servicenow

Compilation of all articles from the Knowledge Base

Trust, Privacy & Compliance

at support.servicenow.com

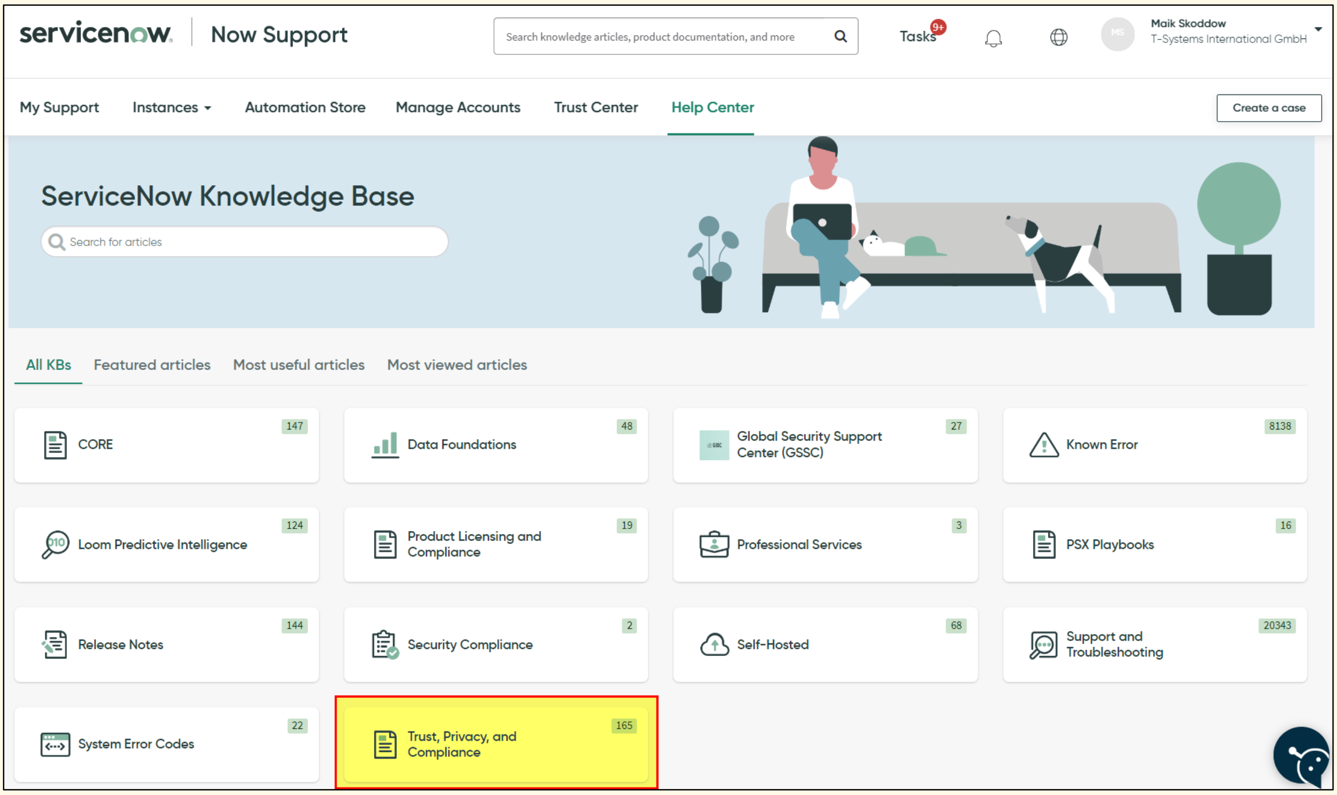
assembled by Maik Skoddow, 2023

Purpose

ServiceNow's support portal at support.servicenow.com is your launchpad to access self-help content, get technical support, and manage your ServiceNow instances.

Many of the knowledge articles stored there are public and can therefore be viewed without having an account. However, access to these articles via the Knowledge Base catalog is only allowed for logged-in users, which is why the Knowledge Base "Trust, Privacy and Compliance" and its over 160 articles remains hidden for most users. But this is a great pity, because this knowledge base is a real treasure and anyone who has direct discussions with ServiceNow customers or other stakeholders should know its contents. You can find answers there for typical questions like "*Does ServiceNow comply with data privacy laws such as the GDPR, CCPA, and others?*" or "*Who has access to customer data?*" In addition, the content articles provide deep insights into how ServiceNow operates its cloud infrastructure and what standard processes are followed behind the scenes[1].

For this reason, I have extracted all the articles[2] and compiled them into this document. That way it is hopefully easier to consume them and search for specific content.



[1] ServiceNow does offer a document "Cloud Security Frequently asked Questions", but this is only an excerpt from the Knowledge Base, as it does not contain its content articles and all the valuable further links

[2] The original articles can be reached via the linked article numbers below the headlines.

Topics

Accessing Data

Contents

ServiceNow's access to customer data

KB0959603

Occasionally, ServiceNow employees may be required to access a customer’s instance to provide support. This is done on an incidental, per-event basis, and not every customer support event will require access to customer data.

Only members of ServiceNow’s support organization who have been specifically assigned to an active incident can be granted access, and that access is granted on a just-in-time basis. Additionally, customers may specify that their explicit authorization is also required when that access is requested.

Access can only be gained via a secure virtual desktop environment accessible only from ServiceNow data centers, requiring a client device authenticated by a digital certificate. Users are required to pass two-factor authentication before access is granted. Host-based data leak prevention (DLP) is enabled, SSH access to production servers is controlled using a proxy, and all user activity is controlled and monitored with a privileged access management (PAM) system.

More information

- Find out more about Data Access Controls and ServiceNow's Access Control Plugin
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Who has access to customer data?

KB0960191

Customer data can be accessed via both the application and the infrastructure. Customers can control access to their data at the application layer via Access Control Lists (ACLs). Default ACLs are available out-of-the-box and can be customized to suit.

ServiceNow does not require access to customer data via the infrastructure layer during normal service provision. However, if issues arise which cannot be resolved by the platform's automation capabilities, a ServiceNow Cloud Administrator may need to access servers or database systems for investigation and resolution. All activity of this type is logged.

ServiceNow support representatives may need access to a customer's instance to resolve customer-raised issues. Any such application layer access is recorded in the system logs and identified with a username ending in '@snc'.

Customers may prevent application layer access by ServiceNow by enabling the ServiceNow Access Control (SNAC) plug-in. SNAC requires explicit approval to be given by the customer before instance access is allowed. Enabling SNCA will delay progress on support activities requiring instance access until the customer grants access.

Multiple preventative and detective controls have been implemented to prevent unauthorized access to infrastructure. These are documented in the SOC 2 Type 2 report which is available to customers in the CORE compliance portal.

More information

- Find out more about Data Access Controls and ServiceNow's Access Control Plugin
- Find out more about ServiceNow Access Control (SNAC)
- Customers can access ServiceNow's Entitlement Review SOP

How do ServiceNow employees access the cloud infrastructure?

KB0960198

Only ServiceNow personnel with a defined and approved support role may access the cloud infrastructure. Access is via regionally deployed, secure virtual desktop environments, and requires two-factor authentication from clients within ServiceNow address space, identified by ServiceNow-issued digital certificates.

- All access is logged, monitored, and controlled by ServiceNow's 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
- All SSH access is controlled using a proxy and activity is logged, monitored, and controlled by our PAM system
- Quarterly privilege reviews are undertaken for all relevant personnel

More information

- Find out more about Data Access Controls and ServiceNow's Access Control Plugin
- Find out more about ServiceNow Access Control (SNAC)
- Customers can access ServiceNow's Entitlement Review SOP

Customer access to data

KB0959602

As the data controller, the customer determines who has access rights to their instance and the data stored in it. As the data processor, ServiceNow provides the tools for customers to secure and audit their instance according to their requirements. In general, ServiceNow does not access customer data, but it is sometimes necessary during the course of resolving customer support tickets.

More information

- Find out more about Data Access Controls and ServiceNow's Access Control Plugin
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Administrative Procedures

Contents

How does ServiceNow onboard/offboard its personnel?

KB0960239

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 noncompliance. ServiceNow employs a significant range of 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 annual 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.

More information

The following resources are accessible by ServiceNow customers only:

- IT Support Onboarding, Role Change, and Offboarding SOPs
- HR Support Onboarding and Offboarding SOPs
- Background Screening SOP
- Training Policy
- Training SOP

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

KB0960240

It is not possible for customers to perform background checks or other vetting on ServiceNow personnel 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.

More information

The following resources are accessible by ServiceNow customers only:

- IT Support Onboarding, Role Change, and Offboarding SOPs
- HR Support Onboarding and Offboarding SOPs
- Background Screening SOP
- Training Policy
- Training SOP

Does ServiceNow perform vendor security risk assessments (VSRAs)?

KB0960250

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 vendor security risk assessment (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.

More information

Customers can access ServiceNow's Vendor Security Risk Assessment SOP for more information.

Asset Data

Contents

Managing asset data

KB0959807

Asset data refers to both direct and related information about an asset, security event data, vulnerability information, stored credentials for discovery and orchestration, and other similar data types.

ITIL is a globally recognized best practice framework for information technology service management (ITSM). This framework recommends the use of a software-based configuration management system (CMS) to manage infrastructure and asset data.

The CMS contains information about configuration items (CI), such as physical or virtual computer systems, network infrastructure devices, printers, mobile devices, and installed software. This, together with related information, forms a configuration management database (CMDB). The accuracy and integrity of CI data is critical for effective ITSM.

Within a customer instance of ServiceNow, the CMDB is a single, authoritative source of customer infrastructure and asset data. It can be integrated with other systems and processes to enable services such as an IT help desk or capacity and performance management. Other uses include ServiceNow's service mapping function, and vulnerability response application.,

More information

Find out more about how ServiceNow Safeguards Customer Data

Data used for machine learning and artificial intelligence

KB0959810

Training and prediction data never leaves the data center (DC) and is transferred between instances and their local dedicated machine learning (ML) servers over HTTPS. Customers determine what data is sent to the ML trainer when they define what to learn, and the scope, e.g. the data from 6 months of closed tickets and short descriptions. These configurations are recorded and available for audit. Once the system training is completed and a training model is returned to the requesting instance, the data and model are deleted from the training and prediction server. No human intervention occurs throughout the process. ML is also used in natural learning understanding (NLU), which powers the virtual agent. NLU uses the same prediction infrastructure, but in this case, customers create models of 'intents' along with associated 'utterances' (e.g. voice commands to open a ticket). No customer data is used other than the utterances themselves.

The DART program (Data Access for Responsible Training)

ServiceNow has introduced the DART program to help accelerate and refine the development of Now Intelligence. This brings the benefits of automation, anomaly detection and prediction to the platform, improving the customer experience and resulting in a faster time to resolution. Features such as artificial intelligence (AI), natural language understanding (NLU), and machine learning (ML) must be tested and optimized during development. This is most effectively done using real–rather than synthetic–datasets. The DART program enables ServiceNow to test Now intelligence algorithms against data stored in temporary clones of customer instances. Customers are automatically enrolled into the program when their contracts are renewed, but retain complete control over the use of their data and are free to start, pause, or stop their participation at any time. Customers' DART clone is deleted when they leave the program. DART clones and the associated Now intelligence infrastructure are all deployed within a carefully controlled, isolated, and secure environment. Only a select, authorized, subset of ServiceNow employees can access the environment – and only from company-provisioned devices via VPNs that are authenticated by multifactor authentication (MFA). It is not possible for DART clones and infrastructure to connect to other instances or to the Internet. There is no data commingling, and the clones are not backed up.

More information

Find out more about how ServiceNow Safeguards Customer Data

Storing CMDB data and related information in the cloud

KB0959808

A common concern over storing asset and related information in the cloud is that if compromised, internal IP & MAC addresses, host names, software/firmware versions, or locations of systems or services could be used maliciously to identify vulnerabilities and enable attacks against the infrastructure. These risks are often overstated, since access to the internal network is required before the data can be used. Skilled attackers would be able to easily determine this information for any network they had compromised by themselves, without the need to first attack a secure CMDB.

Nevertheless, ServiceNow understands the sensitivity and importance of CMDB data, and that it should remain available and accurate at all times. So ServiceNow employs an array of security features to protect the confidentiality, integrity, and availability of this data. More information about these controls is available in Securing the Now Platform.

More information

Find out more about how ServiceNow Safeguards Customer Data

ServiceNow orchestration and discovery

KB0959809

ServiceNow's management, instrumentation, and discovery (MID) servers allow secure controlled communication between customer instances and their internal network services. MID Servers are installed and configured by customers in order to operate entirely within their infrastructure.

As with any other enterprise endpoint deployed by a customer, MID server activities can be limited using network and administrative controls, including credential management systems. MID servers run commands generated on the ServiceNow instance by appropriately credentialed customer administrators and then placed in a fully auditable event queue that can be inspected and monitored in real-time using built-in features. Restrictions can be placed on the commands used, and on the rights of individuals to see and modify them.

Events are retrieved every 15 seconds via a secure transport layer security (TLS) channel between the MID server and its cryptographically paired parent instance. Credentials provided locally or passed along with the command are used to issue the command and record any response. Response data is returned to the instance and stored appropriately.

More information

- Find out more about the ServiceNow MID Server
- Find out more about how ServiceNow Safeguards Customer Data

Authentication & Authorization

Contents

Authorization

KB0959606

Customers have full control of entitlements granted to each of their users in a ServiceNow instance.

A ServiceNow instance includes a built-in role-based access control (RBAC) mechanism providing user, group, and role objects. These can be used by customers to assign access to applications and data within their instances. Customers can add additional users, groups, and roles to those already defined.

Access control lists (ACLs) are used in conjunction with RBAC to control access to entire tables, records, or fields. A number of default ACLs exist in an out-of-the-box ServiceNow instance. Customers can add to those per their own requirement.

ACLs comprise individual entitlements which include create, read, write, and delete. In addition, access can be further controlled on a contextual basis, depending on individual attributes of the object being accessed. These attributes could include the state of a specific kind of record, the value of a field, or even the day, date, or geographic location of the end users. The attributes available also vary, depending on the type of object being secured.

Because integration with a customer's own directory services is possible, existing users and groups in those directory services can be used to manage users and access within the customer's ServiceNow instance(s).

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

High security settings plugin

KB0959608

ServiceNow’s High Security Settings plugin provides advanced security options for instances of ServiceNow and is enabled in all new instances. This plugin cannot be disabled. Security features enforced by the plugin includes the ‘default deny’ access mode, enables access control rules, and provides elevated access functionality and security-related roles for a customer’s administrators.

The settings also include a number of out-of-the-box security-related properties. Customers may access and enable these from a single page in their instances. For example, restrictions can be set on the nature and type of attachments that can be uploaded into the instance, how those attachments behave when downloaded, and other hardening attributes.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Customer access management

KB0959607

ServiceNow customers are responsible for the management of user identities within their instances. This includes the creation of individual identities (credentials) for each of their users, both internal and external, the methods used to authenticate those users, password policies (for built-in authentication), and the entitlements and access levels granted to those users.

User identity synchronization

A ServiceNow instance requires every user to exist as an identity within the database, regardless of authentication mechanism. This identity is necessary to support a wide variety of capabilities within the product, including for role-based access purposes.

To facilitate this requirement, ServiceNow instances support both automated and manual creation of user identities. This includes synchronization of users, their group memberships, and those group objects themselves. Customers may incorporate as few or as many user attributes as they deem necessary. However, user object passwords cannot be synchronized.

A common approach to maintaining identity data is for customers to use their own LDAP directory. This would be configured in an import set as a data source for user and group objects. This then allows synchronizing the information in customers' ServiceNow instances with that in their own directory service. Customers specify the interval or regularity of synchronization per their own requirements. This would usually be daily as a recommended minimum.

Customers may also leverage the ServiceNow MID server component for LDAP synchronization. This component negates the need for customers to allow their ServiceNow instances through their perimeter and firewall in order to access their internal directory servers. Instead, customers can install the MID Server inside their internal network from where it can access the directory server and return a payload of users or groups and their attributes to the customers' instance. These would then be automatically imported or updated in the target user or group tables within the instance.

User and group objects can be uploaded into a ServiceNow instance through the use of import sets. These can use various types of data sources for user and group objects intended for use with a ServiceNow instance. This process is commonly used for initial user uploads to populate the ServiceNow user and group tables in a customer's instance, but it can also be used for ongoing synchronization of these tables. Customers can also simply import a flat file exported from the chosen authoritative identity source.

If a user exists in a customer's IdP but is not in the customer's ServiceNow instance, SAML user provisioning can automatically create the user in the instance.

System for Cross-Domain Identity Management (SCIM) is also supported. This allows customers to easily provision and manage user identities, group membership and other properties from external sources 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 customers from having to create and manage multiple customized SOAP APIs.

More information

- Find out more about Data Access Controls and ServiceNow's Access Control Plugin
- Find out more about the ServiceNow MID Server
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Which authentication methods are available to customers?

KB0960194

Customers can utilize built-in authentication methods, including:

- Multi-provider SSO
- SAML 2.0
- LDAP
- OAuth 2.0, and others

More information

Find out more about authentication and enabling password policies.

Authentication

KB0959604

A ServiceNow instance provides a customer with a number of authentication options that can be used simultaneously within an instance, using a multiple authentication model.

Security Assertion Markup Language (SAML) for Single Sign-On (SSO)

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains. SAML exchanges security information between an identity provider (a producer of assertions, commonly abbreviated to IdP), and a service provider (a consumer of assertions).

The ServiceNow SAML 2.0 integration enables single sign-on by exchanging XML tokens with an external IdP. The identity provider authenticates the user and passes a NameID token to the ServiceNow instance. If the instance finds a user with a matching NameID token (e.g. the email address), the instance logs that user in.

The ServiceNow SAML plugin supports SSO-based authentication via a variety of SAML-compliant identity providers. This includes Active Directory Federation Services (ADFS), as well as third-party identity providers such as Ping, SecureAuth, SailPoint, Okta, or any that are compliant to the SAML 2.0 standard.

Customers who implement their own SAML compliant IdP or opt for a third-party service can then also leverage this with other cloud services. When customers elect to use the SAML plugin, their password and credential policies are governed by their own IdPs.

Lightweight Directory Access Protocol (LDAP)

LDAP authentication lets customers use their own LDAP-compliant directory services, such as active directory (AD) or similar. Customers who elect to use their own LDAP directories have their password and credential policies governed by the policies set within these. A directory needs to be accessible to the relevant ServiceNow instance because these are commonly located

behind a firewall or other perimeter controls. Multiple directory service sources may be configured and secure LDAP (LDAPS) is also supported.

With an LDAP integration, authentication paths commence with end users providing their username and password to the customer’s ServiceNow instance. These credentials are then used by that instance to perform a simple bind against the customer’s target directory service for that user. If successful, the user will be authenticated to the relevant ServiceNow instance.

As part of the LDAP integration, passwords are neither stored nor transferred back to the customer’s ServiceNow instance.

