FAQ

Cloud Security Frequently Asked Questions

servicenow

Document summary

ServiceNow's security team has compiled a list of frequently asked questions about our cloud security processes and the physical, administrative, and logical controls we have in place.

This document is intended as a supplementary handout to the ServiceNow Assurance Pack (SNAP). Prospects can download a copy of the SNAP from ServiceNow **Limited CORE** or view the documents individually on the **ServiceNow Trust Site**. Customers can download an expanded version of the SNAP from **ServiceNow CORE**.

Please note, all information in this document 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.

Table of Contents

Data access

Who has access to my data?

Customers have complete control over who accesses their data. All access is controlled via access control lists (ACLs) according to customer requirements. Except for customer support reasons, any access by ServiceNow personnel must have the customer's written permission, e.g. in the case of a professional services engagement.

Which authentication methods are available?

Built-in, multi-provider SSO, SAML 2.0, LDAP, OAuth 2.0, and others. **More details** are available in our product documentation.

What password policies can I use?

Customers can set their own password policies, either in their instance or in the external directory service used for SAML or LDAP.

How do ServiceNow employees access the cloud infrastructure?

Only ServiceNow personnel with a defined and approved support role may access the cloud infrastructure. Access is via regionally-deployed, secure virtual desktop environments. These require two-factor authentication from clients within ServiceNow address space, identified by ServiceNow-issued digital certificates. All access, authorization, SSH access, and any commands requiring elevated privileges are logged, monitored, and controlled by our centralized Privileged Access Management (PAM) system. A Host-based Data Leak Prevention (DLP) is enabled, and no internet access, email, messaging, or device and clipboard redirection is possible. Quarterly privilege reviews are undertaken for all relevant personnel.

Data residency

Where is customer data hosted?

Customer data is hosted only within their chosen regional data center (DC) pair. Regional DC pairs are pre-defined by ServiceNow. There is no defined primary and secondary site within a DC pair, but an individual instance will be served from one of the DCs at any given time until transferred to the other. Data center transfers are transparent to the end-user.

Where are the data centers located?

ServiceNow operates data centers in North America (Canada is the default location, with additional centers in the United States), South East Asia (South Korea and Singapore), Europe (Germany, Switzerland, The Netherlands, Ireland), U.K. (England and Wales), Japan, Australia, and Brazil.

Can customers have their data hosted in a single data center?

By design, customer data is held within pairs of data centers to provide resilience and be highly available. This approach means it is not possible to host customer data in a single data center. See the **Advanced High Availability eBook** for a detailed description.

Can customers use one of ServiceNow's data centers and pair it with one of their own?

ServiceNow provides leading compliance, security, and availability built on a highly standardized platform. Achieving industry-leading availability and security would not

“ServiceNow operates data centers in North and South America, Europe, United Kingdom, South East Asia, Japan, and Australia.

be feasible, nor technically achievable, using resources outside of ServiceNow's own environment. As such, we do not allow customers to use their own data centers, but customers may choose to export their data into their own environment on a regular schedule.

Is customer data transferred around the world?

No, data always remains in the customer's designated data center pair. Incidental transfers may take place during support or other relevant interactions with ServiceNow. Transfers are made in accordance with customer contractual and relevant legal obligations.

Data backups

How is data backed up, and how often?

For production instances, data is backed up to disk within that instance's data center pair. Sub-production instances exist in and are backed up to a single data center only. Full backups are taken weekly, with incremental backups made daily in between.

How long is backed up data kept?

Backups are maintained for 28 days.

Are backups encrypted?

All instance backups apart from snapshots are encrypted with AES-256. Unique encryption keys are generated for every backup and are kept in a secure keystore. They are retrieved by an automated process only in the event that a data restore is initiated.

Does ServiceNow take tape backups offsite?

Data is backed up to disk, not tape, and remains within the data centers. Production ServiceNow instances are backed up in each data center in a regional pair, each location providing offsite backup storage for the other.

Can customers restore data if they need to?

Customers can restore data if they need to. However, the Advanced High Availability (AHA) Architecture means that restores are only relevant in specific situations, e.g. if a customer accidentally deletes data from an instance. Individual items such as tables or fields can be restored from within the platform. Customer Support can assist in the very rare situation where an entire instance needs to be restored as a last resort.

Encryption

What options are available for customers to encrypt their data?

