Data Access Controls

A look at ServiceNow’s access to customer data
Table of Contents

Introduction ................................................................................................................................. 3
Customer data access and processing ......................................................................................... 3
  Customer access ......................................................................................................................... 3
  ServiceNow access and processing ......................................................................................... 3
Customer Controls ...................................................................................................................... 5
  ServiceNow Access Control Plugin (SNAC) ........................................................................ 5
  High Security Plugin ............................................................................................................. 5
  Authentication and Access Controls ...................................................................................... 5
Monitoring ................................................................................................................................... 6
  Activity Logging ..................................................................................................................... 6
  Instance Security Center ......................................................................................................... 6
  Contextual Security Auditor .................................................................................................... 6
Cloud service providers: Common processing practices .............................................................. 6
Conclusion .................................................................................................................................. 7
Additional Resources ................................................................................................................ 7
Introduction

Please note, all information in this document is related to the standard Now Platform commercial environment. For information related to ServiceNow’s in-country cloud offerings around the globe and how they may differ, please contact your ServiceNow account representative.

The ServiceNow platform enables customers to store a wide range of data, some of which – e.g. Asset, HR, and Security data – could be considered highly sensitive. ServiceNow counts many of the world’s largest companies among its customers. We provide services to a wide range of organizations globally, some of which are in tightly regulated industries, like national and local government, financial services, and healthcare.

Customers naturally have concerns about data privacy and security, and in particular about who can access the data once it is stored in ServiceNow’s cloud. This document gives an overview of the controls and features that ServiceNow has implemented to ensure that customers are in control of how their data is used by ServiceNow. It also explains how we structure processing of customer data when it comes to access, infrastructural integrity and customer control.

ServiceNow utilizes our global network of locations, technology and employees to provide our services. The approach that we (and the specific ServiceNow entities who act as sub-processors) take, is covered in detail in our Data Processing Addendum.

As a Data Processor, ServiceNow provides the tools that enable customers to secure and audit their instance to their requirements.

Processing has an extremely wide meaning in the context of data protection legislation such as the General Data Protection Regulation (“GDPR”) and so the term includes any set of operations performed on data, including storage, hosting, structuring, adaptation, alteration, retrieval, consultation, consultation or deletion of data.

We have described our stringent, industry-standard practices and processes for maintaining the security of our infrastructure and your data in the ServiceNow Assurance Pack (SNAP), which we recommend you read before progressing further in this document. In particular, the documents titled “Safeguarding Your Data – Data Privacy” and “Safeguarding Your Data – Asset Data” are critical to your understanding of how ServiceNow handles customer data.

The ServiceNow platform is under constant scrutiny from our dedicated Security Operations team who look for unusual or malicious activity.

Customer data access and processing

Customer access

As the Data Controller, the customer determines what data is stored in their ServiceNow instances and who has access rights to it. Tools such as Access Control Lists (described later in this document), enable customers to define access permissions.

ServiceNow access and processing

ServiceNow does not access customers data within their ServiceNow instances except where necessary for the purposes of providing customer support. Access occurs on a case-by-case basis and is strictly controlled, with activity being logged and monitored. Customer data
accessed incidentally during support activities is not processed outside what is permitted contractually or under relevant statutory obligations such as GDPR.

Select ServiceNow employees may need to access the ServiceNow cloud infrastructure for administration and management of servers, databases and other components used to provide the service. All SSH access is controlled using a proxy, and a centralized Privileged Access Management (PAM) solution is used to manage authorization and monitoring of any commands requiring elevated privileges. Many of the common administrative functions and processes relevant to these are entirely automated. Operating system patching, service and device configuration, and deployment of new hardware and software utilize automations as far as is possible. Actual processing of customer data in these scenarios is often minimal or does not take place at all and is limited by contractual agreement and adherence to our statutory obligations.