Built-in “native” authentication

In the case of native authentication, passwords are managed solely by customers within their ServiceNow instance(s). This is the only authentication method where both the username and password are stored within a customer’s instance (as a 1-way SHA-256 hash with an appropriate salt value).

When using native ServiceNow authentication, properties such as the length, complexity, rotation, and uniqueness of passwords are customizable by a customer.

OAuth 2.0

OAuth 2.0 allows customers to access instance resources through external clients by obtaining a token rather than by entering login credentials with each resource request. OAuth 2.0 is implemented in the Now Platform for the following scenarios:

Auth external client scenario	Auth provider scenario
A customer’s instance provides an endpoint for third-party clients to pull data from the instance.	A customer’s instance pulls data from a third-party provider.

More information

- Find out more about authentication and enabling password policies.
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

What password policies can customers use?

KB0960196

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

More information

Find out more about authentication and enabling password policies.

Availability

Contents

Advanced high availability (AHA) overview

KB0959443

ServiceNow's data centers and cloud-based infrastructure are designed to be highly available with redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the internet from different providers and with redundant power sources.

ServiceNow's data centers are arranged in pairs, with all customer production data hosted in both data centers simultaneously and kept in sync using asynchronous database replication. Both data centers are always active in a main-main relationship with data replicated from the active (read-write) data center to the passive (read-only) data center. Each single data center in a pair is implemented so it can support the combined production load of both locations.

Within each regional data center pair, there is no concept of a fixed primary location for any customer instance. For example, a customer with two separate instances could have them operating out of different data centers simultaneously.

We leverage AHA for customer production instances for the following purposes:

- Prior to executing maintenance, ServiceNow can proactively transfer operation of a customer instance from one data center to the other. The maintenance can then proceed without impacting service availability.
- In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of the affected instance to the other data center.

With this approach, the transfer between active and standby data centers is regularly executed as part of our standard operating procedures. This ensures that when it is needed to address a failure, the transfer will be successful and service disruption is minimized.

More information

- Find out more about ServiceNow's Advanced High Availability Architecture
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Business continuity and disaster recovery

KB0959447

ServiceNow is divided into two distinct environments for the purposes of business continuity (BC) and disaster recovery (DR). ServiceNow's corporate IT environment and its cloud data centers are both physically and logically isolated from each other. A disaster affecting ServiceNow's corporate environment could occur with little or no impact on the ability for the data centers within the private cloud to continue to operate. In both cases, the BC and the DR procedures are supported by a series of tested processes, automations, and supporting documentation, allowing ServiceNow to quickly and effectively take action when availability of its cloud or critical supporting services are affected.

Execution

ServiceNow's Information System Contingency Plan (ISCP) covers its cloud data center environments. Its scope includes all customer instances of the Now Platform, as well as those ServiceNow uses internally as an organization to support its business. The ISCP uses ServiceNow's Advanced High Availability (AHA) architecture.

Testing and compliance

ServiceNow formally tests its recovery processes on an annual basis and can produce reports relating to this for customer review. ServiceNow also uses the process of transferring instances for maintenance purposes on a daily basis. As a result, ServiceNow is very well practiced at the process of "failing over" or transferring customer instances.

Organizational business continuity

ServiceNow's organizational business continuity process covers its corporate environment and functional offices. It is therefore a separate process from that used in its cloud environment. The business continuity plan (BCP) has been developed in collaboration with the entire business and includes ongoing Business Impact Assessments (BIA) to understand the impact of the loss of any given systems, services, or physical locations.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Corporate Business Continuity Management Policy
- Information System Contingency Plan (ISCP) and Test Report
- Backup and Restoration SOP

Performance and scalability

KB0959621

Our cloud scales to meet the needs of the largest Global 2000 enterprises, with tens of thousands of customer instances operating in our globally distributed data centers. All instances are deployed on a per-customer basis, allowing the multi-instance cloud to scale horizontally to meet each customer's performance needs. Customer instances perform an aggregate of tens of billions of full-page transactions every month, and customers using the ServiceNow configuration management database (CMDB) as their single system of record may manage tens of millions of configuration items (CIs).

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Find out more about ServiceNow's Advanced High Availability Architecture

Critical resources

KB0959622

ServiceNow is responsible for managing its environment, the supporting infrastructure, and vendor relationships. As part of these responsibilities, ServiceNow's site reliability engineering (SRE) center employs a follow-the-sun model that provides continual security, operational monitoring, and support of the ServiceNow environment and infrastructure. ServiceNow rotates operations and technical support daily in North America, the UK, India, Australia, Netherlands, Japan, and Ireland.

Critical system resources, including DNS, email, ServiceNow's cloud operations systems, and customer service system are operated in high availability configurations in a minimum of two data centers. None of these resources rely upon ServiceNow's internal corporate IT infrastructure.

ServiceNow uses AHA for its own development systems, including managing source code control and the software build process, that are also hosted at the production data centers. This ensures the highest continuity for our developers, enabling them to continue to develop and support the application without requiring physical access to ServiceNow offices.

The AHA architecture uses the same transfer process for preventive maintenance and recovery from natural disasters. This approach eliminates the need for a yearly disaster recovery test and creates a practiced transfer event during the performance of normal maintenance.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Find out more about ServiceNow's Advanced High Availability Architecture

Data backup and recovery

KB0959446

ServiceNow's Advanced High Availability (AHA) architecture is the primary means to restore service in the case of a disruption that could impact availability. However, in certain scenarios, it may be desirable to use more traditional data backup and recovery mechanisms. Such circumstances could be, for example, where a customer deletes some data inadvertently, or where a customer's data integration or automation is misconfigured or malfunctions, resulting in data being rendered unusable or inaccessible. In these scenarios, the high availability capability would not assist and restoring from backup is the only option for recovery.

Full backups are performed every seven days direct to disk and are retained for 28 days, with differential backups taken every 24 hours. Backups are stored in the same data centers where the data resides, with production instances backed up in both data centers in the pair. Sub-production instances (commonly used for testing and development purposes) are backed up only in their primary data center, as they are not AHA capable.

All backups are written to disk; tapes and removable media are not used. Backups are not sent offsite, but they are made within both data centers in a pair, therefore benefitting from geographic separation.

Backups are encrypted with AES-256 using randomly generated encryption keys for every backup. These are kept in a secure key store. And it is only retrieved by an automated process if a data restore is initiated. Regular, automated tests are run to ensure the quality of backups, and any failures are reported for remediation within ServiceNow.

The ServiceNow backup architecture is not designed to provide archival records, given the maximum 28-day backup retention period. However, customers may retain data within their instances for as long as they require in accordance with their policy or regulatory requirements. Additionally, there are capabilities available within the Now Platform to allow customers to manage logs and regularly export data to external systems, as required.

More information

- Find out more about ServiceNow's Advanced High Availability Architecture
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Does ServiceNow have a disaster recovery plan (DRP), and what are the target recovery point objective (RPO) and recovery time objective (RTO) durations?

KB0960262

ServiceNow operates a disaster recovery program for customer instances 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.

A separate business continuity plan and processes are in place to ensure availability for the ServiceNow corporate organization and the services it relies on. This is also tested on an annual basis.

Does ServiceNow take tape backups offsite?

KB0960210

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?

KB0960212

Customers can restore data if required. 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.

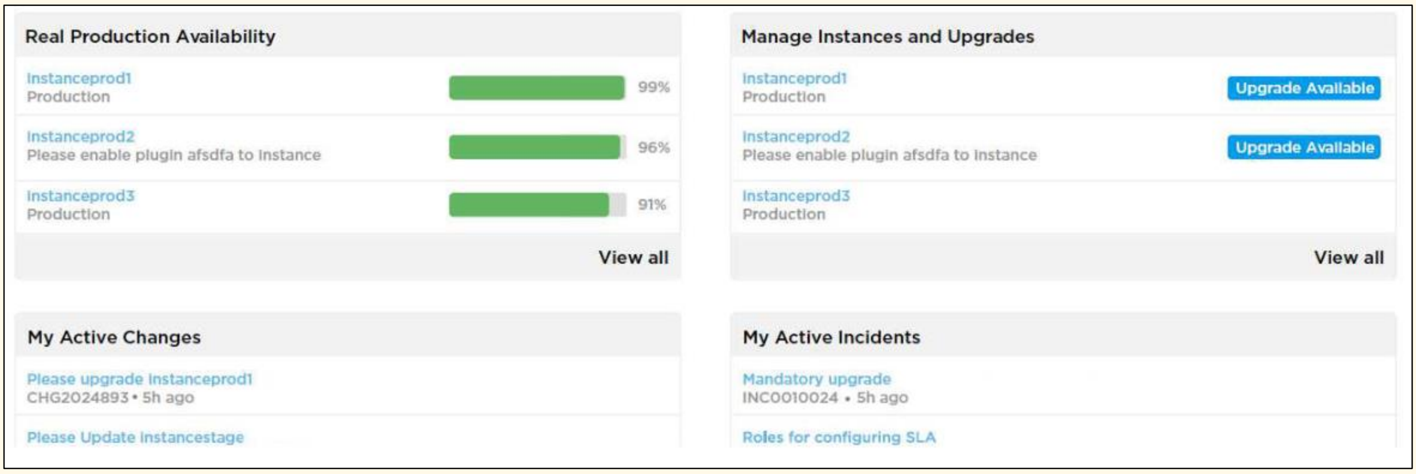
More information

Find out more about ServiceNow's Advanced High Availability Architecture

Real availability dashboard

KB0959620

We provide a real availability dashboard that displays availability information for all of a customer’s instances, providing a true measure of customer availability.



Real Production Availability

Instanceprod1
Production 99%

Instanceprod2
Please enable plugin afsdfa to instance 96%

Instanceprod3
Production 91%

View all

Manage Instances and Upgrades

Instanceprod1
Production Upgrade Available

Instanceprod2
Please enable plugin afsdfa to instance Upgrade Available

Instanceprod3
Production

View all

My Active Changes

Please upgrade instanceprod1
CHG2024893 • 5h ago

Please Update instancestage

My Active Incidents

Mandatory upgrade
INC0010024 • 5h ago

Roles for configuring SLA

More information

Find out more about ServiceNow's Advanced High Availability Architecture

How is data backed up, and how long is backed up data kept?

KB0960207

Production instance data is backed up to disk in both data centers in the regional pair where that instance is hosted

Sub-production instances exist in a single data center, and are backed up in that data center only

Full backups are taken weekly, with incremental backups made daily in between

Backups are maintained for 28 days.

More information

Find out more about ServiceNow's Advanced High Availability Architecture

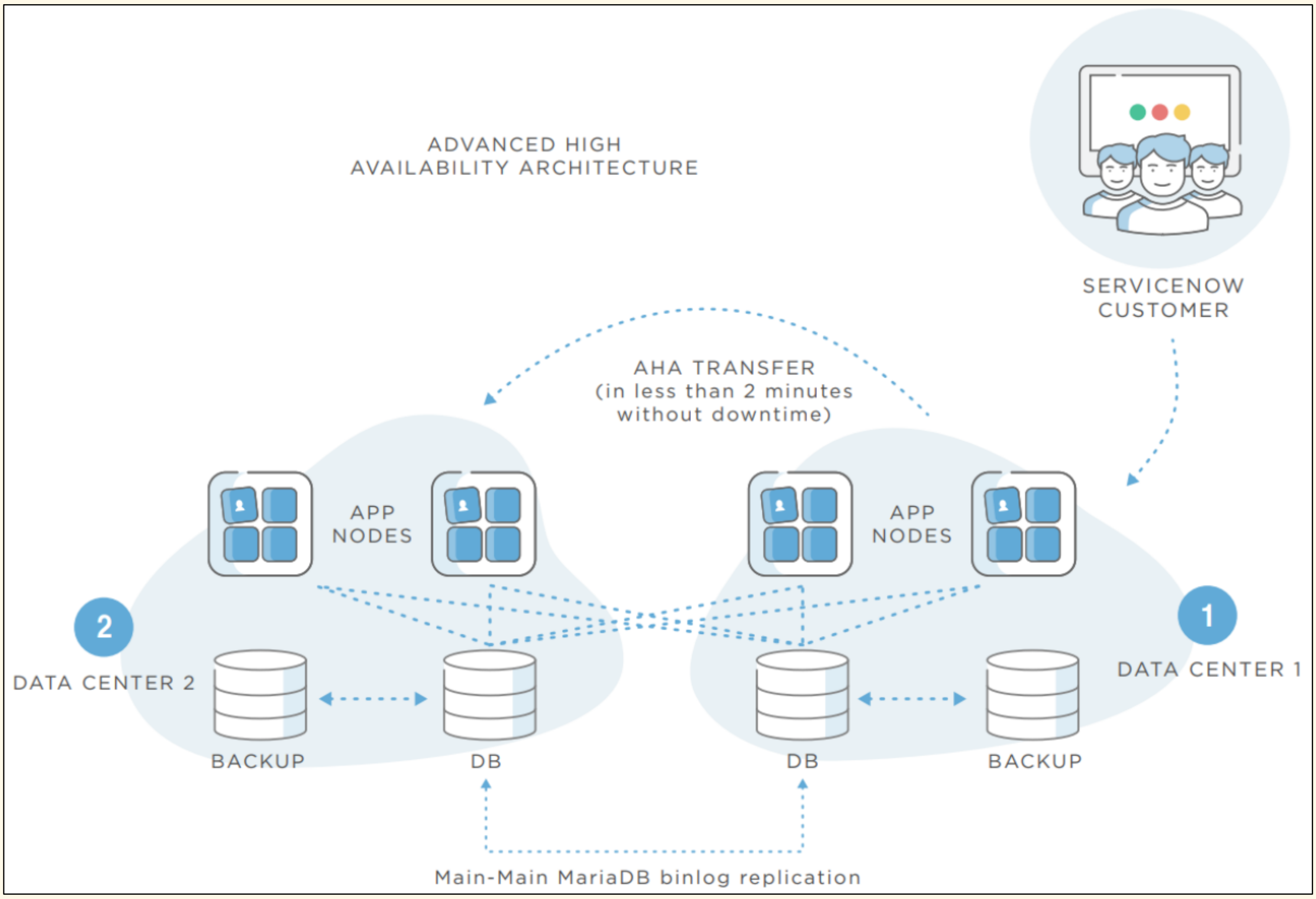
Transfer and failover

KB0959444

ServiceNow has two distinct processes related to ensuring instance availability: transfer and failover.

Transfer

A transfer of an instance is a scheduled event, usually performed for maintenance purposes and always coordinated with a customer. These outages occur within the contracted availability service level agreement that ServiceNow commits to with its customers.


ADVANCED HIGH AVAILABILITY ARCHITECTURE
SERVICENOW CUSTOMER
AHA TRANSFER (in less than 2 minutes without downtime)
APP NODES
APP NODES
2
DATA CENTER 2
1
DATA CENTER 1
BACKUP
DB
DB
BACKUP
Main-Main MariaDB binlog replication

Failover

A failover of an instance is an event usually performed where availability for one or more customer instances cannot be maintained. This could be down to a local component failure, or an event such as a major environmental incident or resource outage

In the case of a local component failure, a failover to a system within the same data center will be attempted first. Where a data center-wide outage is identified, all current active production instances in the impacted data center will be failed over to the passive data center location in the pair. In this circumstance, a recovery time objective (RTO) of two hours, and a recovery point objective (RPO) of one hour is targeted. Due to the almost real-time replication between data centers, these times are usually significantly shorter than the stated RTO/RPO.

Automation technology built on the Now Platform is used to transfer or failover instances when necessary. The mechanism for both processes is very similar. The current passive system is designated active, and vice versa. To complete the process, DNS mappings and instance database configurations are updated accordingly. Redundant DNS providers and DNSSEC are employed to provide robust, resilient name resolution services.

More information

- Find out more about ServiceNow's Advanced High Availability Architecture
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Compliance

Contents

Does ServiceNow maintain an ISO/IEC 27001 certification?

KB0960279

ServiceNow maintains a globally applicable ISO/IEC 27001 certification, incorporating ISO/IEC 27017, ISO/IEC 27018, and ISO/IEC 27701.

More information

View ServiceNow's ISO 27001 Certification (incorporating 27017/27018/27701)

Is ServiceNow's information security policy documentation available?

KB0960252

Customers can obtain extensive security policy, standards, procedure, and other relevant documents from the ServiceNow CORE knowledge base (compliance evidence) in Now Support.

More information

- Customers can access ServiceNow's Information Security Policy and Information Security Standards
- Visit ServiceNow's CORE (compliance evidence) knowledge base

How can customers find out about ServiceNow compliance and standards?

KB0960251

Customers can obtain extensive compliance-related documentation including our ISO certifications, SSAE18/SOC attestations, and our latest penetration test reports from the ServiceNow CORE knowledge base (compliance evidence) in Now Support.

More information

Visit ServiceNow's CORE (compliance evidence) knowledge base

Can customers audit ServiceNow?

KB0960824

As a cloud service provider, 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 knowledge base in Now Support.

More information

Visit ServiceNow's CORE (compliance evidence) knowledge base

Why certification matters

KB0959419

Every year ServiceNow is rigorously audited by independent third-party companies and government bodies to prove that we comply with various global and regional standards governing information security. Each audit represents not just a 'tick in the box', but a significant commitment and ongoing effort; each one involves thousands of point-in-time and ongoing assessments covering every aspect of our information security program and efforts.

Our accreditors are experts in their respective fields with a deep understanding of the different global and regional laws and standards that must be complied with. They thoroughly assess ServiceNow's processes and controls against these standards, verifying that they are met or exceeded at all times. When the audit reports are complete, we make them available to customers.

All of this means that customers can be confident that ServiceNow consistently demonstrates excellent security controls and practices. It reduces the need for customers to generate and assess large quantities of detailed questions on these topics, as multiple well-qualified, independent assessors regularly do this on their behalf.

A note about GDPR

The General Data Protection Regulation (GDPR) is not listed below because GDPR is not a standard - it is a regulation, i.e. a law, and ServiceNow complies with the law in all jurisdictions in which it operates. ServiceNow has found transition to GDPR compliance a relatively pain-free process. It is not yet possible to achieve certification against GDPR, but ServiceNow will consider that in future should it become possible.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Visit ServiceNow's CORE (compliance evidence) knowledge base

Regulatory and industry compliance

KB0959420

ServiceNow has a dedicated audit, risk, and compliance (ARC) team responsible for a number of governance and compliance efforts across the organization, including managing ServiceNow's compliance program. This requires engagement across multiple functional areas within ServiceNow, including legal, finance, and procurement. ServiceNow's legal organization engages both internal and external legal counsel to understand ServiceNow's obligations to existing and new laws and statutory regulations within the jurisdictions in which it operates. The finance department is responsible for ensuring ServiceNow's compliance with relevant financial regulations, including Sarbanes Oxley (SOX), a requirement for all US public companies. ServiceNow itself is not subject directly to vertical-specific regulation, such as HIPAA, PCI, or NERC-CIP; however, it does have many customers who are. And through the features in the Now Platform and organizational transparency, it can support those regulated customers in meeting their obligations. In addition, ServiceNow operates a quality management system (QMS) based on the ISO 9001 standard. The ServiceNow has a dedicated QMS team, quality engineering team, and compliance team to ensure continual improvement. The table below summarizes ServiceNow's security-related certifications.

