Data Access Controls

A Look at ServiceNow’s Access to Customer Data
Table of Contents

Introduction .................................................................................................................................................. 3
Access to Data ........................................................................................................................................... 3
  Customer Access .................................................................................................................................. 3
  ServiceNow Access ............................................................................................................................... 3
Customer Controls .................................................................................................................................... 4
  ServiceNow Access Control Plugin (SNAC) ......................................................................................... 4
  High Security Plugin ............................................................................................................................. 4
  Authentication and Access Controls ..................................................................................................... 4
Monitoring .................................................................................................................................................... 5
  Activity Logging ................................................................................................................................... 5
  Instance Security Dashboard ................................................................................................................ 5
  Contextual Security Auditor .................................................................................................................. 5
Conclusion ................................................................................................................................................... 5
Additional Resources ............................................................................................................................... 6
Introduction

The ServiceNow platform enables customers to store a wide range of data, including Asset, HR, and Security data, which could be considered highly sensitive. ServiceNow counts over 850 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 questions about data privacy and security; specifically, 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 there is no unauthorized access by employees or anyone else.

We have described our stringent, well-recognized 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.

Access to Data

Customer Access

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

ServiceNow Access

As the Data Processor, ServiceNow provides tools for customers to secure and audit their instance according to their requirements.

In general, ServiceNow does not access customer data. It is, however, sometimes necessary for customer support activities. If it is required, access occurs on a case-by-case basis and any access is strictly regulated.

ServiceNow Controlled Access (SNCA)

Strictly defined procedures are followed when ServiceNow employees are required to access a customer instance. These help to control which employees can have access, how authorization is granted on a per-instance and per-employee basis, and how those personnel connect to the customer instance. Temporary access is only granted after an incident or change request is assigned to an employee and is revoked once the item is closed or reassigned.

Access can only take place via the SNCA solution, which comprises a predefined secure Virtual Machine (VM) and Virtual Private Network (VPN), authenticated with Multi-Factor Authentication (MFA). The VM image is security hardened and limits access to any systems outside of the ServiceNow Cloud infrastructure. There is no email access and no data transfer is possible between the VM and host machine, including file transfers and copy/paste functionality. Web access is filtered and restricted to approved sites. Only centrally-controlled and authorized applications can be installed within the VM.
SSH (Secure Shell) Access

Any required access by ServiceNow employees to the ServiceNow cloud infrastructure can only be performed through controlled SSH sessions. These can only be initiated over an MFA-VPN. The SSH sessions are controlled, decrypted, and then audited so all session activity can be fully monitored and recorded.

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)

Customers can use the ServiceNow Access Control plugin for granular control over which ServiceNow employees can access their instance, and when. Once this is activated, access permissions must be explicitly granted to a user with a defined timeframe. 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.

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. Activating 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 others enable integration with external services. Multi-provider Single Sign On (SSO) allows the combination of SSO with other authentication methods.

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 Dashboard

The Instance Security Dashboard 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.

Conclusion

Understandably, customers may have concerns about ServiceNow’s access to their data. In anticipation of these concerns, 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.
Additional Resources

- ServiceNow Assurance Pack (SNAP) – detailed information about ServiceNow’s Platform Security
- Delivering Secure, Scalable, and Compliant Cloud Services eBook – a ServiceNow Security and Compliance overview
- Trust and Compliance Center
- Product Documentation
- www.servicenow.com