servicenow

Cloud security FAQ

The ServiceNow Trust Journey

servicenow

Table of contents

servicenow

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 detail can be found at: https://docs.servicenow.com.

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 ServiceNow cloud infrastructure?

Only ServiceNow personnel with a defined and approved support role may access the cloud infrastructure. Access is via an IPSEC VPN with two-factor authentication and is only possible from ServiceNow-owned and managed equipment. All accesses are logged, and quarterly reviews are undertaken.

Data residency

Where is my data stored?

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 and England), Japan, Australia and Brazil.

Can I have my data stored 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 Delivering Performance, Scalability and Availability eBook for a detailed description.

Can we use one of your data centers and pair it with one of ours?

ServiceNow provides leading compliance, security, and availability built on a highly standardized platform. Achieving industry-leading availability and security would not 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 my data transferred around the world?

No, the data always remains in the 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 obligation and, where relevant, under the terms of the US Privacy Shield Framework.

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, as described above.

Are backups encrypted?

Data is backed up in the same state as in the source customer instance, i.e. plain text or encrypted data remains as-is. No additional encryption is added at rest.

Do you take your tape backups offsite?

No; data is backed up to disk, not tape, and so remains within the data centers.

Can I restore data if I need to?

Yes, however, the Advanced High Availability (AHA) Architecture means that restores are rarely needed, e.g. if a customer accidentally deletes data. 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.

Encryption

What are my options if I want to encrypt my data?

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

- *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 into ServiceNow, or
- *Full Disk Encryption* to protect data in ServiceNow storage in case of loss or theft.

More information is available in the ServiceNow Encryption Technical Summary White Paper supplied with the SNAP and the Data Encryption eBook.

What about data in transit?

Data in transit between the customer and ServiceNow is protected with TLS 1.2[1]. We do not support SSL.

Logging

[1] ServiceNow is deprecating TLS versions 1.0/1.1 through Q1 2020

Can we see your 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 the logs available?

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

Testing

What if I want to perform load testing?

You may do so; however, this must be arranged with our professional services team in advance to ensure tests are carried out correctly and without impacting other customers. More information is available in this document: ServiceNow Load Testing Service Description.

What about security penetration testing?

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 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 Guide and pass pre-testing for all mandatory findings in the Instance Security Dashboard (Jakarta, Kingston, London releases) or Instance Security Center (Madrid release onwards). 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 do I do if I 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 we audit ServiceNow?

As a SaaS vendor, and in keeping with many other vendors, ServiceNow invites its own external auditors to complete regular comprehensive audits, the results of which can be shared with customers. ServiceNow allows self-serve auditing via the CORE facility described above.

Software updates

Is our instance evergreen? Do software updates 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 I need to update my instance?

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

How long should I wait before updating?

Major platform 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 will support the current version and one release prior (N-1).

Customer support

Can I have in-country only support?

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 I 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 sales representative for further information.

Mobile Apps

What do I 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 do I 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 app data secured?

All data in transit is protected with TLS and app preference information is encrypted with AES128. By default, no customer record data is stored on the mobile device, though this is configurable.

Administrative procedures

What is your HR onboarding/offboarding process?

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 we perform background checks or other security vetting on ServiceNow employees?

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.

Do you 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.

Do you perform vendor security risk assessments (VSRAs)?

Yes. All 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, please review the ServiceNow Vendor Security Risk Assessment SOP, which is available in CORE.

Compliance and auditing

How do I find out more about ServiceNow's security compliance and standards?

As a customer, you can find extensive compliance documentation including ISO 27001, ISO 27017:2015, ISO 27018:2014, SSAE18/SOC accreditation, and our latest penetration test reports within CORE, our compliance and operations portal. As a prospect under NDA, you may request access to a limited subset of CORE to see evidence of ServiceNow's standards, policies, SOPs, etc. To request access to CORE or Limited CORE, please contact your ServiceNow representative.

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.

Are you PCI DSS Certified?

No. ServiceNow is not a card payments company in itself, so we have not sought nor will seek compliance. 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.

What about the GDPR?

The General Data Protection Regulation (GDPR) is principally about protecting and enabling the privacy rights of EU citizens. The GDPR establishes global privacy requirements governing how you manage and protect personal data while respecting individual choice, regardless of where data is sent, processed, or stored.

At ServiceNow, we believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. We also understand that GDPR compliance is a shared responsibility. This is why ServiceNow is committed to be GDPR compliant across our enterprise cloud services.

More information on this topic is available in the whitepaper Preparing for the GDPR.

Miscellaneous questions

Which IP addresses does my instance use?

Your instance is uses addresses from an 8-address (/29) subnet. You can use the HI support portal to identify the addresses allocated, along with other useful information.

Can we install our own hardware or software?

As is the case with most cloud providers, this is not possible. As a SaaS solution, instances of the Now Platform are delivered using a completely standardized hardware and software infrastructure. The entire environment is under the complete control and management of ServiceNow, as the vendor and cloud services provider. Now Platform instances are very flexible and can be configured and customized as required, including the use of customer-generated code.

Can you describe your 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 ISCP test was completed in January 2019. Details of the tests are available to customers in CORE: ServiceNow Information System Contingency Plan Test Report.

What happens to my data if I 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 I access my database dump?

You 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 your data destruction process?

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

Drives that are to be replaced or decommissioned go through a process overseen by ServiceNow personnel. A certificate of destruction is produced for each drive. The destruction follows NIST 800-88 standards.

Who are useful contacts and how do I reach them?

All contact is conducted via the HI service portal or your support account manager. 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 Security Best Practice Guide

Existing Customers can also access:

- CORE
- Trust and Compliance Center
- General Technical Support