Certification or attestation	Description	Geography	Industry
ISO/IEC 27001:2013	Specifies information security management best practices and controls	International	All
ISO/IEC 27017:2015	Implementation of cloud-specific information security controls	International	All
ISO/IEC 27018:2019	Securing personally identifiable information (PII) in the cloud	International	All
ISO/IEC 27701: 2019	Establishing, implementing, maintaining, and improving a Privacy Information Management System (PIMS)	International	All
SSAE 18 SOC 1 and SOC 2 Reports	SOC 1 Type 2 focuses on protecting the confidentiality and privacy of information in the cloud that affects the financial reports of customers. SOC 2 Type 2 focuses on controls that are relevant to security, availability, processing integrity, confidentiality, or privacy	International	All

Certification or attestation	Description	Geography	Industry
AICPA SOC 2 TSC + HITRUST CSF	Provides a mechanism for the service auditor to opine on the design and effectiveness of the Trust Services Criteria and the HITRUST CSF in the same report.	International	All
FedRAMP JAB High P-ATO (for US government entities)	US government-wide program that provides a standardized approach for assessing, monitoring, and authorizing cloud computing products and services	United States	US federal government/ DoD
DoD Impact Level 4 Authorization (for US DoD/IC entities)	US government baseline for security requirements for cloud service providers that host DoD/IC information	United States	US federal government/ DoD
DoD Impact Level 5 Provisional Authorization (for National Security Cloud)	Updated US government baseline for security requirements for cloud service providers that host DoD/IC information	United States	US federal government/ DoD
APEC Privacy Recognition for Processes (PRP)	Certifies the adoption of sound risk management and security practices for cloud companies	International	All
ASD IRAP assessed for OFFICIAL and PROTECTED Cloud Services	Helps Australian government agencies effectively engage and consume cloud-based solutions.	Australia	Australian federal government
Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3	Certifies the adoption of sound risk management and security practices for cloud companies	Singapore	All
BSI Cloud Computing Compliance Controls Catalog (C5)	Cloud-specific compliance controls catalog developed by the German Federal Office for Information Security (BSI).	Germany	All
ISMAP Cloud Service	Ensures the level of security in cloud services meets Japanese Government Requirements.	Japan	Japanese Government

More information

Visit ServiceNow's CORE (compliance evidence) knowledge base

Encryption

Contents

Encryption key management overview

KB0959616

Column level encryption enterprise

CLE enterprise differs from 'legacy' column encryption in that it uses ServiceNow's Key Management Framework (KMF). The KMF provides enhanced key management capabilities following NIST 800-57 guidelines and allows customers to provide their own keys. Customer keys are re-encrypted (wrapped) with multiple higher-level keys, with the root key being stored in a FIPS 140-2-L3 compliant Hardware Security Module (HSM) within the ServiceNow cloud infrastructure.

Column encryption

Encryption keys are backed up within the database for the customer instance where they are used. Both instance-generated and customer-supplied keys are re-encrypted using a wrapper key which is securely stored in a ServiceNow-managed HSM within the ServiceNow cloud infrastructure.

Edge encryption and database encryption

Encryption keys for the Edge encryption feature are managed entirely within a customer's network boundary. Encryption keys for database encryption are managed by ServiceNow using a three-level key hierarchy. The first two keys are customer-specific and are created by the database engine, while the third key is instance-specific.

ServiceNow cloud infrastructure

Encryption keys used within ServiceNow's cloud infrastructure are managed by ServiceNow. Keys are stored in redundant secure key storage appliances. Dual controls are required for essential functions such as generating, deleting, or exporting keys. Key custodian forms are required as part of the generation of new keys. Cryptographic management is undertaken by a specific team within the security group, including appliances used to store the per customer instance wrapper key.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Secure communication with the instance

KB0959797

By their nature, customer instances of the Now Platform are designed to be accessible via the Internet, providing maximum flexibility in how, when, and from where they are accessed. The internet, however, is a public network and therefore communications can potentially be intercepted and read if they are not encrypted or otherwise protected.

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

Customers access their instances via a web browser using Transport Layer Security (TLS) encryption using AES with 128-bit or 256- bit cipher suites. This is also true of any data transferred from the on-premises MID server to the Now Platform. All end-user access to a ServiceNow instance attempted over HTTP are redirected to HTTPS. Negotiated ciphers are subject to customer browser versions and may be influenced by customer internet proxy infrastructure. Customers can force specific cipher suites via their own browsers or proxies if desired.

For additional security, customers are also able to use IP range-based authentication to restrict the public networks that are used to access their instances of the Now Platform.

The standard contractual clauses are applicable as a data transfer mechanism, as per section 9 (international data transfers) of ServiceNow's Data Processing Addendum.

More information

- Find out more about how ServiceNow Safeguards Customer Data
- Find out more about the ServiceNow MID Server

Are backups encrypted?

KB0960209

All instance backups 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 if a data restore is initiated.

For those customers who have purchased a Dedicated service, and whose instances reside on SAN storage, data is protected by the FIPS 140-2 level AES 256 encryption performed automatically by the storage arrays. In this case, snapshots take the place of traditional backups. These record the state of the data at the instant a snapshot is taken, and this can be reverted to if data needs to be returned to an earlier state – e.g. in the case of a restore operation.

More information

Find out more about ServiceNow encryption by reading the Data Encryption eBook

What options are available for customers to encrypt their data?

KB0960214

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

- Column Level Encryption (CLE) and CLE Enterprise provide symmetric data encryption for supported data fields.
- Database Encryption to encrypt all data that resides within the database; data is only decrypted while it's being accessed
- Cloud Encryption to encrypt the entire database at rest, and to ensure compatibility with future database technology enhancements
- 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

CLE, CLE Enterprise, and Cloud encryption all use the NIST 800-57 compliant Key Management Framework (KMF), which provides comprehensive key lifecycle management.

More information

Find out more about ServiceNow encryption by reading the Data Encryption eBook

How is data encrypted in transit?

KB0960217

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

More information

Find out more about ServiceNow encryption by reading the Data Encryption eBook

Financial Services

Contents

Overview of how ServiceNow supports Financial Services Customers

KB0960503

The Financial Services industry operates in a unique business environment with very particular requirements. Providing critical services that handle large volumes of sensitive and valuable data while meeting strict regulations for security and privacy can present significant challenges.

Software as a Service (SaaS) solutions can be attractive to Financial Services organizations who prioritize efficiency, flexibility, and scalability. However, any benefits must be considered from a security and compliance perspective: there are many criteria to be met, and these can vary across borders.

ServiceNow’s offerings present an ideal solution for Financial Services organizations because security, along with scalability and resilience, form the foundations of the Now Platform. We have a strong track record of serving a number of Financial Services customers, and this is backed up by excellent regulatory compliance –as demonstrated by the attestations and certifications we have achieved.

More information

The following financial services resources are also available:

- ServiceNow Financial Services Microsite
- ServiceNow: A Secure Platform to Transform Financial Services eBook
- Financial Services: The smarter way to workflow eBook
- Financial Services Operations Product
- Find out more about ServiceNow's Business Continuity Product

Is ServiceNow Payment Card Industry Data Security Standard (PCI DSS) certified?

KB0960254

ServiceNow is not a transaction processor, brand, merchant, or service provider in accordance with Payment Card Industry (PCI) terms, and therefore is not Payment Card Industry Data Security Standard (PCI DSS) certified. However, many of the criteria are already met through our other accreditations, e.g. ISO27001, SOC Reports, etc.

Financial service customers who consider ServiceNow part of their scope can work with their Qualified Security Assessor (QSA) to scope and assure appropriately using ServiceNow's standard assurance material.

More information

The following financial services resources are also available:

- ServiceNow Financial Services Microsite
- ServiceNow: A Secure Platform to Transform Financial Services eBook
- Financial Services: The smarter way to workflow eBook
- Financial Services Operations Product
- Visit ServiceNow's CORE (compliance evidence) knowledge base

What features does the Now Platform have that can help financial services customers process customer workflows?

KB0960273

The Now Platform provides five key control capabilities that can ensure the timely, compliant and auditable processing of financial services customer workflows:

Data Control - The platform Data Policy Management ensures that the completeness and quality of the data captured adheres to strict requirements, which is also mandated through system-to-system integration.

Service Level (SLA) Control - ServiceNow utilizes a powerful service level engine on the platform to intelligently monitor the health and timely delivery of customer cases, and take corrective action where necessary to ensure that regulatory obligations for resolution times are met.

Workflow Control - ServiceNow workflows are data-driven and 'tuned in' to the context of the record in real-time. Steps within the workflow may be subject to regulatory control, such as credit risk assessment. The workflow ensures that these steps are completed in the correct sequence, timeframe, and to the required standard in order to progress. The workflow provides the compliance guide rails for the process.

Governance, Risk and Compliance Control - Uniquely, ServiceNow has an Integrated Risk Management suite on the same platform that drives the processes, which enables true continuous controls monitoring. On the Now Platform, an organization's policies and controls for risk-mitigation and compliance can inform performance targets for customer workflows. These detect and correct issues in real time, avoiding reliance on other lines of defense.

Auditing and Monitoring Controls - every action and update in ServiceNow is recorded through immutable logs with alerting for anomalies.

More information

The following financial services resources are also available:

- ServiceNow Financial Services Microsite
- ServiceNow: A Secure Platform to Transform Financial Services eBook
- Financial Services: The smarter way to workflow eBook
- Financial Services Operations Product

Does ServiceNow have any products that support financial services customers?

KB0960271

Built on our well-established Customer Service platform, ServiceNow's Financial Services Operations product enables work to be routed efficiently across the customer's enterprise in order to increase visibility, enable compliance, and deliver great service. Financial Services Operations removes the legacy system fragmentation that creates the friction in customer experiences, reducing the complexity and cost of delivering quality differentiated services.

More information

The following financial services resources are also available:

- ServiceNow Financial Services Microsite
- ServiceNow: A Secure Platform to Transform Financial Services eBook
- Financial Services: The smarter way to workflow eBook
- Financial Services Operations Product

How can ServiceNow help financial services customers secure their clients' sensitive financial data?

KB0960276

Each ServiceNow account team works closely with their customers to determine how sensitive data points should be secured. We consider the data flows, integrations, reporting, user experience, business logic, and data classification requirements to recommend the best combination of security controls for the data and use case. Our multi-instance architecture gives customers greater flexibility over the way security controls are implemented to best meet their individual needs, including:

Field transformation - ServiceNow can detect a particular type/classification of data and transform its value before it is stored. This could, for example, truncate a credit card number to the last 4 digits, or mask a transaction ID. This can prevent sensitive data from being stored in inappropriate fields.

Encryption at rest - ServiceNow offers three types of complementary (layered approach) encryption at rest solutions: Database encryption (protects the entire database), Column Level Encryption (CLE) and CLE Enterprise provide symmetric data encryption for supported data fields, and Edge encryption (protects data before it leaves the customer's own network). See the Data Encryption e-book for further details.

Remote tables - The Now Platform can connect to third-party sources, or to another instance, to retrieve external data and optionally cache it in memory. You can view external data in lists or forms and process it. You can also group, sort, aggregate, and filter the data just like you would for standard internal tables/data stored in the ServiceNow database.

Just-in-time access - The Now Platform contains an array of industry-grade integration options to exchange data with remote sources. These can be called on-demand without the need to store the data, which can then be displayed in form or Service Portal widgets.

More information

- Find out more about ServiceNow encryption by reading the Data Encryption eBook
- The following financial services resources are also available:
  - ServiceNow Financial Services Microsite
  - ServiceNow: A Secure Platform to Transform Financial Services eBook
  - Financial Services: The smarter way to workflow eBook
  - Financial Services Operations Product

How does ServiceNow help financial services customers mitigate concentration risk?

KB0960267

ServiceNow's in-house service delivery does not rely on subcontractors. Our customers' confidence in our proven resilience and availability allows them to entrust their most critical operations to our platform and services. The Now Platform provides a single source of truth for operational and technical data. An integrated data model combined with a secure, reliable platform significantly reduces the typical risks associated with legacy, fragmented technology systems. It also provides increased efficiency through process streamlining. We have recently released an integrated Business Continuity Management (BCM) suite, to assist customers in the event of major disruption.

More information

Find out more about ServiceNow's Business Continuity Product

The following financial services resources are also available:

- ServiceNow Financial Services Microsite
- ServiceNow: A Secure Platform to Transform Financial Services eBook
- Financial Services: The smarter way to workflow eBook
- Financial Services Operations Product

Does ServiceNow follow the guidelines set out by the European Banking Authority (EBA) regarding outsourcing arrangements with relevance to cloud services?

KB0960269

ServiceNow is not a financial institution so does not fall under the scope of guidelines set out by the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and the UK's Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA). However, ServiceNow recognizes that companies in all industries are challenged to address a growing number of evolving regulatory requirements and is committed to helping its customers navigate the ever-changing regulatory landscape.

More information

The following financial services resources are also available:

- ServiceNow Financial Services Microsite
- ServiceNow: A Secure Platform to Transform Financial Services eBook
- Financial Services: The smarter way to workflow eBook
- Financial Services Operations Product

Information Lifecycle & Data Management

Contents

Information classification

KB0959450

ServiceNow applies relevant data classification levels to all customer data it hosts. ServiceNow does not inspect or monitor its customers' data and has no ability to understand how any data may have been classified by individual customers. For ServiceNow, the overriding requirement towards customer data is that it remains hosted solely in the private cloud and is treated and handled according to its policies for all customer data.

Customers remain the data controller (i.e. data owner) for all data they store in their ServiceNow instance and should therefore apply access controls according to their data classification policies.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Data retention

KB0959451

Customers decide what information is to be stored, how it is to be used, and how long it is retained. ServiceNow does not delete or modify customer data and only processes data in accordance with its contractual obligations.

Data that is deleted from a customer instance will remain backed up for 28 days before it is permanently deleted.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Media disposal

KB0959453

ServiceNow hosts its customer data on solid-state drives (SSD) or mechanical disks within its data center colocation spaces. Tapes and other forms of removable media are not used in providing the service, including for backups (which are also written to disk). Functioning mechanical storage devices that are retired at end-of-life, or for reassignment to new customers, are logically shredded based on NIST best practices. SSD drives are securely erased with processes utilizing appropriate tools provided by the relevant SSD hardware vendor.

All failed storage devices, both mechanical and solid state, are securely retained within the same datacenter colocation space where they resided, regardless of whether they contained customer data or not.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

What happens to a customer's data once a contract has been terminated?

KB0960265

Upon termination or expiration of the agreement with ServiceNow, customers may request the return of all customer data within 45 days. Data is returned using an industry standard format by means of a database dump. After that time, the data is logically wiped from the system following the NIST 800-88 guidelines.

What is ServiceNow's data destruction process?

KB0960268

ServiceNow logically sanitizes mechanical and solid-state drives (SSD) prior to re-use, following a data sanitization standard operating procedure (SOP). This process is consistent with NIST 800–88: Guidelines for Media Sanitization, and the DoD National Industrial Security Program 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, and is performed by a specialist destruction vendor, and overseen by ServiceNow personnel. A certificate of destruction is produced for each destruction event, and each destroyed drive is recorded.

More information

Customers can access ServiceNow's Storage Media Destruction SOP and Secure Data Deletion SOP

How can customers access their database dump?

KB0960266

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

Data return and destruction

KB0959454

Throughout the lifetime of the subscription, data can be directly exported using features available in a ServiceNow instance. This can be via the UI interface through integrations or by using optional ServiceNow components, such as the available ODBC connector or MID Server.

Upon contract expiration or exit, or where requested, ServiceNow will supply a customer's data in an SQL dump format. Exiting customers have 45 days to request their data to be returned, after which all hosted and backed-up data is automatically deleted and overwritten.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Find out more about how ServiceNow Safeguards Customer Data

Information Security Governance & Risk Management

Contents

Security frameworks

KB0959413

ServiceNow’s security framework is based on ISO/IEC 27002:2013. As an ISO/IEC 27001 certified organization, there is a high level of integration between the ISO/IEC 27002:2013 code of practice and the ServiceNow information security management system (ISMS). ServiceNow has been an ISO 27001 certified organization since 2012 and is also ISO/IEC 27017:2015 and 27018:2019 certified.

ServiceNow provides applications within the Now Platform relating to process and service management. This includes IT service management based on the globally recognized ITIL process model. ServiceNow uses this best practice methodology and its principles internally to operate and manage its private cloud environment, as well as its customer-facing support model.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Security management

KB0959415

ServiceNow’s chief information security officer (CISO) reports to the chief information officer (CIO) and in turn to the chief executive officer (CEO). This simple organizational structure provides executive visibility and oversight regarding security and risk.

The CISO is supported by a number of domain specialist teams. These include security architecture; security engineering; security operations and threat response; application security; and audit, risk and compliance. There are also specific teams for liaising with customers on security matters, shaping employee behavior, creating documentation, and other resources.

The roles of each of these teams and individuals within the teams are clearly defined, and ServiceNow employs standard information security best practices in its security processes, such as separation of duties and the four-eyes principle.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Risk management

KB0959416

ServiceNow has defined processes and procedures for managing and assessing information system and operational security risks. Regular assessments are performed to identify and assess the likelihood and impact relating to risks. These risks can include those regarding unauthorized access, use, disclosure, or disruption to ServiceNow systems and customers. Risks are categorized in accordance with a formally documented procedure.

Key security, risk, and compliance stakeholders meet regularly to discuss security and risk items, and any identified risk is quickly and efficiently managed in a timely manner in order to safeguard the confidentiality, integrity, and accessibility of ServiceNow systems and customer data. ServiceNow executive leadership is regularly briefed on current and new security risks, and any potential threats that could impact ServiceNow and its customers.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Security policy, standards, and procedures

KB0959414

ServiceNow’s security program is described in its information security management system (ISMS) and associated security policies and standards. These are reflected in an extensive library of standard operating procedures (SOPs) and other relevant documentation and guidance. SOPs, for example, define the actions that must be carried out in a wide variety of situations according to the overall security policy.

Examples of ServiceNow’s SOPs include:

- Security Incident response
- Data handling
- Secure development procedures
- Risk assessment
- Incident management, problem management, and change management
- Access entitlements and review process
- Configuration management
- Vendor risk management
- Human resources and information

These documents are assessed and updated in the case of significant changes or at least every two years by a managed program.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

ServiceNow organizational entitlement reviews

KB0959417

ServiceNow has a dedicated identity and access management (IAM) team with an active IAM entitlement program that requires frequent reassertion of entitlement and comprehensive review.

At a minimum, quarterly entitlement reviews are carried out to ensure that personnel have the appropriate logical and physical access rights are assigned to them. This includes those responsible for management of its private cloud and physical colocation spaces. Reviews also take place when personnel change roles within ServiceNow.

A service catalog of ServiceNow roles and request types is implemented internally. This is used both for new requests and reassignment of access for existing personnel. This approach mitigates potential incorrect assignment of access, which can occur where access is simply copied from one user to another.

