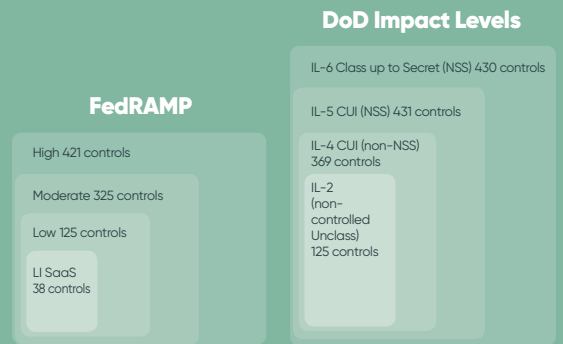


What are FedRAMP and DoD Impact Levels?

An assessment and authorization process which U.S. Federal agencies have been directed to employ to ensure security is in place when accessing cloud computing products and services.

2 separate but similar authorizations - 1 ServiceNow Gov environment



ServiceNow's FedRAMP High/DoD IL-4 Process

ServiceNow now listed as "In Process" on the FedRAMP's website for FedRAMP High.

Infrastructure Buildout	SysEng Svs/ App & DB Capacity Buildout	HI & Data Center Build In FedRAMP	End-to-End Validation/ 3PAO Readiness Assessment (RAR)	3PAO Testing + FedRAMP/ DISA (IL-4) Authorization	<ul style="list-style-type: none"> ✓ SaaS ✓ Moderate (High in Process) ✓ FedRAMP Authorized ✓ 34 Authorizations
-------------------------	---	--	---	--	---

↑ Where we are today

Q&A

1 What is the ServiceNow GovCommunityCloud (US) Migration Project?

Currently, all US Federal and some US State/Local and US government instances reside in ServiceNow's FedRAMP Moderate/DoD IL-2 data center environment. These existing datacenters possess a Joint Authorization Board (JAB) FedRAMP Moderate authorization, as well as a DoD Impact Level 2 authorization from DISA.

ServiceNow has begun its JAB FedRAMP High & DoD Impact Level 4 authorization review for its two new GovCommunityCloud (US) data centers. This migration project is focused on migrating all instances from the existing FedRAMP Moderate/DoD IL-2 data centers to the new ServiceNow GovCommunityCloud (US) data centers.

2 Is there a requirement to move to the ServiceNow GovCommunityCloud (US) data centers or is it possible to remain in the FedRAMP Moderate/DoD IL-2 data centers?

Service Now will not be maintaining the FedRAMP Moderate/DoD IL-2 data centers long term. The intent is to migrate all customers to the ServiceNow GovCommunityCloud (US) facility as soon as possible and decommission the FedRAMP Moderate/DoD IL-2 facilities. The ServiceNow GovCommunityCloud (US) environment has been built in adherence with all FedRAMP High & DoD IL4 compliance requirements. This includes controls to ensure your data is kept safe at a FedRAMP High and DoD Impact Level 4 impact level for ServiceNow's GovCommunityCloud (US) environment.

Please note: Because of the more stringent compliance requirements in this environment, certain systems/systems/plugins will no longer be accessible post migration to this environment. Please refer to KB0743854 for the list of services that will not be available in the ServiceNow GovCommunityCloud (US) environment (As ServiceNow is still in the process of achieving FedRAMP and DISA ATO approval, additional services might need to be limited. You will be updated of any changes to the KB)

3 What actions are required in preparation for the migration to the GovCommunityCloud (US) data centers?

Before the migration to the ServiceNow GovCommunityCloud (US) data center, all instances must satisfy the following ServiceNow GovCommunityCloud (US) migration pre-requisites. (More information about many of these requirements can be found within the answers in this article.)

4 Why do all instances need to be upgraded to London or later versions?

The P-ATO is not valid for any instances prior to the Kingston release. The only approved releases as of March 2019 are the Kingston, London or Madrid releases. Future releases will be added to this list as and when they are approved. Since the New York release will be available closer to the migration timeframe, it is recommended to upgrade to London or Madrid.

5 What is the Customer Responsibility Matrix (CRM) and where is it located?

The ServiceNow GovCommunityCloud (US) Customer Responsibility Matrix (CRM) includes a list of customer agency actions that should be part of an effective security program for a system based on a SaaS offering. As part of the pre-migration checklist, customers must confirm the completion of required actions as listed in the CRM before they can be migrated to the GovCommunityCloud (US) datacenters. Download this document for more information: KB0685212 (As ServiceNow is still in the process of achieving FedRAMP and DISA ATO approval, additional requirements might be added. You will be updated of any changes to the KB)

6 What is a NAT IP address and what is it used for?

Network Address Translation (NAT) is the public/Internet, ServiceNow source IP address seen by your network for traffic initiated from your ServiceNow instance towards your network. ServiceNow specifies a range of IP addresses from which any single one could be used for a connection. If the customer wishes to whitelist NAT IPs, it is mandatory the entire range is allowed.

7 What change will be made to the NAT IP address?

The NAT IP address will be changing from 14996.3.8/29 to 14996.192.8/29 in the HEF100 data center and from 14996.4.8/29 to 14996.193.8/29 in the MIA100 data center. It is the customer's responsibility to add the new NAT IP addresses ranges to their firewall in order to permit connections source from ServiceNow. Appropriate firewall configuration will prevent downtime post-migration.

