, customers can also implement mutual, certificate-based authentication between their instances of their Now Platform and their web service endpoints. Mutual authentication to instances of the Now Platform is not possible within the current ServiceNow architecture.

---

* including proposed TLS1.3 suites, i.e. ECDHE-ECDSA (Forward Secrecy)
Secure signing of SOAP requests for message integrity purposes is also possible.

**Single sign-on (SSO) integrations**

Instances of the Now platform support SSO via the multiple provider SSO or Security Assertion Mark-up Language (SAML) 2.0 plugins.

These options allow instances of the Now Platform to be integrated with a customer’s own compliant SAML 2.0 Identity Providers, known as IdPs. These integrations benefit from transport layer encryption.

Instances also use customer-provided certificates as part of their configuration to verify a SAML assertion is properly signed by the correct IdP.

Instances of the Now Platform include LDAP client functionality and can access multiple LDAP v3 compliant directories in accordance with customer configuration. Both standard and secure LDAP (LDAPS), which uses TLS, are available.

**ServiceNow MID server**

The MID server is a Java application run as a Windows service or UNIX daemon on a server within a customer’s network. The MID server facilitates communication and the movement of data between external applications, data sources, and services, and a customer’s instance of the Now Platform. This communication takes place entirely by HTTPS using TLS 1.2.

The MID server initiates all communications with a customer’s instance, polling on a regular schedule. The instance never initiates communications with the MID server; there is no means for direct connectivity to a MID server by a ServiceNow instance as this is outside of the customer’s own network perimeter.

**Encryption at rest**

This section provides details about encryption options for data at rest in ServiceNow. There are two types of encryption available: those within the Now Platform that operate on the data, and those that operate at an infrastructure level.

**Now Platform capabilities**

Encryption capabilities are available in the Now Platform to provide field-level encryption of targeted data and attachments. It is also possible to encrypt all data within the database.

**Column-level encryption**

Column-level encryption is a built-in feature which permits encryption of both string or attachment fields using AES-128 or AES-256. Customers may encrypt existing non-system string fields or add new fields to use for encryption.

Implementation of column-level encryption begins with customers defining one or more encryption “contexts” in their instances of the Now Platform. This process includes selecting the desired encryption algorithm and providing an appropriate secret key. Access to data subsequently encrypted using the feature is role-based, with context being associated with roles. Users without the correct role will not see the field at all, or if they are assigned a role with a different context, a blank field will be displayed. Figure 1 below illustrates how role-based encryption is enabled.
Figure 1 – Role-based encryption example

Here are the results of the relationships in Figure 1 above:

- User 1 is a member of Role 1, which provides access to Encryption Context 1; this allows User 1 to see the contents of Field A and Field B.
- User 2 and User 3 are members of Group 1; Group 1 is a member of Role 1, which allows everyone in Group 1 access to Encryption Context 1 and allows User 2 and User 3 to see the contents of Field A and Field B.
- User 4 is not a member of any group or role and has no access to Encryption Context 1; not only does User 4 not have access to Field A or Field B, but User 4 will not even see that these fields exist.

Considerably more complex role-based encryption can be implemented as well.

Having access to an encrypted data field by being assigned an encryption context does not necessarily mean a user can modify it. Role-based access also needs to be implemented appropriately for that field to be accessible to users who are assigned the context via a role.

Customer encryption keys for use with column-level encryption, whether provided by a customer or randomly generated by the instance, are stored in the same unique instance database where the data encrypted by them is stored. As a further security measure, they are re-encrypted with a secondary master key unique for that instance. This mitigates direct access to the encryption key for any context, either by an instance administrator or ServiceNow. Column-level encryption does not enable customers to store encryption keys in their own HSM or other key storage appliances or services.

As the system itself does not have access to the user contexts necessary to decrypt data, some actions are not possible on encrypted data. Column-level encrypted data cannot be filtered or sorted. In releases prior to Kingston, the encrypted data cannot be searched, and workflows cannot make use of column-level encrypted data. These capabilities, along with scheduled...
reporting, are executed using a system service that has no access to encrypted data and cannot be assigned the context, groups, or roles to gain access.

**Edge Encryption**

The Edge Encryption feature is an additional cost option that provides customers the ability to control the end-to-end encryption of their data and key management. Edge Encryption uses a proxy application, provided by ServiceNow and installed by a customer within their own network. This tokenizes specified data patterns or encrypts string fields and attachment data before it is sent from a customer's environment to their instance. It also decrypts the same data, again only within the customer's own network, using keys stored only within the customer's own network. Figure 2 below illustrates Edge Encryption in action.

![Figure 2 – Edge Encryption in action](image)

Meanwhile, Figure 3 below illustrates the Edge Encryption process; a field storing social security numbers (SSN) being encrypted within a customer's network by an Edge proxy.

![Figure 3 - Edge Encryption Process](image)

In addition to the Edge proxy configuration and management of rules, customers are responsible for the usual requirements of operating a server within their environment (including hosting, routing, backup, DNS configuration, etc.) to enable and support their Edge proxies.

Edge Encryption is rule-based. Specific fields are identified for encryption or tokenization in accordance with a customer's business requirements. Data in fields encrypted by the Edge proxy will be accessible to any end-user whose roles or other access rights allow them to read or
write to that field. A user’s fundamental permissions to access the field itself is still dependent upon the role-based access controls in place in the instance. The data will be encrypted and decrypted in transit to and from the instance by the Edge proxy, transparently to the user.

Access to Edge encrypted data must always be made through the proxy application, which functions as a web application with a unique customer-defined URL. Attempting to access Edge encrypted data directly from an Edge-enabled instance without first passing through the relevant proxy will result in only the encrypted version of the data being visible. Edge proxies are hosted by customers at their own preferred URL, such as “edgeproxy.customerdomain.com”.