In respect to instances of the Now Platform upgrades, patching, and restoration from backup are examples of tasks where automation is also extensively leveraged, with no human intervention. These processes are either initiated, requested or approved by a customer. They take place solely within the same region as the respective instance and require no external data transfer or offshore resources to complete.

ServiceNow manages the privileged entitlements to the infrastructure by job roles and performs a review of privileged access quarterly to ensure correct entitlements are in place.

Critical resources and files are protected by mandatory access controls available in SE Linux Preventive Mode. File Integrity Monitoring is also enabled for critical & sensitive files.

All infrastructure changes are required to go through a series of Change Management Procedures, including approval from the Change Advisory Board.

**ServiceNow Controlled Access (SNCA)**

ServiceNow support employees follow strictly controlled procedures on the occasions they are required to access a customer instance of the Now Platform. These define which employee roles can be approved for access, how specific authorization is granted on a per-instance and per-employee basis, and how those personnel connect to the customer instance. Access is temporary and only granted after an incident or change request is assigned to an employee. The access is revoked once the activity is closed or reassigned.

Once appropriate approval has been obtained, access is provided via the SNCA solution. SNCA consists of a regionally deployed, secure virtual desktop environment, which can only be accessed after a user authenticates with two-factor authentication from ServiceNow address space with a device identified by a digital certificate.

No internet access, email or messaging is possible from the virtual desktop environment. No data transfer such as file transfers, copy/paste functionality or device/USB redirection can occur between the virtual environment and host endpoint, and a host-based Data Leak Prevention (DLP) system is used.

**SSH (Secure Shell) access**

Access to the ServiceNow cloud infrastructure is only permitted through controlled and encrypted SSH sessions initiated over an MFA-VPN. The SSH sessions are decrypted for auditing so all session activity can be fully monitored and recorded. Infrastructure log data is forwarded to a central Security Incident and Event Monitoring (SIEM) solution for analysis, reporting, and alerting.

SSH access privileges are distinct and separate from those for SNCA, and only the minimum required privileges are granted for the specific task.
Customer Controls

ServiceNow Access Control Plugin (SNAC)

ServiceNow support employees follow strictly controlled procedures on the occasions they are required to access a customer instance of the Now Platform. These define which employee roles can be approved for access, how specific authorization is granted on a per-instance and per-employee basis, and how those personnel connect to the customer instance. Access is temporary and only granted after an incident or change request is assigned to an employee. The access is revoked once the activity is closed or reassigned.

Customers may also use the ServiceNow Access Control plugin (SNAC) for further control over which ServiceNow employees can access their instance, and when. Once this is activated, access permissions must be explicitly granted to a user, including defining a timeframe for access to occur in. Customers can revoke access at any time.

Any login events are recorded, and if successful, all subsequent activity is logged in detail in the Event and Transaction logs, described later in this document.

Customers should be aware that the SNAC only restricts ServiceNow personnel’s access to customer instances of the Now Platform. It does not apply similar restrictions for access by select ServiceNow personnel to the cloud infrastructure on which all Now Platform instances are provisioned on.

High Security Plugin

To help customers to secure their instances more easily, we provide the High Security Plugin. This is a tool for enhancing security Management and configuration and is activated by default on all new instances. The plugin enables High Security Settings, which centralizes critical security settings, creates a distinct Security Administrator Role, and exposes other security properties. It also enables a Default Deny security posture, which prevents use of read, write, create, and delete functionality for all tables, unless explicit permission is given an Access Control List rule (see below).

Authentication and Access Controls

Before any access to an instance is granted, every user must have their identity verified against a user account defined within the instance. User accounts, groups, and memberships can be created manually or imported from an existing directory service.

A selection of authentication mechanisms are available. Basic or Native authentication uses local accounts defined within the instance, while SAML 2.0, LDAP, OAuth2.0, and certificate-based authentication enable integration with external services. Multi-provider Single Sign On (SSO) allows the possibility of combining SSO with other authentication methods including Open ID Connect (OIDC). OIDC allows users to authenticate using third party credentials such as from Google, Azure, Okta or others. For high-security environments, customers can use Personal Identity Verification (PIV) card or Common Access Card (CAC) authentication. This is an extension of certificate-based authentication, with certificates stored on a smartcard.