The Now Platform allows several options for encrypting data at rest. Customers may choose to use:

- *Platform encryption* (previously named column-level encryption) for database fields and attachments
- *Database Encryption* to encrypt all data that resides within the database; data is

only decrypted while it's being accessed

- *Edge Encryption* to encrypt or tokenize data onsite before it's sent to a ServiceNow instance
- *Full Disk Encryption* to protect data in ServiceNow storage in case of loss or theft.

More information is available in the ServiceNow **Data Encryption eBook**.

How is data encrypted in transit?

Data in transit between the customer and ServiceNow is protected with TLS 1.2 . We do not support SSL.

Logging

Can customers see ServiceNow's firewall and infrastructure logs?

Customers are free to access their own instance's audit and monitoring logs, but not those of the wider ServiceNow infrastructure, as this could include other customers' activity. ServiceNow can however, share redacted logs in the case of a security incident.

How long are logs available?

Network logs are retained for a minimum of 90 days, and OS and security logs are maintained for one year.

Testing

Can customers perform load testing?

Customers may perform load testing only by pre-arrangement, and on an isolated environment provisioned specifically for this purpose. This ensures testing can be carried out correctly and without impacting other customers. Please contact your ServiceNow account representative if you'd like to request a load test. **More information** on load testing is available on the Now Support (HI) portal.

Can customers perform a penetration test on their ServiceNow instance?

ServiceNow allows customers to penetration test their instance(s) once per year provided pre-requisites are met and the test is specifically scheduled and authorized via the Now Support (HI) service catalog.

Pre-requisites are detailed as part of the request process, but are primarily that:

1. The target instance must be running the latest update and hotfix set for the supported version, and
2. The instance must be hardened per the **Instance Hardening Settings** and pass pre-testing for all mandatory findings in the Instance Security Center. ServiceNow's **High Security Plugin (HSP)** can be used to assist with hardening the instance.

Customers can schedule a new penetration test through the service catalog via Self-Service > Service Requests > **Schedule A Penetration Test**.

All security testing outside of this process is expressly forbidden.

What should customers do if they discover a vulnerability?

ServiceNow does not condone any attempts to actively audit our infrastructure. However, we recognize that vulnerabilities in our systems, products, or network infrastructure are occasionally discovered incidentally. If you discover a vulnerability, please report it to us in a responsible manner per our **published guidelines**.

Can customers audit ServiceNow?

As a SaaS vendor, and in keeping with common industry practice, ServiceNow invites its own external auditors to undertake regular, comprehensive audits. The results of these audits can be shared with customers, who may self-serve the relevant documents via the ServiceNow CORE portal.

Software updates

Do software updates and patches happen automatically?

The **ServiceNow Patching Program** updates customer instances to required patch versions throughout the year. With this program, instances get the latest security, performance, and functional fixes. Most importantly, patching remediates known security vulnerabilities and is an essential component of any patch management process.

Why do instances need to be patched?

Patches improve reliability, availability, performance, and most importantly, security. Version upgrades bring enhanced functionality, improved appearance and usability, as well as other benefits. Security patches help protect all customers collectively, as well as individually.

When do customers need to upgrade their instances to the latest version?

Major platform version updates are typically released twice per year, with one full patch version each quarter and two incremental security patches each quarter. ServiceNow will notify customers in advance when they should update. Customers must comply with the **ServiceNow Patching Program** to ensure continuous support. ServiceNow provides support for the current release version and one release prior (N-1).

Can customers roll back an update?

All updates, patches and hotfixes undergo extensive and rigorous testing before release to ensure compatibility and reliability. However, should you need to roll back an update for any reason, you can do so by contacting Customer Support within a configurable window (10 days by default).

Customer support

Can standard commercial customers have in-country only support?

For information about a specific ServiceNow in-country cloud offering, please discuss specific support options with your account representative.

US-only support is available for a fee for any entity that requires their support to be exclusively provided by ServiceNow US Citizen/Soil personnel. In all other regions, ServiceNow provides 24/7 customer support using a 'follow-the-sun' model. This entails provision from different global locations throughout the day. These locations are: San Diego, Kirkland, London, Amsterdam, Orlando, Sydney, Hyderabad, Dublin, and Tokyo.

Can customers have dedicated or named support people only?

Qualified personnel are assigned to incidents, rather than individual customers, based on demand and availability. Customers can use the ServiceNow Access Control plugin to control who may access their instance during a specific incident.