The majority of ServiceNow personnel have no access to any systems hosting customer data, or to customer data in general.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Customers can access ServiceNow's Entitlement Review SOP

Human resources security

KB0959418

Upon commencement of the employment process for all prospective candidates, ServiceNow undertakes background checks and screening. Subject to per-country restrictions, these include criminal, employment, financial, citizen status, and government watch lists. Drug testing also takes place in jurisdictions that allow it. Failure to pass these tests will result in either mandatory disqualification from the employment process or a further follow-up investigation. As a condition of accepting employment, ServiceNow personnel are required to sign a non-disclosure agreement and review and confirm their understanding of the ServiceNow Code of Conduct & Ethics policy along with the Acceptable Use Policy. This confirmation is recorded electronically. Without exception, all ServiceNow personnel are required to undergo annual general security awareness (GSAT) training, and fulfillment of training requirements is measured and enforced. The content of the training varies from year to year, as different security topics, risks, threats, and requirements are identified. Some examples are listed below:

- Privacy and data protection
- Code of conduct and ethics
- Insider trading & foreign corrupt practices
- Email and instant messaging
- Physical security
- Cloud technologies

Personnel whose roles may bring them into contact with customer data are also required to undertake additional training. The lifecycle of a user within ServiceNow is controlled by standard operating procedures for the creation, modification, and deletion of user identities. ServiceNow operates integrated HR, IT, and IAM processes using ServiceNow's own products; these products operate independently for both the corporate environment and the completely separate customer cloud environment. Access control is based on job function and in line with the principle of least privilege. Regular entitlement reviews are conducted to ensure that the processes are working and to remediate any changes or removals that have not been processed appropriately. Employees exiting ServiceNow have all access removed within a maximum period of 24 hours.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- IT Support Onboarding, Role Change, and Offboarding SOPs
- HR Support Onboarding and Offboarding SOPs
- Background Screening SOP
- Training Policy & Training SOP

Security policy, standards, and procedures

KB0959414

ServiceNow's security program is described in its information security management system (ISMS) and associated security policies and standards. These are reflected in an extensive library of standard operating procedures (SOPs) and other relevant documentation and guidance. SOPs, for example, define the actions that must be carried out in a wide variety of situations according to the overall security policy.

Examples of ServiceNow's SOPs include:

- Security Incident response
- Data handling
- Secure development procedures
- Risk assessment
- Incident management, problem management, and change management
- Access entitlements and review process
- Configuration management
- Vendor risk management
- Human resources and information

These documents are assessed and updated in the case of significant changes or at least every two years by a managed program.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Customers can access ServiceNow's Information Security Policy and Information Security Standards

Overview of instance integrations

KB0959593

The Now Platform is based on service-oriented architecture (SOA). To support customer workflows, all data objects can use web services to access bidirectional data-level integrations. Integrations may be implemented programmatically or through the use of features in the Now Platform, including IntegrationHub, to simplify and accelerate customer integrations.

Additionally, the platform offers a rich interface for loading external data using import sets. Using this feature, customers can load from various data sources such as HTTPS, FTPS, and SCP using file formats such as XML, CSV, and Microsoft Excel XLS files.

Information can also be pulled from a data source using a direct JDBC connection, provided customer network connectivity permits it.

For integration with systems, services, or applications within a customer’s network, ServiceNow provides the MID Server component. This capability enables secure integration and collaboration between a customer’s own applications and services and a customer’s ServiceNow instances. MID Servers may also be combined with import sets for data sources not accessible to a customer’s ServiceNow instance.

Information within an instance can be exported and migrated to an external platform using an open database connectivity (ODBC) driver that’s provided by ServiceNow. Forms, lists, and reports on the platform can be accessed directly using a URL, which facilitates integration between two or more web applications.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Instance Integrations

Contents

Overview of instance integrations

KB0959593

The Now Platform is based on service-oriented architecture (SOA). To support customer workflows, all data objects can use web services to access bidirectional data-level integrations. Integrations may be implemented programmatically or through the use of features in the Now Platform, including IntegrationHub, to simplify and accelerate customer integrations.

Additionally, the platform offers a rich interface for loading external data using import sets. Using this feature, customers can load from various data sources such as HTTPS, FTPS, and SCP using file formats such as XML, CSV, and Microsoft Excel XLS files.

Information can also be pulled from a data source using a direct JDBC connection, provided customer network connectivity permits it.

For integration with systems, services, or applications within a customer's network, ServiceNow provides the MID Server component. This capability enables secure integration and collaboration between a customer's own applications and services and a customer's ServiceNow instances. MID Servers may also be combined with import sets for data sources not accessible to a customer's ServiceNow instance.

Information within an instance can be exported and migrated to an external platform using an open database connectivity (ODBC) driver that's provided by ServiceNow. Forms, lists, and reports on the platform can be accessed directly using a URL, which facilitates integration between two or more web applications.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Instance communication hierarchy

KB0959601

Customers initiate communication from their network to their ServiceNow instances over HTTPS from any endpoint device with a browser, or from a system or application level integration.

An instance itself never initiates communication into the customer's network unless a data source or other integration within the customers environment is configured by the customer themselves.

Activities such as ServiceNow Discovery or Orchestration that can 'touch' customer infrastructure are executed only on customer direction. These are via activities they define in their instances and actioned using MID Servers they have deployed. Output that is produced as part of an activity is sent back to the relevant instance over HTTPS.

Customers can place as many MID Servers in their environment as necessary to support any network topology ranging from a flat to a highly segmented network.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Web services integration

KB0959595

ServiceNow supports web services using SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) for integration, all traffic is encrypted using TLS.

Web service security is enforced using the combination of basic authentication challenge/response and system-level access using contextual security. Additionally, there is a set of web service-specific roles that may be granted to the web service user.

For incoming SOAP requests, support for WS-Security 1.1 in the form of WSS X.509 token profile and WSS username token profile is available. In this context, “incoming” means requests targeting a web services resource in a customer ServiceNow instance.

Mutual web services authentication is supported for inbound and outbound HTTPS connections, such as SOAP, REST, or direct HTTPS calls, as well as those sent through a MID Server.

Secure signing of SOAP requests for message integrity purposes is also available.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Now Platform malware protection

KB0959600

Now Platform instances feature antivirus protection to protect against uploading or downloading malicious content. File attachments are scanned by dedicated servers in each regional data center to guard against viruses or malware being distributed from an instance.

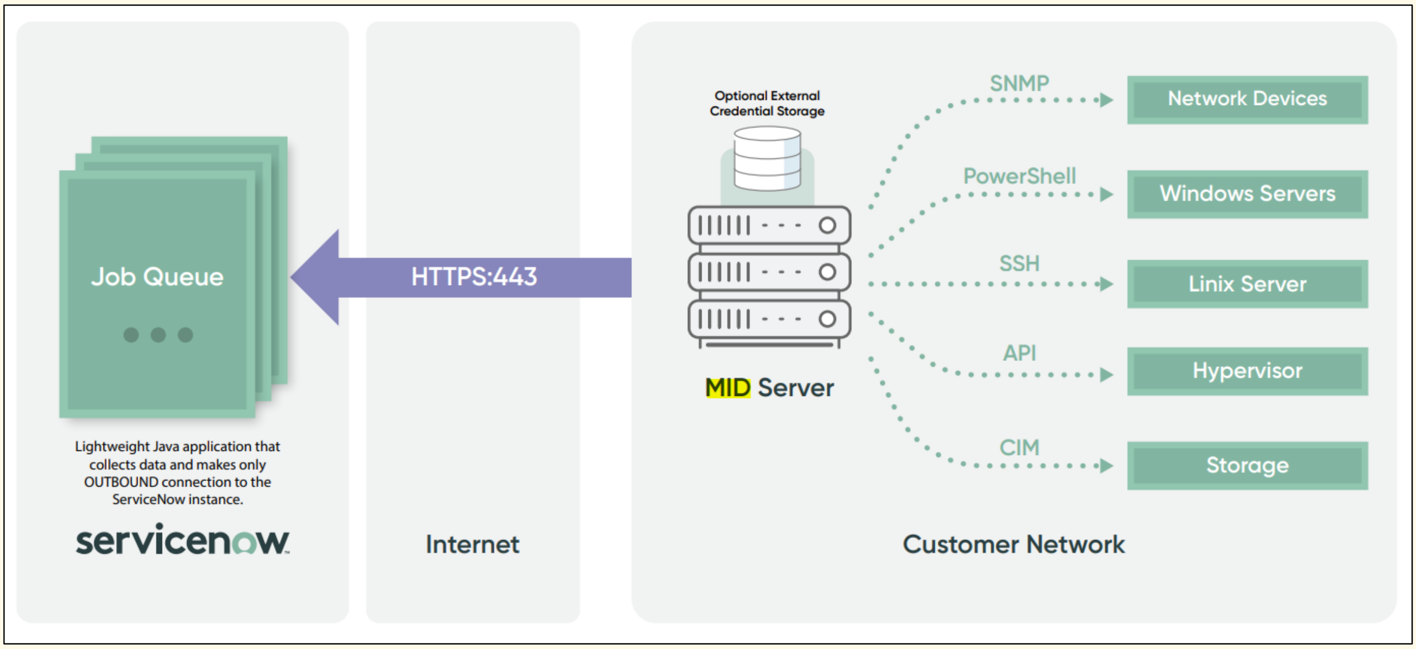
More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

ServiceNow MID Server

KB0959594

The ServiceNow management, instrumentation, and discovery (MID) Server is an optional, free ServiceNow component. It facilitates communication of data between the customer instances and external applications, data sources, and services. MID Servers are used by customers in conjunction with their instances for enterprise application and service monitoring, integration, orchestration, and discovery. The MID Server is a Java application provided to customers via a download link within their instance. It may be installed by the customer on a suitable host system within their environment. The server can use Windows or Linux operating systems. MID Servers are cryptographically paired with an individual instance during installation and need to be approved by the customers ServiceNow administrators before they can be used. At a customer defined interval, a MID server securely initiates an outbound session to a customer's instance over HTTPS using TLS 1.2, looking for activities to perform. The activity is retrieved and executed, and any output or resulting data is returned to the originating instance. This outbound, or 'pull' approach negates the need to permit inbound access through a customer's perimeter or firewalls directly to the internet.


Job Queue
Lightweight Java application that collects data and makes only OUTBOUND connection to the ServiceNow instance.
servicenow
HTTPS:443
Internet
Optional External Credential Storage
MID Server
SNMP
PowerShell
SSH
API
CIM
Network Devices
Windows Servers
Linix Server
Hypervisor
Storage
Customer Network

More information

- Find out more about the ServiceNow MID Server
- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Find out more about ServiceNow encryption by reading the Data Encryption eBook

Miscellaneous

Contents

How do customers find their instance IP address?

KB0960258

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

More information

Find out more about finding the IP address for your instance

How can customers communicate with ServiceNow?

KB0960270

All communication between ServiceNow and its customers is conducted via the Now Support portal or support account manager (SAM) where applicable. This ensures that all customer queries are captured, prioritized, and routed immediately, without reliance on individual availability.

Frequently Asked Questions: Trust Center on Now Support

KB1171625

How is the Trust Center helping customers and prospects self-serve content needed for due diligence, vendor risk assessment, and auditing?

The Trust Center on NOW Support provides a single source of truth for customers and prospects to find content to support their due diligence, vendor risk assessment, and auditing needs. Self-serve features include a customer-vetted user interface, AI search (which searches content on relevant pages as well as content within attachments), and Virtual Agent including multiple conversations around the most frequently requested CORE assets. Additionally, CORE has been moved from NOW Community to NOW Support and has been re-formatted as KB articles to improve knowledge search and management to help customers and prospects quickly and efficiently self-serve what they need, when they need it.

What is CORE and what is it used for?

CORE (Compliance Operations Readiness Evidence) is the repository of ServiceNow's corporate policies and procedures that is typically used by customers and prospects to support due diligence, vendor risk assessment, and auditing. CORE access is contractually guaranteed for ServiceNow's customers.

How will moving CORE from NOW Community to NOW Support help customers and prospects?

Customers have provided feedback that obtaining access to CORE Community and searching for content within CORE Community aren't easy and take too long. CORE is moving to NOW Support as of September 23, 2022 in order to simplify and accelerate how customers and prospects perform due diligence, vendor risk assessment, and auditing. Customers and prospects will be able to leverage the Trust Center UI, AI search, and Virtual Agent to easily and quickly find content. Customers can also create a Trust case for further assistance, which will be managed by the Customer Service team with a guaranteed response within 24 hours.

Why is ServiceNow improving the CORE provisioning process and when will this take effect?

Customers have provided feedback that CORE provisioning isn't easy and takes too long. On September 23, 2022 ServiceNow will simplify and accelerate how customers, prospects, and 3rd party auditors perform due diligence, vendor risk assessment, and auditing by streamlining how customers, prospects, and 3rd party auditors access CORE – instead of submitting a request through the Legal team using coreaccess@servicenow.com:

- Customer and partner admins will be able to provision end users to CORE from their own instance
- Account teams will be able to provision prospects to CORE
- Security Compliance will be able to provision 3rd party auditors to CORE from NOW Support

These changes will be effective September 23, 2022 for commercial customers. Customers operating in regulated market environments (GCC, NSC, SPP) will also have Trust Center (CORE) access starting in October, and customer and partner admins in those environments will be able to provision end users to CORE.

If CORE is moving to NOW Support, what is happening to CORE in NOW Community?

For commercial customers: Starting on September 23, 2022:

- Existing CORE Community users with a NOW Support account will be migrated to CORE on the Trust Center on NOW Support.
- Existing CORE Community users without a NOW Support account, or who used a personal email address for CORE Community access, can request Trust Center (CORE) access from their customer or partner admin by creating a NOW Support account.

On October 23, 2022 the CORE Community site will be deprecated, and CORE will only be accessible through the Trust Center on NOW Support.

For regulated market customers operating in the GCC, NSC & SPP environments:

- Until September 30, 2022 new GCC, NSC, and SPP end users should continue to use coreaccess@servicenow.com to request CORE access.
- Starting September 30, 2022, new CORE end users in the GCC environment can request Trust Center (CORE) access from their admin.
- Until October 7, 2022 new NSC and SPP end users should continue to use coreaccess@servicenow.com to request CORE access.
- Starting October 7, 2022, new CORE users in the NSC and SPP environments can request Trust Center (CORE) access from their admin.
- On October 23, 2022 the CORE Community site will be deprecated, and CORE will only be accessible through the Trust Center on NOW Support.

How is provisioning CORE access for customers and partners being improved?

On September 23, 2022 customer and partner admins (commercial accounts) will be able to provision end users to CORE via the Automation Store (new NOW Support users) or Manage Accounts (existing NOW Support users). End users will receive a notification (including a click-through NDA) to log into NOW Support, and they will be able to access CORE from the Trust Center. This will eliminate the lead time and overhead of managing end users' CORE access via the Legal team and will simplify and accelerate end users' ability to self-serve CORE content that they need for due diligence, vendor risk assessment, and auditing.

Starting on September 30, 2022 GCC customer and partner admins (and starting on October 7, 2022 NSC and SPP customer and partner admins) will be able to provision end users to CORE via the Automation Store (new NOW Support users) or Manage Accounts (existing NOW Support users).

See KB1167040 for instructions on adding new users to the Trust Center.

How can a customer or partner identify who their customer or partner admin is?

Customers can use the "Identifying your customer administrator" KB to identify their customer or partner admin.

How can customers or partners obtain CORE access if their customer or partner admin is unable to do so?

- Customers and partners should contact their ServiceNow Account team to request CORE access and provide justification.
- The ServiceNow Account Team will have a case created in Now Support
- Details to be provided:
    - User Name (first + last name)
    - Email
    - Phone
    - Company name
    - ACCT Number
    - Trust Center access type (Permanent or Temp)
- The account team will inform the requestor

How is prospect provisioning to CORE being simplified?

On September 23, 2022 account teams will be able to provision prospects to CORE. Prospects will receive a notification (including a click-through NDA) to log into NOW Support, and they will be able to access (for 30 days) CORE from the Trust Center. Prospects can leverage the Trust Center UI, AI search, and Virtual Agent to quickly and efficiently self-serve the information needed to support their due diligence, vendor risk assessment, and auditing. Prospects can also request a one-time 30-day extension for CORE access from their account team. This will eliminate the lead time and overhead of managing prospects' CORE access via the Legal team.

If a case is created on behalf of a customer, how will requestors be kept informed of the status of their request?

Requestors are automatically added to the case watch list in order to keep them informed of the case status.

How do I enable customer 3rd Party Auditors to access CORE?

In all cases where an Audit is being requested, please contact your ServiceNow Account Executive who can help steer you through the process. Please complete this form which requests details of the Audit Requirement and the 3rd Party Audit company. It will trigger the ServiceNow Customer Audit team to provide access to CORE for the named 3rd Party Auditors, as well as capture important details about your audit needs.

If you have any questions, please contact customeraudit@servicenow.com.

Mobile Application Security

Contents

What do customers need to know about mobile app security?

KB0960235

ServiceNow has developed 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.

More information

Find out more about Mobile Security

How is mobile app data secured?

KB0960237

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

Find out more about Mobile Security

How can customers control what mobile users can access?

KB0960236

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

More information

Find out more about Mobile Security

Mobile Security

KB0959617

The native ServiceNow mobile applications for iOS and Android enable instances to be accessed from mobile devices. These apps use the same robust authentication mechanisms available in instances of the Now Platform. Once authenticated, mobile users are subject to the same access controls.

Mobile application security controls

The apps benefit from mobile-specific security controls, such as restricting clipboard operations, requiring a PIN for access, disabling attachments, and obscuring the app screen when in the background.

Data security

All data in transit is protected with TLS, and application preference information stored on-device is encrypted. By default, no data from an instance is stored on the mobile device.

Application distribution

ServiceNow's mobile applications can be distributed with common enterprise mobility management (EMM) or mobile device management (MDM) platforms.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Personal Data & Data Privacy

Contents

Does ServiceNow have privacy policies and procedures in place that are regularly reviewed and revised?

KB0960275

ServiceNow maintains privacy policies and procedures that are reviewed and revised as appropriate against applicable data privacy laws and standards. For further information, please refer to the ServiceNow Privacy Statement and the privacy section on the ServiceNow Trust Site.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite
- Customers can access ServiceNow's Data Protection Policy

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

KB0960256

ServiceNow is an advocate of consumer privacy rights.

ServiceNow's Data Processing Addendum (DPA) outlines how personal information is only processed to the extent necessary to provide our products and services, and describes the privacy and security measures in place.

ServiceNow is committed to complying with the EU General Data Protection Regulation (GDPR) across 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. Additional information can be found on the GDPR page of the ServiceNow Trust Site.

Similarly, the Californian Consumer Privacy Act (CCPA) focuses on data privacy for residents of the state of California. Under the CCPA, ServiceNow is considered a “service provider”. ServiceNow's DPA addresses the CCPA’s requirements for data privacy and information security.

