ServiceNow Government Community Cloud (GCC) and FedRAMP

How GCC helps customers meet their FedRAMP requirements

Release: Washington, DC
Document Summary

This document outlines the security and privacy controls available for national and federal agencies using the ServiceNow Government Community Cloud (GCC) to meet the U.S. government’s Federal Risk and Authorization Management Program (FedRAMP®) requirements.

This document is designed to be read alongside Securing the Now Platform which gives a holistic overview of the physical, administrative, and technical controls ServiceNow has in place to protect customer data.

The information in this document is not meant to serve as an exhaustive attestation of ServiceNow compliance with FedRAMP security and privacy requirements; covered entities should contact their sales support at ServiceNow directly for further GCC-related queries.
# Table of contents

Document Summary .................................................. 2

The ServiceNow Government Community

Cloud (GCC) environment ............................................. 4
  ServiceNow FedRAMP Authorization .......................... 4
  The GCC Customer Responsibility Matrix ....................... 5
  Benefits of the GCC ............................................. 5
ServiceNow GCC vs. the standard commercial cloud ......... 6
  Implications of the GCC and the ServiceNow commercial cloud being physically separate .................................. 6

Who can use the ServiceNow FedRAMP GCC environment? .......................................................... 7
  Non-federal customers and the GCC environment ........ 7
  Obligations for using the GCC environment ............... 7
  The United States Government (USG) Addendum ........... 8

Using apps in the GCC environment ................................. 8
  Products from the AppStore ...................................... 8
  Mobile apps .................................................... 8
  Technical support for GCC customers .......................... 8
  Documentation for the ServiceNow GCC environment .... 8

Conclusion ...................................................................... 9

Resources ...................................................................... 9
The ServiceNow Government Community Cloud (GCC) environment

The ServiceNow GCC environment is a FedRAMP-authorized cloud platform made up of a specialized operating environment and application suite:

- **The ServiceNow GCC environment**
  A Continental United States (CONUS)-based dedicated infrastructure (**facilities, servers, databases, networking devices**) to process, store, and transmit government information using a multi-instance architecture.

- **The Now Platform**
  A collection of natively integrated applications designed to support IT service automation, resource management and shared support services.

The ServiceNow Government Community Cloud (GCC) was granted a Joint Authorization Board (JAB) Provisional Authorization to Operate (p-ATO) with a High system categorization on August 12, 2019 and was approved at the U.S. Department of Defense Impact Level 4 on October 6, 2019.

GCC 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 U.S. Federal Government security standards.

Customers must demonstrate that they qualify for this environment by being validated through the ServiceNow Government Community Cloud GCC approval program.

**ServiceNow FedRAMP Authorization**

For the ServiceNow FedRAMP authorization, click [here](#).
The GCC Customer Responsibility Matrix

Securing an instance of the Now Platform and the data it contains is a joint responsibility between the customer and ServiceNow, the Cloud Service Provider (CSP).

The GCC Customer Responsibility Matrix outlines the actions a GCC customer needs to take to operate their instances securely.

Benefits of the GCC

The ServiceNow 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 by default**
  - This is an additional cost option in the commercial cloud environment
- **U.S. person support and administration**
- **Simplified path to Authority To Operate (ATO)**
  - Agencies can leverage the ServiceNow FedRAMP Provisional authorization to issue their own ATO
- **Continuous monitoring** by the FedRAMP Program Management Office (PMO)
  - Annual assessment by FedRAMP Third Party Assessment Organization (3PAO)
  - 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 GCC
- **Documentation repository**
  - This provides access to all authorization package documents, annual assessment results, and monthly continuous monitoring documentation
ServiceNow GCC vs. the standard commercial cloud

With the exception of the benefits listed on the previous page, security controls are generally implemented in the same manner in both the standard commercial and GCC environments. This simplifies management and operations.