**Figure 4 - Edge encrypted data accessibility through the Edge proxy or directly**

The first example in Figure 4 shows an incident record which has Edge Encryption applied to the “Short description” field. This field illustrates how it would appear to an appropriately credentialed user accessing that record via the customer’s Edge proxy.

The second example in Figure 4 shows the same record and field when it is accessed directly at the customer’s instance. Because this form of access bypasses the customer’s Edge proxy, the data is inaccessible to any user, including administrators.

The relevant encryption keys and configuration exist only on the Edge proxy within the customer’s network and are not visible to ServiceNow. The data is encrypted from the moment it leaves the customer environment and is only decrypted upon retrieval. At no point is the data accessible in clear text by ServiceNow systems or personnel.

As with column-level encryption, Edge Encryption imposes some functional limitations within an instance as a result of the additional security. The local Edge proxy does however also provide some additional functionality relating to sorting when compared to column-level encryption.

For additional detail on Edge Encryption please review the [Data Encryption eBook](#).

**ServiceNow infrastructure encryption capability**

ServiceNow offers two additional encryption options for customers with statutory obligations towards data protection which may require at-rest protection for all data in-scope of such regulations or commitments.

**Database Encryption**

Database Encryption enables all data to be protected with symmetric AES-256 encryption, whether the database is online or offline. This capability is available for all supported releases.
With Database Encryption, all stored data is encrypted, and individual records or tables are decrypted in memory only while being accessed. Any new or changed data is encrypted as it is entered into a table, and associated activity log files, (e.g. bin, redo, undo, and error) are also encrypted.

Database Encryption is completely transparent to users, and there is no loss of functionality. When using this feature, all instances are encrypted, along with replication traffic and backups, and instance cloning is still available. However, there is a minor performance impact for using Database Encryption of up to 5%. Both new and existing instances on supported releases of the Now Platform can take advantage of database encryption.

As illustrated in Figure 6 to the right, keys are stored and managed by ServiceNow using a three-level key hierarchy:

- **1st level**: An AES-256 key is used to encrypt the data.
- **2nd level**: Another AES-256 key is used to protect the 1st level key.
- **3rd level**: An additional AES-256 key, used to protect the 2nd level key, is created by and stored within our FIPS 140-2 compliant key management appliances in the ServiceNow data centers.

The first two keys are customer-specific and are created by the database engine. The third key is unique per customer instance.

**Full disk encryption**

Full disk encryption (FDE) utilizes self-encrypting AES-128 storage devices in conjunction with a ServiceNow dedicated hardware option at an additional cost.

FDE applies to the hardware itself and therefore provides customers who take this option with encryption at rest for all data stored by them in every instance assigned to them.

![Database Encryption Diagram](image-url)
Encryption is applied to the entire storage system within the database server only, as this is the only customer-data storing component.

FDE protects only against physical loss or theft of storage devices. When encrypted disk servers are powered on and providing data, the encryption provides no additional protection.

For further details on selecting FDE and dedicated hardware options, please contact your ServiceNow representative.

**Summary**

The available encryption options from ServiceNow are intended to address common additional data protection and privacy needs for its customers.

- **Column-level encryption** provides simple, secure encryption out-of-the-box, but may not meet all customer requirements around key storage and management.
- **Edge Encryption** is a significant enhancement over standard column-level encryption and allows customers to control where and how data is encrypted as well as management and configuration of all keys. However, it requires significant planning on the part of the customer.
- **Database Encryption** allows all stored data to be encrypted in real-time, providing protection for data online and offline, with no loss of functionality.
- **Full disk encryption** protects offline data in case of disk loss or theft, and may be relevant to heavily regulated organizations, but can add significant cost to a customer’s ServiceNow deployment. Measures in place by ServiceNow to mitigate loss or theft of storage devices may also be a factor in its selection.

<table>
<thead>
<tr>
<th></th>
<th>Database Encryption</th>
<th>Column-level encryption</th>
<th>Edge Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Encryption of data at rest when not being processed in the instance.</td>
<td>Equality Preserving Encryption of data at rest within the database based on user role in the instance.</td>
<td>Standard, Equality Preserving, and Order Preserving encryption of data at rest within the database and instance. Data sent to ServiceNow already encrypted by customer.</td>
</tr>
<tr>
<td><strong>Field Types Supported for Encryption</strong></td>
<td>All</td>
<td>• String Text • Attachments • URL</td>
<td>• String Text • Attachments • URL • Journal</td>
</tr>
<tr>
<td><strong>Encryption Types</strong></td>
<td>AES-256</td>
<td>AES-128 and AES-256</td>
<td>AES-128 and AES-256</td>
</tr>
<tr>
<td><strong>Tokenization</strong></td>
<td>No</td>
<td>No</td>
<td>Yes, for pattern-matched data</td>
</tr>
<tr>
<td><strong>Encryption Key Creation</strong></td>
<td>ServiceNow</td>
<td>Managed by ServiceNow and the customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Additional Requirements</strong></td>
<td>None</td>
<td>None</td>
<td>• On-premises Encryption Proxy</td>
</tr>
</tbody>
</table>
Encryption Key Store
Optional on-premises MySQL Database for Tokenization and Order Preserving encryption

Table 2 – Comparison of available encryption options

For further information regarding ServiceNow’s technical and organizational security measures, please refer to other material in the ServiceNow Trust Journey.

Resources

Encryption-specific resources
- [Data Encryption eBook](#)
- [Product Documentation](#)
  - Column-level encryption technical implementation and configuration
  - Edge Encryption technical implementation and configuration

Further reading
- [Trust and Compliance Center](#)
- [CORE (Compliance Operations Readiness Evidence) platform](#)