More information

- View ServiceNow's Data Processing Addendum (DPA) and read frequently asked questions about ServiceNow's Privacy Program
- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

Does ServiceNow have a defined process to archive or delete customer data?

KB0960220

As the data controller, customers own the data in their ServiceNow instances, and ServiceNow does not archive or delete data on behalf of a customer during the subscription term. For customers that want to archive and/or purge data within their ServiceNow application, there is a built-in feature that can be leveraged. For more information, please see the data archiving product documentation.

If a customer chooses to terminate their agreement with ServiceNow, ServiceNow gives the customer a 45-day grace period to request their data, and if requested, will supply their data in a standard SQL export. After 45 days, the data is logically wiped from the system following the NIST 800-88 guidelines.

More information

Find out more about data archiving with ServiceNow

Can customers use ServiceNow instances to delete personal data?

KB0960216

As 'data controller' customers can choose to delete any data they store in their ServiceNow instances at their discretion, including personal data, during the subscription term.

Is the principle of privacy by design implemented within the development of ServiceNow systems and products?

KB0960204

ServiceNow maintains a comprehensive privacy by design program, including policies, procedures, and controls governing the processing, storage, transmission, and security of customer data. Additionally, our privacy and security programs include industry-standard practices designed to protect customer data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ServiceNow regularly tests, assesses, and evaluates the effectiveness of the privacy and security programs and may periodically review and update these programs to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

Does ServiceNow have a data protection officer?

KB0960274

ServiceNow has a head of global privacy and a dedicated privacy team to respond to data protection inquiries. The head of global privacy and the privacy team can be contacted at privacy@servicenow.com.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

Are there mechanisms in place for registering and managing consumer consents (opt-ins) and permissions (such as privacy consents)?

KB0960208

ServiceNow can be used to automate and record the delivery and acceptance of privacy notices. Basic platform features allow recording and reporting on processing activities. However, these activities (together with all notification responsibilities) are entirely the responsibility of the data controller.

How does ServiceNow define their obligations under the EU General Data Protection Regulation (GDPR)?

KB0960272

Under the EU General Data Protection Regulation (GDPR) ServiceNow is considered the 'data processor'. As the 'data processor', ServiceNow supports the customer by providing necessary security measures, following applicable instructions, notifying the customer in the case of a data breach, and supporting the customer's obligation to respond to data subject requests. ServiceNow is responsible for meeting its requirements as a data processor under the GDPR.

The customer is considered the 'data controller' under GDPR. As 'data controller', the customer is responsible for determining how data is collected, stored, used, shared, archived, and destroyed, as well as maintaining the accuracy of that data. The customer is also responsible for meeting their requirements as a data controller under the applicable data protection laws, including the GDPR.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

What data transfer mechanisms are in place with customers and with sub-processors?

KB0960201

The Standard Contractual Clauses are applicable as a data transfer mechanism as per section 9 (International Data Transfers) of the Data Processing Addendum (DPA).

More information

View ServiceNow's Data Processing Addendum (DPA) and read frequently asked questions about ServiceNow's Privacy Program

Does ServiceNow provide privacy and security awareness training for its personnel?

KB0960188

ServiceNow employees have to successfully complete privacy awareness training annually. In addition, access to personal data by ServiceNow is limited to personnel who require such access to perform ServiceNow's obligations under the agreement with the customer and who are bound by confidentiality obligations at least as protective as those set forth in the agreement.

Can customers adhere to the 'Right to Erasure' within their ServiceNow instance?

KB0960213

During the subscription term, ServiceNow provides the 'data controller' (customer) with the ability to identify, locate, and erase personal data within customer ServiceNow instances, as may be required under data protection laws. Data controllers are fully responsible for the erasure of data. Once data is deleted from the active instance, it is very quickly deleted in the corresponding passive data center in the pair, and that data will no longer be backed up.

Does ServiceNow commit to notifying customers of relevant data breaches?

KB0960193

ServiceNow will report to affected customers any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to customer data that it becomes aware of without undue delay.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

Does ServiceNow help customers obtain authorizations from authorities?

KB1116663

ServiceNow provides reasonable assistance in connection with any prior consultation customers are required to undertake with a supervisory authority under data protection laws with respect to processing of personal data in the subscription service.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

Can ServiceNow help customers satisfy their obligations under applicable data protection laws?

KB0960197

As the ‘data processor’, ServiceNow provides features to enable customers (the 'data controller') to have access to and control of data processing activities and obligations, including implementing necessary security measures, notifying the controller in the case of a data breach, and directing any lawful requests made by authorized parties to the controller.

Does ServiceNow provide assistance/information to enable customers to process data subject access requests (DSARs)?

KB0960192

ServiceNow provides its customers with a number of capabilities with respect to data subject access requests (DSARs). These include the ability to access, correct, rectify, erase, or block personal data, or to transfer or port such personal data, within the subscription service, as may be required under data protection laws (collectively, 'data subject requests'). However, it is the role of the data controller (customer) to respond to data subject requests.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

Does ServiceNow conduct privacy risk assessments?

KB0960206

ServiceNow performs privacy risk assessments annually as part of its general privacy and security risk program.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

Can customers use ServiceNow instances to mask personal data?

KB0960218

ServiceNow instances can mask, as well as encrypt, specific data. Customers can enable business scripts to mask and/or remove pattern matched data.

More information

Find out more about enabling business scripts

Are there formalized procedures to assist customers in responding to requests related to processing of personal data (e.g. including the provision of GDPR required content)?

KB0960211

As 'data controller', the customer is solely responsible for responding to any 'data subject' requests. Therefore, in the event that ServiceNow receives a 'data subject' request that relates to a customer, the 'data subject' making the request will be instructed to contact the customer directly.

ServiceNow provides comprehensive search and reporting features that allow immediate identification and presentation of data relating to individual subjects, and supports a large variety of output formats and integrations to meet this obligation.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

How can personally identifiable information be protected from unauthorized access or loss?

KB0960224

ServiceNow instances include a number of capabilities available to customers to help protect data from unauthorized access or loss:

- Authentication of users before access and integrations for customer credential services (SSO)
- Encryption of passwords and requiring additional authentication methods (multi-factor)
- Enforcement of password strength and complexity polices, and allow users to manage passwords
- Prevention of access by users with an inactive or disabled credentials

Customers manage each user's access to and use of their ServiceNow instances by assigning to each user a credential and user type that controls the level of access to the subscription service. The customer is responsible for implementing access controls relevant to that user to assist in protecting all customer data, including personal data. Other controls such as encryption can also be applied for further assurance. The customer is solely responsible for its decision not to encrypt such data, and ServiceNow will have no liability to the extent that damages would have been mitigated by the customer's use of such encryption measures. The customer is also responsible for protecting the confidentiality of each user's login and password and managing each user's access to the subscription service.

ServiceNow maintains sufficient controls to meet the objectives stated in ISO 27001, ISO 27018 (or equivalent standards) for the information security management system supporting the subscription service. This is independently verified by assessments that follow SSAE 18/SOC 1 and SOC 2 Type 2 attestation standards.

More information

- Find out more about authentication and enabling password policies.
- Find out more about ServiceNow encryption by reading the Data Encryption eBook
- View ServiceNow's ISO 27001 Certification (incorporating 27017/27018/27701)

Can ServiceNow help customers conduct Data Protection Impact Assessments (DPIAs)?

KB0960195

ServiceNow maintains a knowledge base called CORE. CORE contains information around the processing of customer data, which can help customers conduct their data protection impact assessments.

More information

Visit ServiceNow's CORE (compliance evidence) knowledge base

How can ServiceNow help customers manage their GDPR requirements?

KB0960277

ServiceNow provides an eBook Complying with the General Data Protection Regulation (GDPR). Additional information can be found on the GDPR page of the ServiceNow Trust Site.

More information

- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

What is data privacy?

KB0959804

Data privacy addresses the rights of an individual over personally identifiable information (PII) held about them. This type of information is often subject to strict regulation.

PII refers to any information that relates to a living person, such as a person's name, date/place of birth, social security number, and biometric data. Sensitive personal information (SPI) is an extension of PII which includes sensitive data such as ethnic origin, political opinions, health information, and criminal record. In some jurisdictions, there are additional classifications of SPI, such as protected health information (PHI) in the U.S., which relates to an individual's health status or healthcare.

Some data items that cannot be used individually to identify a person could still be classified as personal information when used in combination with other information (e.g. age, gender, and address).

More information

Find out more about how ServiceNow Safeguards Customer Data

Protecting personal data

KB0959805

Personal data must be protected from unauthorized access or data loss. The Now Platform provides the capabilities to:

- Authenticate users before access
- Encrypt passwords
- Allow users to manage passwords
- Prevent access by users with an inactive account

ServiceNow maintains controls that meet the objectives stated in ISO 27001, ISO 27018, SSAE18/SOC 1 and SOC 2 Type 2 (or equivalent standards) for the information security management system supporting the subscription service. At least once per calendar year, ServiceNow obtains an assessment against the standards by an independent third-party auditor. Additionally, ServiceNow provides the self-serve CORE Compliance Portal to help customers conduct data protection impact analyses (DPIA), if required.

In addition to our security measures, customers also have a share of responsibility in protecting their data, which includes:

- Managing each user’s access to (and use of) the service
- Implementing encryption and/or access control functionalities that are available within the subscription service
- Protecting the confidentiality of each user’s login and password

More information

Find out more about how ServiceNow Safeguards Customer Data

Data privacy operations

KB0959806

Data subjects have basic rights to privacy. The responsibility for upholding and supporting these rights is shared between the data controller and data processor. The GDPR is currently the highest standard of data privacy regulation globally, so GDPR is a useful benchmark for operations related to data privacy.

ServiceNow provides data controllers with the ability to access, correct, rectify, erase or block personal data – or to transfer or port such personal data within the subscription service, as may be required under data protection laws (collectively called data subject requests). However, it is the responsibility of the data controller (customer) to respond to data subject requests.

The following table outlines the legal rights of an individual and how ServiceNow can be used to support these rights:

Individual's rights	Description and how ServiceNow supports these rights
Right to be informed	Data subjects must be informed that their data is being collected and how it will be used. ServiceNow can be used to automate and record the delivery and acceptance of privacy notices. Basic platform features allow recording and reporting on processing activities. These activities are entirely the responsibility of the data controller.
Right of access	Data subjects may request information regarding their personal data from the data controller free of charge, and this should normally be supplied within one month of receipt. If subject access requests (SARs) are made to ServiceNow, they will be redirected to the data controller without undue delay. Comprehensive search and reporting features allow immediate identification and presentation of data relating to individual subjects, and ServiceNow supports a large variety of output formats and integrations in order to meet this obligation. These activities are entirely the responsibility of the data controller.

Individual's rights	Description and how ServiceNow supports these rights
Right to rectification	Data subjects may request that inaccurate personal data is rectified. They must be informed where this inaccurate data has been disclosed to third parties and these third parties must be informed of the rectification where possible. ServiceNow has comprehensive logging features which allow data controllers to determine when data has been changed, and by whom, and produce complete audit trails where enabled. Web services integrations allow real-time integrations with third parties where necessary. These activities are entirely the responsibility of the data controller.
Right to erasure	Data subjects may request the deletion or removal of personal data where there is no compelling reason for its continued processing, e.g. the individual withdrawing consent. Data controllers are fully responsible for the erasure of data. ServiceNow has comprehensive auditing and reporting features which can provide visibility into such data, and evidence of erasure. ServiceNow is responsible for ensuring that data deleted from customer instances is reflected in all locations in which this data is stored. Once data is deleted from the active instance, it is very quickly reflected in the corresponding passive data center (DC), and that data will no longer be backed up. Backups are aged over a period of 28 days after which no record of deleted data will remain in ServiceNow infrastructure. At the end of their working life, disks are securely wiped or destroyed such that no data remains.
Right to restrict processing	Data subjects may request that certain processing is blocked. This is a wide-reaching topic which may involve many variables. ServiceNow has a flexible database and business rules system which allows easy tagging of individual records and conditional processing (i.e. respecting a "do not share" restriction and reporting on such activities or restrictions). These activities are the responsibility of the data controller.
Right to data portability	Data subjects may request to obtain and reuse their personal data for their own purposes, and must be able to transfer the data easily and securely. ServiceNow supports a wide variety of structured data formats, including the common open CSV format, XML, JSON, etc. The ability to extract data in a variety of forms is a built-in feature supported universally throughout the platform, allowing data controllers to easily comply with this requirement. These activities are entirely the responsibility of the data controller.

Individual's rights	Description and how ServiceNow supports these rights
Right to object	Data subjects have the right to object to processing, and individuals must be clearly informed of this right at the first point of communication. ServiceNow can be used to automate and record this. These activities are entirely the responsibility of the data controller.
Rights related to automated decision-making and profiling	These rights introduce safeguards against the risk of a potentially damaging decision being taken without human intervention. ServiceNow's comprehensive workflow engine allows for comments, approvals, conditional processing, and multi-channel integration with human decision makers. This allows data controllers to build processes that comply with this right, and existing platform auditing and reporting features allow the easy identification of events and individuals subject to specific processes covered by this right. These activities are entirely the responsibility of the data controller.

More information

Find out more about how ServiceNow Safeguards Customer Data

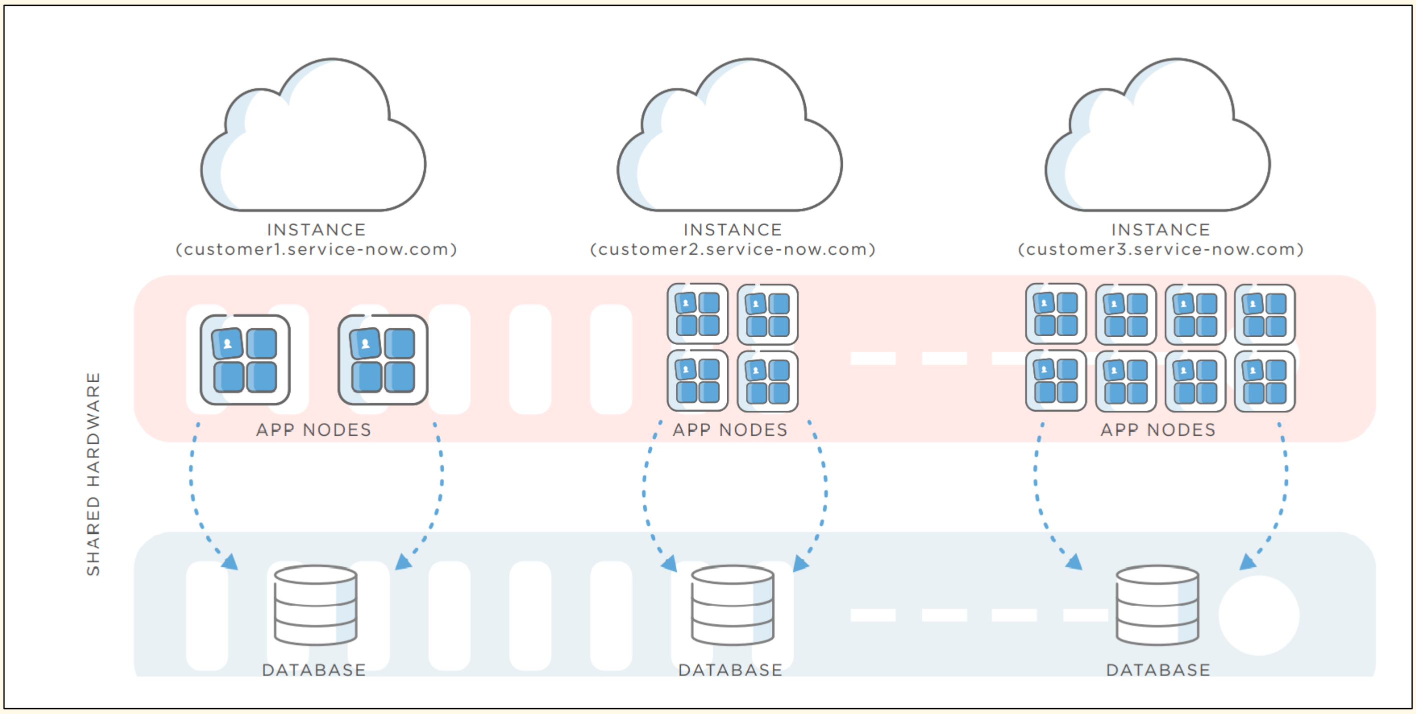
Physical & Logical Architecture

Contents

Multi-instance architecture

KB0959619

Instances of the Now Platform® are deployed on an advanced, multi-instance architecture that provides separate application nodes and database processes for each customer. This ensures that there is no possibility of co-mingling of customer data, even between instances assigned to the same customer, unlike multi-tenant architectures where a shared database is used.



Each instance runs its own application logic and database processes, meaning that an instance does not have to be on the same version or upgraded at the same time as other customers' instances. Customers can choose to upgrade their instances on a schedule that best meets their needs and compliance requirements. No downtime is necessary for upgrades.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Find out more about ServiceNow's Advanced High Availability Architecture

Data center physical security and environmental controls

KB0959425

Physical controls

Data centers procured by ServiceNow are provided by specialist colocation data center operators. These operators provide ServiceNow with a secure and reliable space to operate in. The data centers are highly secure facilities with 24/7 security guards, CCTV, multiple levels of entry controls, and strict procedures for physically entering the facility.

Data centers feature a hardened exterior perimeter with defense-in-depth provided by various access control boundaries. Within each data center, all ServiceNow equipment is stored in one or more dedicated, anonymous cage spaces or private suites.

The details of individual data centers may vary slightly; however, all facilities have similar operating characteristics. In all cases, contractually, the data center providers must be either ISO/IEC 27001:2013 accredited and/or conduct regular SSAE18 SOC 2 Type 2 audits.

Data center physical boundaries

All data centers have external anti-climb fencing, crash resistant walls, and data center halls that are not directly adjacent to exterior walls. Some locations also feature anti-vehicle bollards.

Data centers are divided into zones; these include public, internal, power, environmental, UPS and battery rooms, loading bays, and other zones. Although the detail of the zones will vary between the data centers, the principle is applied across them all. Access controls are applied to prevent movement of unauthorized data center staff between each zone in the data center.

The external perimeter of all data centers is lit to allow CCTV systems to provide detailed views of entrance and exit points. Some data center locations also include motion detection systems on the exterior. Within the data center physical boundaries, ServiceNow has its own dedicated cages or suites enabling isolation from other data center tenants, including biometric secondary access controls.

Physical intrusion detection

All data centers that ServiceNow operates from have extensive recording CCTV systems internally, as well as at the perimeter. Low light cameras and lighting are used to ensure that details such as facial features and number plates can be clearly identified, even at night. Typically, recordings are held for at least 30 days, although the length of recording varies from data center to data center. Only authorized personnel have access to the recording systems (controlled by ACL), and all access is audited. Entrances and exits are alarmed both externally for opening and internally for being jammed open. Exterior glass is alarmed for breakage, and data center floors are windowless.

Data center providers are contractually obliged to notify ServiceNow in the case of security incidents, and activities surrounding this obligation are assessed by audit.