However, although functionality and application code are the same in both environments, there are some differences:

• There can be a delay in the availability of a major version release in GCC due to the JAB approval process.
• Some features may not be currently available in GCC. This changes over time and is tracked for customers in a knowledge base article in the dedicated support portal for GCC customers. Currently this list includes:
  – Benchmarks
  – User Experience Analytics

Implications of the GCC and the ServiceNow commercial cloud being physically separate

There are some implications to the GCC and commercial clouds being physically separate:

• There can be no cloning of instances between commercial and GCC clouds.
  – Update sets can be used to migrate application changes from commercial to production environment and vice versa.
• Code migration, such as in the team development functionality, does not span between commercial and GCC environments.
• Development, test, and production instances typically all reside within the GCC 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. persons to be administrators in the instance.
Who can use the ServiceNow FedRAMP GCC environment?

All federal agencies (and some associated organizations) can use our GCC environment:

- U.S. federal, state, local, and tribal governments with registered .gov or .mil domain addresses
- Government consultants
- Federally Funded Research and Development Centers (FFRDCs)

Non-federal customers and the GCC environment

Approval for organizations other than U.S. Federal Government entities or instrumentalities to access the GCC environment is solely at the discretion of ServiceNow. Such organizations must demonstrate that they qualify for this environment by being validated through the ServiceNow GCC approval program.

Specifically, any organization other than U.S. Federal Government entities or instrumentalities must meet the following criteria before ServiceNow can consider provisioning such organizations in the GCC environment:

The organization must demonstrate they have a requirement to meet U.S. Federal Government security standards by contractually agreeing to the terms in the ServiceNow United States Government (USG) contract addendum.

Below are examples of U.S. Federal Government data types, contract clauses, and security standards that may demonstrate that an organization other than U.S. Federal Government entities or instrumentalities are required to be included in the ServiceNow GCC environment:

- 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 U.S. 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

Obligations for using the GCC environment

Eligible customers must sign the ServiceNow United States Government (USG) Addendum and review the recommendations in the GCC Customer Responsibility Matrix.
The United States Government (USG) Addendum

This form is part of the contract between ServiceNow and customers wishing to use the GCC environment. The main points of the USG Addendum are:

- Administrative access to customer instances of the Now Platform in GCC must be restricted solely to U.S. persons who have been adjudicated (security cleared)
- The customer must have a Chief Information Security Officer (CISO) or equivalent position designated
- The customer must have an Acceptable Use Policy in place

Note: Most of these items are typically in place if the customer is meeting the Federal Acquisition Regulation Supplement (FAR) or Defense Federal Acquisition Regulation Supplement (DFAR) requirements.

Using apps in the GCC environment

Products from the AppStore

ServiceNow has a separate app store for use with GCC, known as the FedAppStore. The FedRAMP authorization for the ServiceNow Government Community Cloud (GCC) covers the GCC system and the ServiceNow developed code, including apps developed by ServiceNow in the FedAppStore.

Third-party developed applications in the FedAppStore have gone through a certification process run by ServiceNow but are not in scope for the GCC FedRAMP authorization. It is the customer responsibility to determine if they are appropriate for use with their GCC instances.

Mobile apps

The mobile apps for iOS and Android (including push notifications) are available for use with GCC instances and use appropriate security controls including FIPS 140-2 validated encryption.

Find out more about how the ServiceNow mobile apps comply with security standards for the GCC cloud environment here.

Support in the GCC environment

Technical support for GCC customers

GCC technical support is managed on a 24/7/365 basis by a ServiceNow dedicated U.S. Government Support team. Customer requests are placed and managed through the dedicated GCC HiWave Support Portal.

All ServiceNow GCC support staff are required to undergo Fed Pass screening per the U.S. Federal Personnel Authorization Screening Standards SOP.

Documentation for the ServiceNow GCC environment

All ServiceNow FedRAMP-specific security documentation is available to GCC customers via the GCC HiWave Support Portal.
Conclusion

It is common for U.S. government agencies to use a cloud service for their data processing and storage needs. The information presented in this document outlines the security and privacy controls available in the Now Platform which customer admins can implement to help comply with FedRAMP’s requirements.

The ServiceNow Government Community Cloud (GCC) environment has been developed explicitly for the benefit of federal agencies and is authorized by FedRAMP and DoD.

The ServiceNow GCC allows government agencies to provide their users with the services they need along with the confidence that they are entrusting their data to a flexible and reliable system that has high levels of security and a proven track record.

Resources

- U.S. Government FedRAMP site
- FedRAMP Documents and Templates
- ServiceNow Product Documentation
- Cloud Security Trust and Compliance Center