8 Why does the NAT IP address need to be updated?

The ServiceNow GovCommunityCloud (US) environment is built on an entirely new network architecture and is separate from the old networks. This mandates the use of new IP address blocks for NAT.

Q&A *Continued*

9 What is the External Domain Name Space (DNS) address?

The External DNS address is the IP address that is used when accessing or initiating connections into a ServiceNow instance. It is the IP associated with an instance (<https://<customer>.servicenowservices.com>). The IP is unique for each of the two redundant data centers. In the new network, the IP address will change to a unique address per customer (for example, from 14996.3.100 to 14996.192.100 in the HEF100 data center and from 14996.4.100 to 14996.193.100 in the MIA100 data center). The details about your specific IP address change will be provided as part of migration communications.

10 Why does a new External DNS address need to be added?

The DNS for instances within the new ServiceNow GovCommunityCloud (US) requires a distinct name space from our existing cloud. The domain has changed from service-now.com to servicenowservices.com to meet this requirement. New external DNS address needs to be added to avoid downtime after the instance is moved to the ServiceNow GovCommunityCloud (US) environment.

11 What is the difference between a NAT IP address and an External DNS IP address?

The External DNS address is the IP address that is used when accessing or initiating connections into a ServiceNow instance. The NAT IP address is used when an instance is making an outbound connection from ServiceNow.

12 What is the impact to VPN customers?

ServiceNow recommends against the use of VPNs as there are options that are far better and easier to manage. Please refer to our community blog on alternatives to using a VPN.

13 Will the ServiceNow team be able to verify that the changes to the VPN have been made successfully?

ServiceNow will be able to test each tunnel from the ServiceNow GovCommunityCloud (US) environment to confirm that it has been configured correctly prior to signing off. This will be performed at the time of the scheduled change. You will be informed once all test passes have been completed successfully.

14 Are there alternatives to using a VPN?

ServiceNow strongly recommends against the use of VPNs. As an alternative, ServiceNow also enables the use of private connectivity via the Equinix Cloud Exchange (ECX) or via DirectConnect of circuits to the ServiceNow network edge. For DoD IL4 customers, requirements are still being finalized around DISA Cloud Access Point (CAP).

15 How will all of these required changes be coordinated?

Customer will receive a communication containing all of the pre-requisite requirements for ServiceNow GovCommunityCloud (US) compliance. Instance migration activities and associated change records (CHG#) will be visible on your service portal.

16 What if there are already existing plans for a London or Madrid upgrade?

You can follow the normal upgrade process as long as the upgrade is going to complete ahead of the migration date. The change records for the instance migration activities will provide the date for the planned migration. If the upgrade timeline you are planning to follow is not going to be completed ahead of the ServiceNow GovCommunityCloud (US) migration timeline, visit your portal page or contact the ServiceNow Global Technical Support team.

17 When can I expect my instance(s) to be migrated, and what happens if I am not ready by that date?

Your instance is eligible for a move after prerequisites have been met (please refer to Qs.3). At this time, ServiceNow is targeting the September 2019 timeframe pending ATO approval. If your instance is not ready by then, ServiceNow will engage with you to discuss options on a case-by-case basis.

18 How long will the move take, and will there be any down time during the move?

The migration is estimated to take anywhere from 6 to 96 hours. There is expected to be an outage during the cut-over window as the instance comes online in the new ServiceNow GovCommunityCloud (US) environment. This outage window will be communicated on a per-instance basis as part of the overall migration and will be performed within the scheduled maintenance window.

19 What happens if we have instances in the current FedRAMP Moderate/DoD IL-2 and ServiceNow GovCommunityCloud (US) environments concurrently? Will we be able to access instances in both environments concurrently?

Yes. As long as the new external DNS IP address has been added, the instance URL will resolve appropriately to FedRAMP Moderate/DoD IL-2 or ServiceNow GovCommunityCloud (US) depending on the location of the instance. A separate instance of HI will be available inside ServiceNow GovCommunityCloud (US) – this instance, named HiWave, will be available at <https://hiwave.servicenowservices.com>. You will have access to this instance of HI once the migration process for your instances begins. Information for instances migrated to ServiceNow GovCommunityCloud (US) can be accessed via HiWave. Once all of your instances have been migrated to ServiceNow GovCommunityCloud (US) you will no longer have access to HI and all access will be exclusively via HIWAVE inside ServiceNow GovCommunityCloud (US).

20 What happens if we are unable to access an instance after it has moved to ServiceNow GovCommunityCloud (US)?

After the move is completed, part of the final test and sign-off will be confirming that you can access the instances. If issues occur, please contact the ServiceNow Global Technical Support team at <http://www.servicenow.com/support/contact-support.html> and reference the migration ticket number; The normal escalation processes will be followed to remediate the problem.

21 What is Multi-Factor Authentication?

Multi-factor authentication (MFA), also known as two-step verification, is a security requirement that requires a user to enter more than one set of credentials in order to authenticate or log in to a system. The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Multi-factor authentication can be achieved through the use of a third-party SSO solution, such as SAML.

22 I still have questions not answered in this FAQ?

If you have additional questions, please contact ServiceNow Global Technical Support team at <http://www.servicenow.com/support/contact-support.html>

Resources

KB0747349 ServiceNow GovCommunityCloud (US)

KB07745039 FedRAMP High/IL-4 Migration FAQ

KB0743854 Products/services not available for FedRAMP Mod/High/Self-Hosted customers

KB0685212 Revised Customer Responsibility Matrix (CRM)

servicenow