Security guards

Appropriately cleared security guards are present at each data center. The security guards manage the exterior gates and reception areas/front desk, respond to alarms, and conduct scheduled and random patrols of the facilities. All security guards are trained in the operational procedures of the data center.

Facility access control

The data center operators control access to their facilities via multiple levels of locking mechanisms. While the precise details of the individual data centers vary, all data centers make use of a mixture of access control mechanisms, including mechanical, biometric readers, and access card readers requiring PIN entry. Data center access logs are retained for audit purposes, but the retention period varies across providers. Interlocking mantraps are used to control movement between reception areas and corridors that lead to data center floors.

Data center access control systems prevent staff from entering any area in which they are not permitted. ServiceNow maintains access control lists for its own cages and suites, only permitting limited access for data center personnel where absolutely necessary (i.e. for health and safety purposes).

Personnel access control

Logical access to the infrastructure hosting the ServiceNow cloud and all hosted customer data is granted only to ServiceNow personnel with the specific requirement to do so. Access where required is provided on a per-role basis, according to specific job functions and a least-privilege model and reviewed regularly.

In accordance with separation-of-duties good practice, ServiceNow personnel with physical access to data centers do not have logical access to data environments, and staff with logical access to data do not have physical access to data centers. The private cloud environment is both physically and logically isolated from ServiceNow's corporate environment and is also subject to different standards, policies, and governance reflecting its different purposes and dispositions. To manage the private cloud infrastructure, ServiceNow operational personnel must use a secure virtual desktop environment accessible only from ServiceNow issued endpoints identified by digital certificates. Access requires two-factor authentication and takes place within a virtual environment, from which employees cannot extract or copy data. Host-based data leak prevention (DLP) is enabled, SSH access to production servers is controlled using a proxy, and all user activity is controlled and monitored with a privileged access management (PAM) system.

ServiceNow does not outsource any service, operational, or management functions that would provide any third party with access to systems hosting customer data or to customer data itself. ServiceNow limits the infrastructure supporting its cloud's footprint to only those technologies, infrastructure, and components required to support the Now Platform.

Physical access audits

ServiceNow maintains and regularly reviews visitor access logs for its cages or suites. Both physical and electronic records of access are made, and ServiceNow requires its data center providers to supply these on a regular basis.

Electrical and environmental controls

ServiceNow's data centers are highly available facilities with redundant electrical and mechanical systems. While not formally accredited, the data centers are designed to operate equivalently to a minimum of the TIA942 Tier 3 standard.

Electrical systems

ServiceNow's data center providers typically offer between 99.999% and 100% power uptime. These levels of reliability are achieved through the use of redundant power providers where available, multiple redundant power distribution paths, generators, UPS systems, multiday fuel suppliers, and multiple independent fuel suppliers. These data centers can typically operate for at least 24 hours at full electrical load without the requirement of additional fuel. As data center pairs are generally geographically diverse, each data center receives power from a different supplier wherever possible. Generators and transformers in the data centers are at least N+1 enabled, with distribution networks being either N+1 or 2N. Within the data center ServiceNow will power devices from disparate distribution networks to ensure that loss of electricity supply on one power networks does not affect others. Uninterruptible power supply (UPS) is provided either by battery or flywheel systems that can sustain systems until generators can be activated.

Environmental controls

The heating, ventilation, and air conditioning (HVAC) systems in the data centers maintain the humidity and temperature within the data center at an optimal level. Data centers are N+1 redundant for all environmental controls. If humidity or temperature within a part of the data center breaches the parameters defined for that zone, alarms will be triggered, notifying building management to resolve the issue.

Fire detection and suppression

All data centers feature fire detection and suppression systems. The specific system implemented may vary among data centers.

Fire detection is provided by very early smoke detection apparatus (VESDA) and heat alarms that are monitored on a 24/7 basis. Fire suppression may be multi-zone, dry-type, double interlock pre-action, and zoned gaseous-based systems, or a combination of both. Fire extinguishers are located throughout the facilities, and exit signs are prominently displayed. Safe and mandatory disable of flammable materials (e.g. cardboard, polystyrene etc.) is also required in all data center location.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Can standard commercial customers have in-country only support?

KB0960232

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 the option of 24/7 customer support - with 12/5 as the standard offering - 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.

Where is customer data hosted?

KB0960200

Customer data is hosted only within their selected regional data center pair.

Regional data center pairs are pre-defined by ServiceNow.

There is no defined primary and secondary site within a DC pair.

Data center transfers are transparent to the end-user.

More information

Find out more about ServiceNow's Advanced High Availability Architecture

Is customer data transferred around the world?

KB0960205

No, data always remains in the customer's designated regional 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.

Where are ServiceNow's data centers located?

KB0960673

ServiceNow operates the following data center pairs:

Area	Data Center Locations
US Commercial	Santa Clara, CA and Ashburn, VA Sterling, VA and Phoenix, AZ
US Federal	Miami, FL and Culpeper, VA
Canada	Brampton and Calgary
Brazil	Campinas and Sao Paulo
UK	London (Slough) and Newport, Wales
European Union	Amsterdam, Netherlands and Dublin, Ireland
Germany (German customers only)	Düsseldorf and Frankfurt
Switzerland	Geneva and Zurich
Australia	Melbourne and Sydney
Japan	Tokyo and Osaka
Asia	Singapore and South Korea

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

KB0960203

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, ServiceNow does 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.

More information

Find out more about ServiceNow's Advanced High Availability Architecture

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

KB0960260

As is the case with most cloud service providers, ServiceNow does not allow 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, and 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.

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

KB0960202

By design, customer data is held within regional 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.

More information

Find out more about ServiceNow's Advanced High Availability Architecture

Can customers have dedicated or named support people only?

KB0960234

Qualified personnel are assigned to cases, rather than to 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.

More information

- Find out more about Data Access Controls and ServiceNow's Access Control Plugin
- Find out more about ServiceNow Access Control (SNAC)

Overview of physical architecture

KB0959421

ServiceNow's physical architecture supporting its private cloud is deployed into dedicated, ServiceNow-managed colocation spaces and is implemented globally. In these locations, ServiceNow's own onsite personnel exclusively provide management, installation, maintenance, and support. ServiceNow builds and deploys pre-integrated racks (PIRs) for all server and appliance infrastructure and cabling, and rack design standards are rigorously enforced. Within each space, multiple levels of redundancy are established for networking infrastructure, internal links, and related components. At a minimum, this network infrastructure is mirrored, both within a single colocation space and between ServiceNow data center pairs. Multiple diverse internet connections terminate within these spaces, providing redundant internet access. Servers, appliances, and network devices are multi-homed with redundant components and commodity supplies (i.e. power and network) fed from multiple separate circuits. Where supported, some data centers also feature electrical supply resilience across multiple grid suppliers.

Infrastructure operations management

As a cloud service provider (CSP), a significant element of ServiceNow's responsibilities is to provide and manage the underlying infrastructure on which instances of its Now Platform are deployed. A number of complementary activities and processes are undertaken in managing this environment, all using ServiceNow's own products:

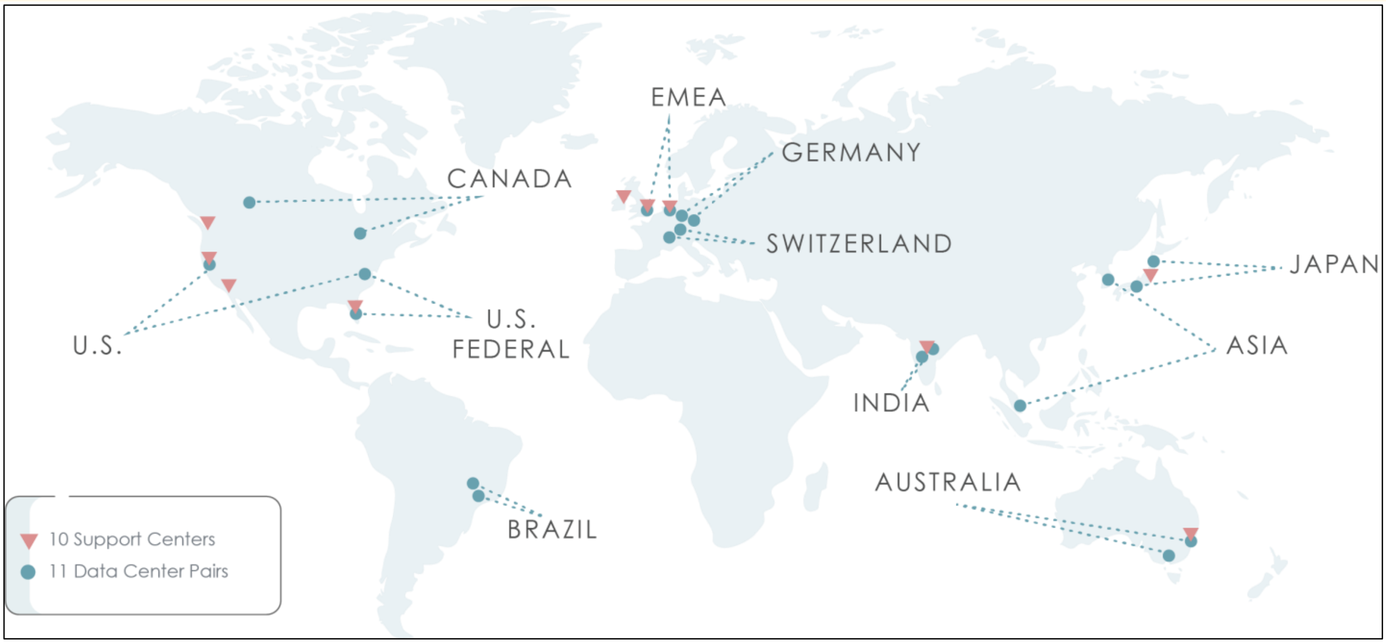
- A capacity management team ensures the private cloud is able to support current and reasonably anticipated future load.
- Continuous monitoring is undertaken to validate the configurations for each of the system and application components that make up the private cloud.
- ServiceNow adheres to a rigorous change management process that includes mandatory online training for all ServiceNow personnel with an operational role. Change management processes adhere to ITIL v3 principles.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Global data center pairs

KB0959422



ServiceNow's data centers are arranged in pairs. There are 10 support centers and 11 high availability data center pairs, spanning five continents: Asia, Australia, Europe, North America, and South America. All customer production data is stored in both data centers and kept in sync using real-time database replication. Both data centers are active at all times, each with the ability to support the combined production load of the pair. ServiceNow maintains continuous, asynchronous replication from the database in the current primary data center (read-write) to the secondary data center (read-only). ServiceNow uses top-tier global data center providers. These providers have no logical access to any ServiceNow systems or customer data and solely provide private colocation spaces and environmental resources. Only ServiceNow personnel with a direct responsibility for (or role in) maintaining colocation spaces are able to physically access data center locations. There are also pairs exclusively for qualified US Federal and Swiss banking customers. Meeting regulatory and sovereignty obligations is a significant factor in ServiceNow selecting data center facilities within specific geographic boundaries.

More information

- Find out more about ServiceNow's Advanced High Availability Architecture
- Customers can access the following data center resources:
    - Data Center Certifications
    - Data Center Media Handling SOP

Overview of logical architecture

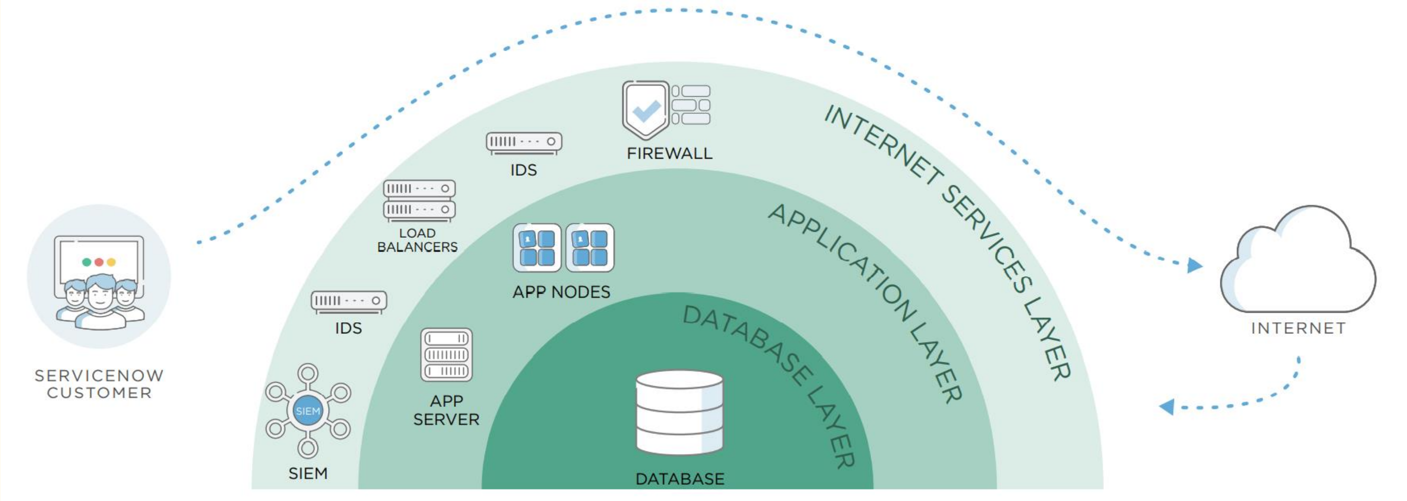
KB0959618

ServiceNow's highly defined and limited environment allows for a number of key benefits:

Automation: Many activities in the ServiceNow infrastructure are conducted entirely using automation with minimal to zero human interaction. For example, where ServiceNow provisions new instances for its customers, this is a completely automated process. Using this approach as an operational pattern creates consistent configurations and expected outcomes, and reduces the potential for, and impact of, human error.

Support, scalability, security: ServiceNow is solely focused on supporting one service: the Now Platform. This is deployed in a private cloud environment dedicated solely to this purpose, and implemented identically in all regions in which ServiceNow operates. The cloud environment supports thousands of identically provisioned ServiceNow instances allowing for significant economies of scale and operational agility. The security risks in a highly homogenous service are often more predictable and easier to manage than in highly diverse environments typical of many enterprises. ServiceNow is focused on only one thing, securing data processed within its infrastructure and instance of the Now Platform.,

Control: ServiceNow fully manages the underlying software, services, and supporting infrastructure as well as the software development lifecycle. This allows ServiceNow complete control over all components in its environment and vastly reduces supply chain risks.



Internet services layer (proxy layer)

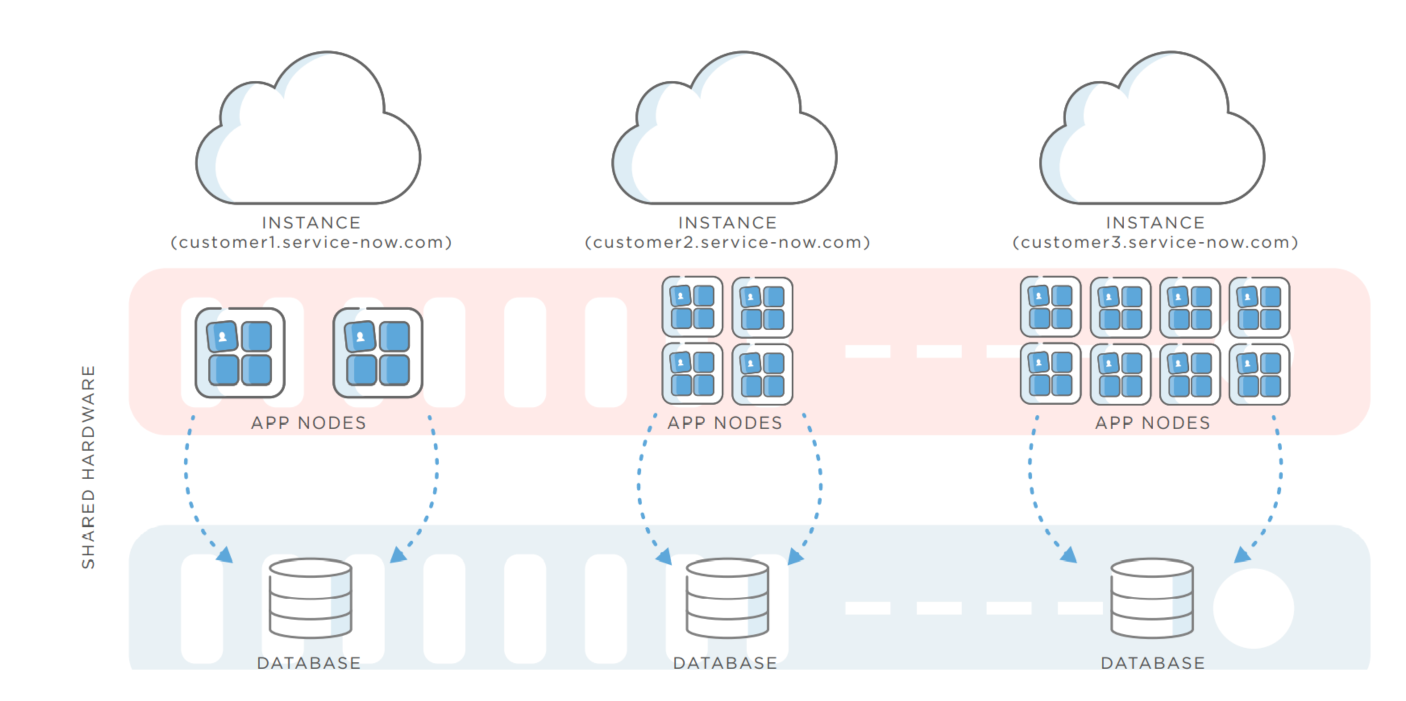
Customers and web services connect to the ServiceNow private cloud over HTTPS using TLS 1.2 for communication to and from a ServiceNow instance. All interactive end-user activities are performed using a standard web browser. There is no requirement for customers to install any client software on any desktop, laptop, tablet, or smartphone in order to access their ServiceNow instances. However, for additional convenience, ServiceNow offers native mobile apps for iOS and Android. The proxy layer forwards requests made from customers' end-users or integrations to the relevant customer instance. This first tier of the application architecture includes network routers, switches, load balancers, firewalls, and intrusion detection systems. All are deployed at a minimum 2N basis (a fully redundant mirrored system with two independent distribution systems). Translation of Universal Resource Identifiers (URIs) to ServiceNow internal IP addresses is performed in this tier.

Application layer

In this second tier are application servers in a discrete network segment accessed only via the proxy layer and not directly accessible from the internet. These servers host clustered application nodes for each customer's instance. ServiceNow instances are the termination point for all inbound requests made by end users of those instances. Requests are received and processed by application nodes (including being escaped or encoded as required) before passing to the relevant database service in the database server tier. Application and database servers have protections - such as host-based and network-level default deny firewall rules - in place to prevent host-level traffic from reaching the Internet.