Once a user has successfully authenticated, access to parts of the instance interface, functions, and the data within it are controlled with Access Control Lists (ACLs) and Role Based Access Control (RBAC). ACLs use the account ID and associated Groups to determine what access should be granted to an object, e.g. read, write, delete, create.
Various Roles can be defined within an instance. These might cater to different types of users, or different job roles. User accounts and groups are assigned to Roles, and permissions are applied to the Roles with ACLs to form RBAC Rules.

**Monitoring**

*Activity Logging*

ServiceNow instances generate detailed logs recording various aspects of operation. These logs are stored within the instance itself, are immediately visible to customers, and benefit from the same level of security as other data in the instance – they cannot be inspected by ServiceNow employees without permission. Event and Transaction Logs can be a valuable source of security information and can reveal details of any user’s activity. Any access or actions taken by ServiceNow support are always logged under the employee name in the format ‘first.last@SNC’. Logs can be inspected manually or analyzed with a tool such as a SIEM, which could also be used to trigger alerts.

The Event Log records system activity, including login events (successful or otherwise) and privilege escalation; Transaction Logs record all web-browser activity for an instance; System Logs show general activity, including configuration changes, system errors, workflows, and data connections. These logs can be helpful in identifying unusual or malicious 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.

**Instance Security Center**

The Instance Security Center enables customers to monitor and evaluate the security of their instance. It provides a straightforward, easily digestible Dashboard and a Compliance Score representing the overall security level of the instance. From here, customers can monitor and drill into activity such as admin-level or failed logins and navigate directly to relevant configuration pages, e.g. access controls and logging.

**Contextual Security Auditor**

Customers can check which users have access to which database tables, and to what degree, using the Contextual Security Auditor plugin. This is an interactive tool which evaluates table access permissions and displays them in an easily understandable format.

**Cloud service providers: Common processing practices**

Cloud service providers (CSPs) must offer technical support for the services offered to their customers. This is commonly provided via regional support centers on a follow-the-sun model. This means that outside of local working hours, support may be provided from another region.

A customer’s data may be accessed during support activity performed on their behalf – either directly, in the course of addressing an issue related to that data – or incidentally, whilst resolving an unrelated matter such as infrastructure configuration.

Many cloud providers including ServiceNow, factor these requirements into their services and reflect this in their customer contracts. Each has mechanisms to permit authorized, controlled, and monitored access and processing of customer data, and for safe transfers to take place when and where they occur.
These arrangements are intended to ensure access to, or processing of customer data only takes place under specific circumstances, and in accordance with customer understanding, agreed contractual commitments, and relevant statutory obligations.

The safety and security of customer data is our highest priority, and this includes when it is processed outside of its originating region. Compliance with and provision of EU standard (model) contract clauses, aim to ensure that data access and processing are in alignment with statutory regulations like the GDPR.

**Conclusion**

Understandably, customers may have concerns about ServiceNow’s access to their data. In anticipation of this, we have provided customers with granular controls and extensive logging and monitoring capabilities to put data security and access auditing in their hands. We have also implemented technical and procedural measures to prevent unauthorized access to data.

We have consistently demonstrated our commitment to data access security through our third-party compliance audits and the various accreditations we have achieved. Customers can be assured that their data is kept safe and private when using the ServiceNow platform, in line with the commitments we make in our customer contracts, regardless of where it is processed.

**Additional Resources**

- [ServiceNow Assurance Pack (SNAP)] – detailed information about ServiceNow’s Platform Security
- [Securing the Now Platform eBook] – a ServiceNow security and compliance overview
- [CSP practices for customer data access and transfers]
- [Cloud Security, Trust and Compliance Center]
- [Trust Site]
- [ServiceNow legal schedules]
- [Product Documentation]
- [www.servicenow.com]