A customer may also optionally subscribe to the Support Account Manager service for a dedicated point of contact for support and other relevant matters. Contact your ServiceNow account representative for further information.

> "The ServiceNow Patching Program updates customer instances to required patch versions throughout the year.
>
> Patching remediates known security vulnerabilities and is an essential component of any patch management process.

Mobile applications

What do customers need to know about mobile app security?

ServiceNow has developed new native mobile apps for iOS and Android. These apps use OAuth 2.0 and benefit from the robust authentication mechanisms (optionally augmented with multi-factor authentication) that customers already use with ServiceNow, including SAML, LDAP, and local authentication, along with AppAuth.

Security information on these new mobile applications along with configuration best practices can found **here**.

How can customers control what mobile users can access?

Once authenticated, user sessions are managed with access tokens and mobile users are subject to the same access controls as any other users.

How is mobile app data secured?

All data in transit is protected with TLS and app preference information is encrypted with AES-128. By default, no customer record data is stored on the mobile device, though this is configurable. More information on mobile security can be found **here**.

Administrative procedures

How does ServiceNow onboard/offboard its personnel?

Onboarding: ServiceNow human resources security starts at the very beginning of the employment process with ServiceNow. Mandatory screening includes criminal, employment, financial, citizen checks, and government watch lists, as well as drug tests in jurisdictions that allow it. Failure to pass these tests will result in either mandatory disqualification or a follow-up investigation, depending on the nature of the non-compliance. ServiceNow employs a significant range of detective controls to monitor and prevent potential DDoS attacks from impacting the ServiceNow private cloud environment.

Once employed, any new member of staff must sign a non-disclosure agreement, sign the ServiceNow Code of Conduct and Ethics Agreement, read and accept the ServiceNow Acceptable Use Policy, and undergo security training and compliance training.

Offboarding: ServiceNow has a standard operating procedure that involves both HR and IT. When an employee is departing, HR informs IT of their last day of service and based on their role, IT removes their access. The stated time to do this is within 24 hours of the employee leaving, however, in practice it generally happens much sooner than this.

Can customers perform background checks or other vetting on ServiceNow personnel?

This is not possible due to legal and other obligations towards ServiceNow employees. However, ServiceNow performs extensive background checks and training for our personnel as part of our ongoing compliance accreditations and certifications. Customers may in some circumstances request proof for individuals, for example in the event of a professional services engagement.

Does ServiceNow use subcontractors?

All equipment is owned and managed by ServiceNow and held within ServiceNow-owned and managed cages or suites. This includes servers, network equipment, storage infrastructure, and security solutions. External network connectivity is direct from the provider to our assigned cage/suite, and network traffic does not traverse the hosting data center's network equipment. ServiceNow has a very small number of onsite personnel globally with access to manage our data center equipment.

Does ServiceNow perform vendor security risk assessments (VSRAs)?

ServiceNow performs vendor security risk assessments (VSRAs), and relevant third-party vendors are reviewed for compliance as part of our vendor management program. This process is owned by a dedicated VSRA compliance team, who ensure that the appropriate level of assessment is conducted according to the types of services and assets involved. The compliance team works with the vendors and with internal SMEs to perform the assessment. This results in a vendor risk assessment report, which is reviewed and either approved or rejected by the executive management team.

For more information, customers with access to ServiceNow CORE can review the ServiceNow **Vendor Security Risk Assessment SOP**. Instructions on how to access CORE (customers) and Limited CORE (prospects) can be found **here**.

Compliance and auditing

How can customers find out more about ServiceNow compliance and standards?

Customers can obtain extensive security policy, standards, procedure, and other relevant documents from the ServiceNow **CORE** (Compliance Operations Readiness Evidence) portal. Prospects under NDA may request access to a limited subset of CORE to see evidence of ServiceNow's standards, policies, SOPs, etc.

Instructions on how to access CORE (customers) and Limited CORE (prospects) can be found **here**.

Can I see your information security policy documentation?

Yes, if you are a customer. ServiceNow has a very detailed set of information security policies and standards that are based on ISO 27001 and assessed as part of this certification. ServiceNow's information security policy is reviewed and approved by the CISO at least annually and is owned by the director of governance, risk management, and compliance at ServiceNow. Prospective customers are able to access the table of contents of specific policies and standards after registering for **Limited CORE**.