Database layer

The third and final tier consists of database servers, again installed in a discrete, non-internet routable network segment. Requests from end users or integrations cannot be made directly to the database tier and are only issued from a customer's ServiceNow instance. Each instance has a single database present on a database server running multiple discrete and segregated database services. There is no co-mingling of any customer data between instances and databases: If a customer has four instances of ServiceNow, they will have four entirely separate databases and database services, one unique to each instance.



More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Data sovereignty

KB0959424

Data is subject to the laws of the country in which the data is physically stored and to the jurisdiction to which the data subject belongs (e.g. in the case of GDPR). ServiceNow ensures that data is hosted in data center (DC) pairs, where both members are either within the same jurisdiction or within mutually compatible jurisdictions so that even when data is transferred from one data center to another, the sovereignty of the data is preserved.

More information

- Find out more about ServiceNow's Advanced High Availability Architecture
- Find out more about how ServiceNow Safeguards Customer Data

Security Logging & Monitoring

Contents

Logging and monitoring ServiceNow security infrastructure

KB0959610

A key component of any security program is to maintain detective controls to monitor for potential threat actors and intrusion attempts into the ServiceNow cloud and corporate environments. ServiceNow has a formal, documented security incident response policy, process, and workflow. ServiceNow's incident response process includes event discovery, triage, escalation, notification (including customer notification), remediation, and post-mortem review.

If a customer's environment or data is impacted, the customer will be notified without undue delay. Contractual commitments can be viewed by accessing the DPA at ServiceNow/Schedules.

ServiceNow has deployed a redundant intrusion detection system (IDS) that monitors network traffic as it transits into its cloud network. Additionally, a Host and network-based Data Leak Prevention(DLP) system is used to guard against data transfer and exfiltration from corporate systems, and also between the Cloud and corporate networks. These systems feed into ServiceNow's security information and event management (SIEM) systems.

ServiceNow maintains separate SIEM systems for its corporate and cloud environments, with further logical separation for SIEMs tasked with network, device, and security events. Alerts and notifications are generated by the SIEM systems in accordance with pre-defined triggers and metrics. These are reviewed by a 24/7 security operations capability with global coverage.

ServiceNow tunes and adjusts monitoring to meet the specific characteristics of ServiceNow instances. For example, approved customer penetration tests need to be differentiated from illegitimate or malicious penetration attempts. The SIEM helps support the processes in place that enable ServiceNow security operations to undertake such determinations reliably and promptly.

Events, alerts, and relevant logs are also fed from other systems, including all servers, network devices, and ancillary systems into the SIEM. This allows ServiceNow to build and maintain a comprehensive manifest of the activities that are occurring in its environment on a day-to-day basis. Security alerts, events, multiple threat feeds, and other relevant information are stored and aggregated into an internal ServiceNow instance for ongoing management.

ServiceNow is responsible for managing its SIEM environment and securing the events within it. Separate teams are responsible for the configuration and maintenance of the logging infrastructure and the data it generates to ensure good separation of duties. Network event logs and infrastructure events are retained for a minimum of 90 days.

ServiceNow's security operations team is also responsible for completing daily checklists across a range of security domains, including privileged account usage, IDS alerts, file integrity monitoring (FIM), and database access. The daily checklists and captured events are managed through a ServiceNow instance. Any variances that are discovered are raised as incidents for tracking, notifications, and investigation.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

How long are logs available?

KB0960221

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

Can customers see ServiceNow's firewall and infrastructure logs?

KB0960219

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

Logging and monitoring ServiceNow instances

KB0959611

A ServiceNow instance generates detailed log and audit information regarding activities which take place within it. ServiceNow's default application logging capabilities include verbose transaction, client, event, email, and system logs.

Log information is stored, like all customer data, within tables in a customer's instance. As with any customer data, ServiceNow does not access this data during normal provision of its service. Customers manage and monitor the various logs in their instances as they would any other information within an instance.

Log and audit data is protected by access control rules in the same manner as all other customer data. Access to log information is usually limited to administrative roles only.

Logs and events can also be forwarded to a customer's own logging system or security information and event management (SIEM) environment. This can be achieved using the syslog probe, the MID server, or by making direct web service calls to the various log tables. Customers may also simply download or export log table entries or list views containing items of interest. These techniques allow for log and audit events to be stored within a customer's environment and retained according to the customer's specific requirements.

Transaction logs represent every click, view, and system event that occurs in an instance. These logs include a level of detail useful for customers when troubleshooting issues, as well as providing detailed intelligence on behaviors within an instance.

Event logs include the creation of an incident, or deletion of problem, or any one of a number of standard, pre-configured events. They may also be extended to contain customer defined events. A number of security-related events are also available in the event log. These include those recording successful login, failed login, security privilege escalation, and viewing of tables or records.

In addition to reviewing logs manually, workflows or actions can execute when a specific event or log entry is detected or a metric is reached, such as failed logins per minute or access to sensitive administrative roles. These actions could be to issue a notification via email, raise an incident to investigate the matter, or even perform an activity against an application, system, or device within a customer's network.

Audit history is the final aspect of activity logging and recording. This feature relates to recording all activities in respect to data and customizations within customer instances. For any particular table or field, audit history may be turned on (or off). The audit history feature then maintains a record of who made any change, when the change took place, and what was changed. A number of tables are audit-enabled by default, and audit history is perpetual for the lifetime of that record.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Overview of logging and monitoring

KB0959609

Most activities within an instance can be recorded in an audit log, and the Now Platform includes comprehensive access, event, and transaction logging.

The extent of logging is customer configurable, and detailed logging can be used to record and report on all activity within an instance. Logs can be reviewed directly within the ServiceNow instance or exported to a customer's security information and event management (SIEM) tool. Workflows or incidents can be automatically created based upon detected activity. Customers can also enable auditing for database tables to track and view details of any changes made to data at a record or field level.

ServiceNow collects and retains logs and events relevant to its entire cloud infrastructure, including information regarding requests made to instances of the Now Platform in order to detect potentially malicious actions or activities in relation to its service.

ServiceNow uses such log and event management in conjunction with its ongoing operational security and incident management processes.

This information is not available to customers within their ServiceNow instances. However, events that occur within a specific customer's instance are accessible to that customer through their instance logs. These events are also captured in ServiceNow's infrastructure logs.

Log type	Description
Transaction	All browser activity for an instance
Email and push	All email notifications and push messages sent from all instances within the system
Event	All system events that occur within the system
Import	Data import activity within the platform
Table changes	Changes made to all tables in the system
Outbound HTTP request	All outbound web services requests, such as REST and SOAP requests
Signature image	Electronic signatures for the HR signature pad
System	Warnings and errors for instance processes, records, and non-critical events, such as memory usage on the server machine

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Security Responsibilities

Contents

The shared security model

KB0959412

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 following table:

Responsibility	Customer	ServiceNow	Colocation (Data center providers)
Data management (classification and retention)	X		
Media disposal and destruction		X	
Backup and restore		X	
Authentication and authorization	X		
Data encryption at rest	X		
Data encryption in flight	X	X	
Encryption key management	X	X	
Security logging and monitoring	X	X	
Vulnerability management	X	X	
Business continuity and disaster recovery		X	
Secure SDLC processes	X	X	
Penetration testing	X	X	
Privacy	X	X	
Compliance: regulatory and legal	X	X	X
Infrastructure management		X	
Security management		X	
Secure configuration of instance	X		
Employee vetting or screening	X	X	X
Environment controls		X	X
Physical security		X	X

Data roles and responsibilities

KB0959376

As the ‘data controller,’ customers always retain ownership of their data and are therefore responsible for meeting the requirements of privacy legislation in the jurisdictions in which they operate and from which they collect personal data. If an individual requests information directly from ServiceNow regarding data that may be stored about them on the Now Platform, ServiceNow will always refer that individual to the customer.

ServiceNow fulfills the role of ‘data processor’ and complies with the associated obligations it entails. However, ServiceNow has no visibility of the conditions under which the data was collected by the customer, whether appropriate permission was obtained, or if it is being used in accordance with those conditions.

Regardless of how customers classify data that is stored in their instance, ServiceNow’s single operating and security model ensures that data is protected.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video
- Find out more about how ServiceNow Safeguards Customer Data

Security and Privacy Considerations by use case

Contents

IT service management (ITSM) security considerations

KB0959798

IT departments handle large quantities of data daily. This data includes requests related to incidents, problems, and changes, such as password resets, computer hardware issues, patch management, and maintenance. Information related to applications, systems, services, information assets, and infrastructure managed within ITSM is stored in the configuration management database (CMDB).

Effective ITSM relies upon maintaining accurate data and connecting business users, assets, processes, and more. Securing all aspects of that integration is essential. We understand that processes involving user-generated data can sometimes cause additional unnecessary but sensitive information to be collected. When this occurs, that additional information also requires identification and protection.

The data assets stored in the CMDB include information about the internal infrastructure of the organization and IT-related assets, such as server models, OS versions, patch levels, dependencies, and IP addresses. This key configuration data could be easily used to identify vulnerabilities in a system. While not directly enabling attacks, detailed maps of corporate infrastructure should be considered sensitive information. For this reason, it is vital that all data stored in the CMDB is properly protected at all times.

More information

Find out more about how ServiceNow Safeguards Customer Data

Human Resources (HR) security considerations

KB0959801

HR organizations store and process a wide variety of personal data that is of a highly sensitive nature, such as ID numbers, copies of passports, disciplinary data, or medical history. Employees may also confide in HR representatives about personal matters, including mental health and work/life balance. HR teams have a unique and important function within any organization, and due to the sensitive nature of the data connected to HR requests, we ensure that only authorized HR personnel are able to access such sensitive, personal information. Even the IT system administrators do not have authorization to access the data in the HR application.

HR departments typically use multiple systems and applications to manage core HR, benefits, payroll, recruiting, talent management, employee documents, and employee communications – sometimes all separately. Secure integrations into these existing systems are vital. ServiceNow currently supports a wide range of integration methods with third-party HR applications.

More information

Find out more about how ServiceNow Safeguards Customer Data

Customer service management (CSM) security considerations

KB0959802

ServiceNow offers a powerful CSM application on the Now Platform, which can unlock almost limitless possibilities for a company wanting to directly interact with its customers. Common requests, such as changes of personal details, password resets, and warranty registrations can be automated. The application is likely to handle large amounts of personal information. Any compromise of the confidentiality, integrity, and availability of this data could have severe consequences, especially in the case of highly sensitive information. We adhere to information security best practices in protecting this data.

Customers can browse service catalog items, request assistance, and participate in community groups to share experiences and solve problems. This functionality raises additional considerations for securing customer data. In particular, it is essential that controls are in place to manage the identification, authentication, and authorization of users, while keeping public and private access separate at all times.

More information

Find out more about how ServiceNow Safeguards Customer Data

Security operations product security considerations

KB0959803

ServiceNow has a thorough understanding of the security-based activities used to protect customers' environments and data, and uses the same practices in securing both its private cloud and its own internal corporate environments. These activities are essential components of a comprehensive approach to security and, by their nature, produce sensitive information about the organization. Information collected about vulnerabilities, threat vectors, security incidents patches, remediation, and the assets involved is highly sensitive and must be protected to reduce risk and exposure.

The ServiceNow security operations application integrates with many of the commercially available security tools customers already use and augments these tools to apply business service mapping and workflow automation. Most responsible organizations undertake security incident response, vulnerability management, threat intelligence, or governance risk and compliance (GRC) programs.

More information

Find out more about how ServiceNow Safeguards Customer Data

ServiceNow Security & Operations Management

Contents

Distributed denial of service (DDoS)

KB0959589

ServiceNow employs a significant range of detective controls to monitor and prevent potential distributed denial-of-service (DDoS) attacks from impacting the ServiceNow private cloud environment. This includes the implementation of in-house DDoS protection mechanisms, provision of significant Internet bandwidth connectivity, and the use of third-party protective services to mitigate against such attacks.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Operation system security

KB0959587

ServiceNow builds and maintains standard network device, appliance, and operating system build configurations. New devices and servers are deployed with automatic configurations relating to their function, and these are reapplied on an ongoing basis when changes are detected.

Controls relating to the monitoring of sensitive operating system files and restrictions on lateral movement across data centers are also in place. Anti-malware measures with regular updates are made to all servers within the private cloud, as well as all ServiceNow corporate IT systems and endpoints.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Infrastructure and application security services

KB0959588

ServiceNow has intrusion detection capabilities within its private cloud, and all relevant services and system components send security logs and events to a SIEM for security monitoring and alerting. See Security logging and monitoring – ServiceNow security infrastructure for more details.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Infrastructure vulnerability management

KB0959586

ServiceNow maintains an ongoing infrastructure vulnerability program using third-party commercial and in-house tools to identify vulnerabilities in the ServiceNow perimeter and for all cloud and corporate systems.

Identified vulnerabilities feed into the overarching vulnerability monitoring and remediation program. As necessary, patching of affected systems, services, or applications is undertaken promptly, in accordance with ServiceNow criteria and processes.

Infrastructure vulnerability scans occur daily for public facing infrastructure on an unauthenticated basis. Weekly scans are performed on an authenticated basis for internal, non-internet routable infrastructure.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Can customers perform load testing?

KB0960222

Customers may perform load testing only by pre-arrangement in 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 portal.

Can customers perform a penetration test on their ServiceNow instance?

KB0960223

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

Customers can schedule a new penetration test through the Schedule a Penetration Test catalog item.

All security testing outside this process is expressly forbidden.

More information

- Main Pen Test KB0538598 "Customer Instance Security Testing | Policy and Procedure"
- FAQ KB0953526 "Frequently asked security questions"
- Find out more in ServiceNow's Security Best Practice Guide and assess your security posture with the TuneUp Your Security catalog item
- The following resources are publicly available on the ServiceNow docs site:
  - Instance Security Hardening Settings
  - High Security Settings Plugin
  - Instance Security Center (ISC)

Secure software development

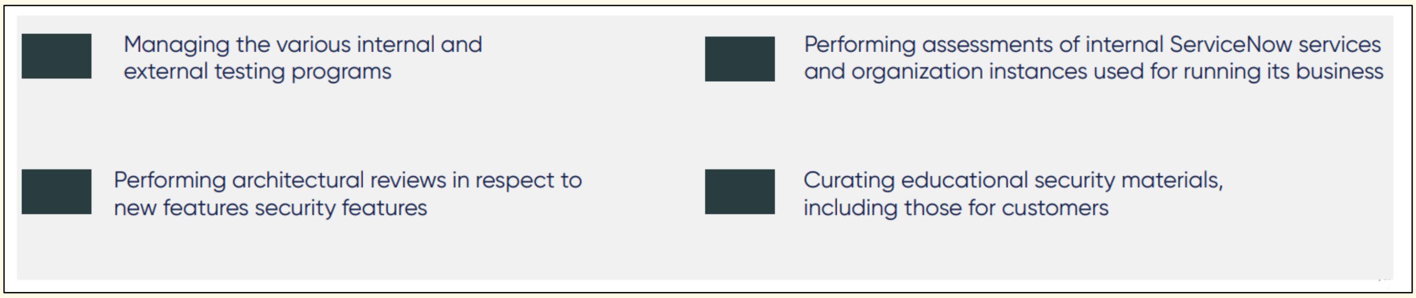
KB0959448

ServiceNow uses an agile development process that includes independent validation steps run by a separate quality team. A requirement of this process is to produce a validation report that includes security as a required signatory to the release process. This allows effective prioritization of remediation efforts and provides security feature requests into the application.

Developers and other relevant personnel are trained on an ongoing basis through a variety of methods, including classroom-based training that covers web application security.

Application security teams

ServiceNow Security Office (SSO) has dedicated teams of security engineers who are deeply integrated into the overall software development program. The teams perform a number of functions, including but not limited to:



- Managing the various internal and external testing programs
- Performing assessments of internal ServiceNow services and organization instances used for running its business
- Performing architectural reviews in respect to new features security features
- Curating educational security materials, including those for customers

Application security testing

ServiceNow's penetration testing program is a vital component of its development practices and is therefore wide-ranging and extensive.

Testing during development

During development, code for the Now Platform is subject to continuous ongoing testing and review within ServiceNow using a variety of methods. Third-party commercial and in-house automated tool sets, including static and dynamic application security testing, are used as well as manual testing and peer code reviews. These efforts are all specifically in relation to security and detection of vulnerabilities at the application code level.

Any validated security issue found is also checked for and, if necessary, remediated in supported versions of the Now Platform. This remediation is provided either in the next patch for that release or as a hotfix, subject to criticality.

Application penetration testing

After internal testing, external application penetration testing is carried out, providing independent review and transparency around ServiceNow's secure development practices. A third-party organization is given an extended period of time and access to the resources necessary to review and test the next release of the Now Platform before it is made available to customers.

On completion of a first round of testing, any confirmed issues are entered into the ServiceNow problem resolution process, prioritized, and categorized. Those whose impact and criticality meet pre-defined ServiceNow criteria are remediated prior to any re-testing.

Once the remediation completes, a second round of testing is conducted again by the same third-party organization. This is in order to confirm the provided remediation or mitigation functions as expected.

Results of the third-party testing are consolidated into an executive summary report accessible to customers from the ServiceNow Compliance and Operational Readiness Evidence (CORE) portal.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Customer application penetration testing

KB0959449

Another significant aspect of ServiceNow's application penetration testing program involves tests performed by its customers on their own ServiceNow instances, in accordance with a documented process. Customers are permitted to perform one penetration test per year.

Scheduling of testing must be pre-approved and conducted at a date and time agreed with ServiceNow. This is necessary to allow ServiceNow to continue to conduct its monitoring activities and be able to differentiate potential attacks from authorized customer testing.

As recommended testing prerequisites, customers should upgrade their instances to the latest release and patch version and implement ServiceNow's hardening guide. Testing without these prerequisites would likely result in false positive identification of previously identified issues. As a further condition of testing, customers are required to share the validated steps to reproduce any finding from their test with ServiceNow in accordance with the documented process.

Validated customer findings help contribute to the collective security of the ServiceNow environment and enable a continuously improving security posture, and the customer penetration testing scheme supports a significant number of tests annually across the customer base. Once validated by ServiceNow, confirmed vulnerabilities discovered by this process are remediated according to ServiceNow's vulnerability management criteria.

The release notes on the ServiceNow docs site for each major version, patch, and hotfix include information regarding what has been remediated in each release, including those that are security-related.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

UK Public Sector

Contents

How ServiceNow supports UK Public Sector customers

KB0960502

The UK Government introduced their ‘Cloud First Policy’ in 2013, and ever since departments have been looking to the cloud to provide effective and scalable solutions to support their business requirements.

To find out how ServiceNow can be successfully adopted to support the UK Government’s Cloud First Policy, including a detailed point-by-point response to the UK Government National Cyber Security Centre (NCSC)’s ‘Cloud Security Principles’ please see ServiceNow Security for the UK Public Sector.

More information

Find out more about ServiceNow Security for the UK Public Sector

How does ServiceNow support the UK Government's National Cyber Security Centre (NCSC) Cloud Security Principles?