Is ServiceNow PCI DSS certified?

ServiceNow is not a transaction processor, brand, merchant, or service provider in accordance with PCI terms, and therefore is not PCI DSS certified. However, many of the criteria are already met through our other accreditations, e.g. ISO27001, SOC, etc. Customers who consider ServiceNow part of their scope can work with their QSA to scope and assure appropriately using our standard assurance material.

Does ServiceNow comply with data privacy laws like the GDPR, CCPA, and others?

ServiceNow is **an advocate** of consumer privacy rights.

Our **Data Processing Addendum ("DPA")** outlines how we process personal information only to the extent necessary to provide our products and services, and describes the privacy and security measures in place.

ServiceNow is committed to GDPR compliance across our enterprise cloud services. In the context of customer instances of the Now Platform, GDPR compliance is also a shared responsibility between ServiceNow and its customers. Guidance in this respect is available in the whitepaper **Complying with the General Data Protection Regulation (GDPR)**.

Similarly, the CCPA focuses on data privacy for residents of the state of California. ServiceNow is considered a "service provider" under the CCPA. Our **DPA** addresses the CCPA's requirements for data privacy and information security.

> "ServiceNow is committed to GDPR compliance across our enterprise cloud services. We believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights.

Miscellaneous questions

How do customers find their instance IP address?

Customer instances use IP addresses from an 8-address (/29) subnet. You can use the Now Support (HI) portal to **identify the addresses** allocated, along with other useful information.

Can customers install their own hardware or software in the ServiceNow cloud?

As is the case with most cloud providers, it is not possible for customers to install their own hardware or software in the ServiceNow cloud. Instances of the Now Platform are delivered using a completely standardized cloud infrastructure. The entire environment is under the complete control and management of ServiceNow on behalf of its customers. Now Platform instances are very flexible and can be configured and customized as required, including the use of customer-generated code.

Does ServiceNow have a disaster recovery plan?

ServiceNow operates a disaster recovery (DR) program for customer environments called the information system contingency plan (ISCP). In the event of a disaster, ServiceNow activates a failover process that transfers customer operations to the unaffected data center. In this model, the targeted recovery point objective (RPO) and recovery time objective (RTO) durations are one and two hours, respectively.

The ISCP is tested annually and the results are documented in the ICSP test report. The exercise scenarios are designed to test Advanced High Availability (AHA) failover to a secondary data center as well as recovery from backup. These procedures are often completed well within expected RPO and RTO windows as transfers between data centers are also performed for maintenance purposes, making this a highly practiced process for ServiceNow.

The latest **ServiceNow Information System Contingency Plan Test Report** can be found in ServiceNow CORE. Instructions on how to access CORE can be found **here**.

What happens to a customer's data if they stop being a customer?

ServiceNow will make a customer's data available to them within 30 days of contract termination. This will be in an industry standard format, by means of a database dump.

After that time, data is securely removed.

How do customers access their database dump?

Customers can only obtain your data by downloading it from our secure file transfer service, which uses FTPS to keep the transmission secure. No other method is available.

What is ServiceNow's data destruction process?

ServiceNow logically sanitizes mechanical and solid-state drives (SSD) prior to re-use.

We follow a data sanitization standard operating procedure (SOP) to destroy data on mechanical disks. This process is consistent with NIST 800–88, Guidelines for Media Sanitization, and NISP Operating Manual (NISPOM) DOD 5220.22–M. Where mechanical or SSD disks are unable to be logically sanitized, i.e. due to failure, they are physically destroyed.

Drives to be destroyed go through a process that follows NIST 800-88 standards, is performed by a specialist destruction vendor, and is overseen by ServiceNow personnel. A certificate of destruction is produced for each destruction event, and each destroyed drive is recorded.

How can customers communicate with ServiceNow?

All communication between ServiceNow and its customers is conducted via the Now Support (HI) service portal or your support account manager (SAM) if you have one. This ensures that your queries are captured, prioritized, and routed immediately, without reliance on individual availability.

Resources

There is a wealth of information available online in the following publicly accessible locations:

- **Product Documentation**
- **Community Support**
- **ServiceNow Trust Site**

Existing customers can also access the following resources:

- **CORE**
- **Trust and Compliance Center**
- **General Technical Support**
- **ServiceNow Security Best Practice Guide**

servicenow