KB0960282

The UK government has made considerable efforts to enable adoption of cloud services. A "Cloud First" policy was introduced in 2013 for UK public sector organizations and government departments when making technology decisions. Supporting guidance in the form of the Cloud Security Principles were first published in April 2014 by the Communications-Electronics Security Group (CESG), a UK government agency. The principles are currently available at the UK National Cyber Security Centre (NCSC).

The principles are intended to assist cloud service consumers with assessing and evaluating associated risks, and are aligned with ISO/IEC 27001, an internationally recognized information security management standard. ServiceNow has implemented an ISO/IEC 27001 information security management system (ISMS) in accordance with reference to and guidance from the ISO/IEC 27002 code of practice. As such, ServiceNow has been accredited as an ISO/IEC 27001:2013 certified organization.

More information

- Find out more about ServiceNow Security for the UK Public Sector
- View ServiceNow's ISO 27001 Certification (incorporating 27017/27018/27701)

Does all UK Public Sector data always remain in (and only accessed from) within the UK?

KB0960278

Data Protection regulations such as the EU GDPR and UK Data Protection Act (the UK implementation of GDPR) include provisions for data transfers. In the case of the Data Protection Act, transfers can include those to “third countries” outside of the UK.

ServiceNow customer data is not routinely transmitted or stored outside of the customer’s chosen data center region.

For the UK region, customer data centers are located in Newport, Wales and London (Slough), England. Customer data remains hosted within these locations in the UK at all times. However, incidental data transfers in conjunction with support activities undertaken by ServiceNow personnel from outside the UK may occur occasionally. This possibility is stated in the contractual agreements ServiceNow signs with its customers. ServiceNow is also able to contract that its provisions regarding data transfers are adequate through the use of Standard Contract Clauses (SCC), also known as EU Model Clauses.

More information

- Find out more about ServiceNow Security for the UK Public Sector
- View ServiceNow's Privacy Statement
- Find out more about how ServiceNow helps customers comply with the GDPR
- Visit ServiceNow's GDPR microsite

What classification of data can UK public sector customers store in the ServiceNow cloud?

KB0960281

Customers that are using ServiceNow's cloud to process 'OFFICIAL' and 'OFFICIAL-SENSITIVE' data have satisfied their own risk management process, the OFFICIAL handling principles and controls, followed the GOV UK and National Cyber Security Centre (NCSC) Cloud guidance, and successfully demonstrated to their accreditors that this is the case.

More information

Find out more about ServiceNow Security for the UK Public Sector

Are ServiceNow personnel security cleared (SC) to handle UK public sector data?

KB0960280

According to the UK Cabinet Office Government Security Classifications, data classified as 'OFFICIAL' only requires Baseline Personnel Security Standard (BPSS) or equivalent security clearance, not the more stringent ‘SC’or ‘SC Cleared’.

ServiceNow’s staff are background cleared to a standard equivalent to or exceeding BPSS, e.g. requiring 5 years of full background checks (as opposed to 3 years of employment checks only). It is on this basis that customers using ServiceNow for 'OFFICIAL' and 'OFFICIAL-SENSITIVE' classified data are able to proceed without the need for SC clearance.

More information

- Find out more about ServiceNow Security for the UK Public Sector
- Customers can access ServiceNow's Entitlement Review SOP
- The following resources are accessible by ServiceNow customers only:
    - IT Support Onboarding, Role Change, and Offboarding SOPs
    - HR Support Onboarding and Offboarding SOPs
    - Background Screening SOP
    - Training Policy
    - Training SOP

US Healthcare / HIPAA

Contents

How ServiceNow supports healthcare customers

KB0960504

ServiceNow has developed the Now Platform to include options and features that enable its US healthcare/HIPAA customers to comply with privacy and security requirements stipulated by law. These requirements include:

- Ensuring the confidentiality, integrity, and availability of electronic protected health information (ePHI) the organization creates, receives, maintains, or transmits as customer data
- Protecting against any reasonably anticipated threats and hazards to the security or integrity of ePHI
- Protecting against reasonably anticipated uses or disclosures of such information not permitted by the Privacy Rule

More information

Find out more about ServiceNow security and HIPAA

How do ServiceNow security controls support the HIPAA Security Rule standards (Subpart C of 45 CFR Part 164)?

KB0960284

The HIPAA Security Rule standards (Subpart C of 45 CFR Part 164) covers:

- Administrative, physical, and technical safeguards
- Organizational requirements
- Policies and procedures documentation
- Notification by a business associate
- Law enforcement delay
- Administrative requirements and burden of proof
- Uses and disclosures: organizational requirements

More information

Find out more about ServiceNow security and HIPAA

Does ServiceNow enter into a Business Associate Agreement (BAA) with HIPAA customers?

KB0960283

Under the Health Insurance Portability and Accountability Act (HIPAA), a business associate is an entity that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity. Covered entities are required to enter into a written contract or written arrangement with their business associates, often referred to as a business associate agreement or addendum (BAA).

ServiceNow satisfies its obligations as a business associate differently than traditional business associates. For example, some BAAs require business associates to provide an individual access to its ePHI within their "Designated Record Set" and within a prescribed period of time. However, customers are able to and responsible for providing access to individuals who request access to their ePHI directly by using the Now Platform and accessing the relevant information requested.

ServiceNow will enter into a BAA if the covered entity customer chooses to store electronic protected health information (ePHI) in their instance. However, while ServiceNow enters into a BAA with customers that may process ePHI within the subscription service, it is important to understand that ServiceNow is not a typical business associate. ServiceNow will not enter into a BAA that requires ServiceNow to carry out the customer’s obligations under HIPAA as the covered entity.

More information

Find out more about ServiceNow security and HIPAA

US Public Sector / FedRamp

Contents

Overview of ServiceNow FedRAMP and Government Community Cloud (GCC) environment

KB0960500

FedRAMP is the US Government Federal Risk Management Authorization Program.

Its purpose is to encourage the use of secure cloud services for government agencies (and non-governmental entities who have contracts with the US Government with contractual Defense Federal Acquisition Regulation (DFAR) requirements). Any cloud service processing, storing, or transmitting government data must be approved for FedRAMP.

ServiceNow supports FedRAMP customers with the ServiceNow Government Community Cloud (GCC), and is authorized for FedRAMP High and DoD Impact Level 4 data and workloads. The user community includes federal, state, local, and tribal governments along with regulated organizations that have a requirement to meet US federal government security standards.

Customers must demonstrate that they qualify for this environment by being validated through ServiceNow's GovCommunityCloud (GCC) approval program.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

How does the FedRAMP environment being physically separate from ServiceNow's commercial environment affect the way instances can be used?

KB0960238

There are some implications to the FedRAMP and commercial environments being physically separate:

- There can be no cloning of instances between commercial and FedRAMP clouds. Update sets can be used to migrate application changes from commercial to production environment and vice versa if required.
- Code migration, such as in the team development functionality, does not span between commercial and FedRAMP environments
- Development, test, and production instances typically all reside within the FedRAMP cloud. This allows simple code migration/cloning between development, test, and production instances. There is some flexibility dependent on need e.g. the development instance could be in the commercial cloud to allow non-U.S.citizens to be administrators in the instance

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

Does data in the Government Community Cloud (GCC) environment traverse the ServiceNow global infrastructure or remain in the US?

KB0960263

Data in the Government Community Cloud (GCC) environment remains within US borders. Customers in GCC are also responsible for controlling access to ServiceNow instance.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

Where can customers find documentation about the ServiceNow FedRAMP environment?

KB0960261

All ServiceNow FedRAMP-specific security documentation is stored within the ServiceNow boundary on the Kiteworks repository. Agencies can request access through the FedRAMP Program Management Office (PMO) by using the FedRAMP Package Request Form, quoting:

- Package Name: ServiceNow Service Automation Government Cloud Suite
- Package ID: F1305072116

Requests should be sent to info@fedramp.gov, asking for the 'FedRAMP High Authorization Package' in Kiteworks.

(Non-Government Customers should contact Customer Support and they will forward the request to ServiceNow's Field Security Team for follow-up).

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

When will ServiceNow's US DoD IL4 environment 'Provisional Authorization to Operate' (P-ATO) become a full 'Authorization to Operate' (ATO)?

KB0960674

The term 'Provisional Authorization' is used because the Joint Advisory Board (JAB) and the Defense Information Systems Agency (DISA) cannot accept risk on behalf of other System Owners. The FISMA legislation states that the agency executive that owns the data is required to accept the risk for all information systems that they use. Therefore, ServiceNow's authorization from the FedRAMP JAB and DISA will always be a 'Provisional Authorization', and does not in any way suggest that there are any issues with the service or lack of controls.

Who can use ServiceNow's FedRAMP Government Community Cloud (GCC) environment?

KB0960243

All US federal agencies (and some associated organizations) are able to use our Government Community Cloud (GCC) FedRAMP environment:

- US federal, state, local, and tribal government with registered .gov or .mil domain addresses
- Government consultants
- Federally funded research and development centers (FFRDCs)

Non-governmental entities who have contracts with the US Government with contractual Defense Federal Aquisition Regulation (DFAR) requirements may also qualify for the GCC environment at ServiceNow's discretion. Such organizations must demonstrate that they qualify for this environment by being validated through ServiceNow's GCC approval program, and contractually agree to the terms laid out in ServiceNow's United States Government Addendum (USG Addendum). Examples of non-governmental entities that may qualify for the GCC environment include:

- International Traffic in Arms (ITAR)
- Covered Defense Information
- Controlled Unclassified Information (CUI)
- Department of Defense (DoD) Unclassified Controlled Nuclear Information (UCNI)
- Department of Energy (DoE) UCNI
- Criminal Justice Information (CJI)
- Department of Defense Impact Level Data (up to DoD Impact Level 4)
- FedRAMP Data (up to FedRAMP High)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- Requirements imposed on organizations from US Federal Government agencies (i.e.,Department of Homeland Security, Department of the Treasury, Office of the Comptroller of the Currency, Centers for Medicare and Medicaid Services, etc.)
- Federal Acquisition Regulation and Agency Supplement (e.g., DFARS) clauses

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

Can customers use products from the ServiceNow App Store in their FedRAMP instance?

KB0960259

FedRAMP customers can use products from the ServiceNow App Store, although they are not within the scope of ServiceNow's FedRAMP authorization. FedRAMP customers must request a desired product in HIWAVE and 'accept the risk' that is outside ServiceNow's FedRAMP scope. Once acquired, customers must perform their own analysis on the product to determine whether it meets their security needs.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

Is ServiceNows FedRAMP offering authorized for the US Department of Defense (DoD) Impact Level 4 (IL4)?

KB0960241

ServiceNow has received the US Department of Defense (DoD) Cloud Provisional Authorization for Impact Level 4 (IL4).

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

What is the FedRAMP Customer Responsibility Matrix?

KB0960246

Securing a ServiceNow instance and the data it contains is a joint responsibility between the customer and ServiceNow, the cloud service provider (CSP). While ServiceNow has its own obligations for securing the platform and infrastructure, the FedRAMP Customer Responsibility Matrix outlines the actions a FedRAMP customer needs to take to operate their instances securely.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

Can mobile apps be used with the Government Community Cloud (GCC)?

KB0960253

Mobile apps for iOS and Android (including push notifications) are accredited for use with Government Community Cloud (GCC), and use appropriate security controls including FIPS 140-2 certified encryption.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

Are ServiceNow's emergency response management apps approved for FedRAMP customers?

KB0960255

ServiceNow's emergency response management apps received Joint Advoisory Board (JAB) approval for US Government customers (as of March 18, 2020) and can be used in the Government Community Cloud (GCC) environment. This applies specifically to:

- Emergency Exposure Management
- Emergency Outreach
- Emergency Self Report

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

Are ServiceNow's safe workplace apps approved for FedRAMP customers?

KB0960257

ServiceNow's safe workplace apps received Joint Advisory Board (JAB) approval for US Government customers (as of July 9th, 2020) and can be used in the Government Community Cloud (GCC) environment. This applies specifically to:

- Employee Health Screening
- Employee Readiness Surveys
- Workplace PPE Management
- Workplace Safety Management
- Safe Workplace Dashboard
- COVID-19 Global Health Data
- Contact Tracing
- Employee Readiness Core

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

What is ServiceNow's United States Government Addendum (USG Addendum)?

KB0960245

ServiceNow's United States Government Addendum (USG Addendum) forms part of the contract between ServiceNow and non-government entity customers who qualify for the Government Community Cloud (GCC) environment. The key points of the USG Addendum are:

- Administrative access to their ServiceNow instance(s) must be restricted solely to US citizens who have been adjudicated (security cleared)
- A chief information security officer (CISO) or equivalent must be designated
- Acceptable Use Policies must be in place

This is usually already in place if a customer is meeting Federal Acquisition Regulation (FAR) or Defense Federal Acquisition Regulation Supplement (DFARS) requirements.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

What are the benefits of the ServiceNow GovCommunityCloud (GCC)?

KB0960227

The ServiceNow FedRAMP GCC environment is a physically and logically separate environment at ServiceNow, offering all the security and functionality of the standard commercial offering, plus these additional benefits:

- Compliance with NIST SP 800-53 Revision 4 controls, per the FedRAMP High baseline
- Compliance with the DoD Impact Level 4 controls, per the DISA Cloud Computing SRG
- Full Disk Encryption (FDE) for data at rest as standard (this is an additional cost option in the commercial environment)
- US citizen support and administration
- Simplified path to ATO (Agencies can leverage ServiceNow's FedRAMP Provisional authorization to issue their own ATO)
- Continuous monitoring by the FedRAMP Program Management Office (PMO) - Annual assessment and penetration test against FedRAMP Third Party Assessment Organization (3PAO) standards. Annual penetration test by FedRAMP 3PAO. Monthly deliverables to the FedRAMP PMO: Vulnerability scans of operating system, database, and web applications. Inventory. Plan of action and milestones (POA&M).
- Customer responsibility matrix (Part of the FedRAMP Control Implementation Summary worksheet) - Provides information on controls with shared responsibilities. Guides customer actions needed for secure use of the ServiceNow FedRAMP cloud.
- Documentation Repository (Kiteworks) - This provides access to all authorization package documents, annual assessment results and monthly continuous monitoring submissions.

More Information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Customers can access the following FedRAMP resources:

- FedRAMP Government Community Cloud (GCC) environment
- FedRAMP Consolidated Playbook
- US Federal Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)

How is technical support provided for FedRAMP customers?

KB0960249

Technical support for FedRAMP customers is managed on a 24x7 basis by our dedicated federal government customer support team. Customer requests are placed and managed through the HIWAVE portal. All ServiceNow FedRAMP support staff are required to undergo a US government background check and are adjudicated by the federal government for a Public Trust designation.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

What are the differences between ServiceNow's FedRAMP and commercial data centers?

KB0960231

Security controls are generally implemented in the same manner in both commercial and federal environments. This simplifies management and operations. While functionality and application code are the same in ServiceNow's FedRAMP and commercial environments, there are some differences:

- There can be a delay in the availability of a major version release in FedRAMP due to the JAB approval process.
- Dedicated hardware is available as an option. However, unlike the commercial environment, this is not a pre-requisite for Full Disk encryption (FDE), which is included by default with all FedRAMP instances.

Some features are not currently available in FedRAMP:

- Benchmarks
- Document viewer
- Instance data replication

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

What are the customer obligations for using the ServiceNow FedRAMP environment?

KB0960247

Customers eligible for the FedRAMP environment must sign the ServiceNow United States Government (USG) Addendum and also adhere to the recommendations in the Customer Responsibility Matrix.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Is ServiceNow classified as an electronic telecommunications provider for FISA (Foreign Intelligence Surveillance Act) purposes?

KB0960264

ServiceNow is not classified as an electronic telecommunications provider for FISA (Foreign Intelligence Surveillance Act) purposes. ServiceNow is classified as a SaaS (Software as as Service) Cloud Provider. We do not transmit, handle, or process 'signals' in the context of FISA. We are a platform that stores data in records, executes workflows but more importantly processes 'tasks'.

More information

- Visit ServiceNow's National and Federal Government microsite
- Find out more about how ServiceNow supports FedRAMP customers
- Register for the webinar Transitioning to ServiceNow's GovCommunityCloud
- Find out how to access the US Federal Security Compliance Authorization Package

Vulnerability Management

Contents

Now Platform vulnerability management

KB0959591

ServiceNow produces two releases of the Now Platform annually. In addition, patches and hotfixes are produced throughout the supported lifetime of a major release and rolled into the codebase for inclusion in the next version.

To ensure customers are benefiting from the most current security, performance and functional fixes, ServiceNow will apply patches to customer instances on a continual basis as part of the new ServiceNow Patching Program. Each quarter, one full patch and two security patches will be automatically scheduled to update your instance(s).

An instance of ServiceNow may continue to be used while a major release upgrade, patch, or hotfix installation takes place. Patch application leverages the Advanced High Availability capability and results in minimal impact to service where any update is applied.

ServiceNow requires customers to remain on a supported release of the Now Platform and will actively engage with customers' risk and security personnel to highlight the risks of non-compliance.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Cloud infrastructure vulnerability management

KB0959592

Findings reported from the continuous scanning of its infrastructure by ServiceNow's vulnerability management tools are automatically logged within an internal ServiceNow instance. These are first reviewed by ServiceNow personnel to determine that the appropriate level of priority is assigned, taking into factors such as relevant mitigating controls and exposure. Those issues identified at the highest risk classification level will be targeted for remediation as quickly as possible.

ServiceNow's infrastructure stack is customized at each layer to specifically support the Now Platform. Publicly identified vulnerabilities in common software platforms (e.g. CVEs) may not necessarily present a risk within the context of the Now Platform. This can be due to factors such as absence of the affected software or component in the ServiceNow environment or its limited or complete inability to access the Internet.

Once it is determined that a patch needs to be deployed, this effort enters the change management process. During this process, the assets, risk, and potential impact to the relevant environment are identified along with the testing required, back-out plan, and timeline for deployment. Where no clear remediation is available virtual patching is implemented.

ServiceNow leverages the Advanced High Availability architecture to transfer customers' production instances between data centers when performing infrastructure maintenance such as patching, thereby minimizing the impact to availability.

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 customers discover a vulnerability, they should report it to ServiceNow in a responsible manner per the Responsible Disclosure Program.

More information

- Find out more about how ServiceNow secures the Now Platform
- Watch the Cloud Security at ServiceNow: What you should know webinar
- Watch ServiceNow's Overview of Platform Architecture video

Do software updates and patches happen automatically?

KB0960226

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.

More information

Find out more about ServiceNow's Patching Program

What should customers do if they discover a vulnerability?

KB0960225

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.

More information

Find out more about ServiceNow's Responsible Disclosure Program

Can customers roll back an update?

KB0960230

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

More information

Find out more about ServiceNow's Patching Program

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

KB0960229

Major platform version updates are typically released twice per year

ServiceNow will notify customers in advance of upcoming patches

One full patch version and two incremental security patches are released each quarter

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)

More information

Find out more about ServiceNow's Patching Program

Why do instances need to be patched?

KB0960228

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.

More information

Find out more about ServiceNow's Patching Program