Pega Cloud for Government

4 March 2024

CONTENTS

Pega Cloud for Government

Pega Cloud® for Government is a comprehensive cloud solution that provides the tools, environments and operational support built for the US Government clients.

> **Note:** This content applies only to Pega Cloud for Government environments.

Pega empowers agencies to achieve outcomes through superior operational efficiency and customer engagement. Our software, Pega Infinity™, is highly adaptable and ready to take on evolving government mandates at a moment's notice. Leading organizations meet their mission with Pega using the unified, adaptive, and cloud-based technology, which helps you start quickly and then scale without limits.

Who can use Pega Cloud for Government?

US Government agencies have a myriad of missions for which Pega Cloud is an excellent solution. Government agency missions can be best served using the Pega Cloud for Government (PCFG) in the following scenarios:

- The agency RFI/RFP requires FedRAMP Low or Moderate authorization of the cloud service provider.
- The Government applications and data ratings require Low or Moderate IT security functionality under FIPS-199.
- The DoD organization requires Impact Level 2 IT security for the application and data. Impact level 2 is appropriate only for public or non-critical mission information.

Because PCFG supplies the infrastructure, operational support, and life cycle management to support Pega applications as an AWS GovCloud-delivered solution, PCFG is the preferred solution for Federal Government clients or DoD organizations.

State, local and tribal government organizations are eligible and encouraged to use PCFG by the FedRAMP Program Management Office (PMO) to take advantage of the higher grade of IT security represented in PCFG compared to Pega Cloud services. However, since PCFG only provides limited public Internet access, Pega recommends that organizations that require public Internet access to Pega applications (to fill out forms, for example, or for some other need) use the commercial Pega Cloud services.

Outbound network traffic from any PCFG environment is restricted to only approved services, as part of FedRAMP compliance. Any request for sending outbound traffic to a new service must be approved by Pega CloudSecurity.

Only United States Federal, state, local or tribal government agencies may use PCFG; it is not available for use by commercial businesses or entities. The location of the government agency service must be in the continental United States (CONUS), US outlying areas, or DoD on-premise locations.

Data Security

Restrictions to access are not limited just to direct access to client data; client metadata is considered to be potentially as sensitive as the actual Government entity data.

This is particularly true of information found in service requests, which often contain system vulnerability discussions, or include issue description details that could lead to exploitation by unauthorized parties.

For more information on security, see Security standards for Pega Cloud for Government

Personnel Security

Pega personnel working on PCFG are required to complete a minimum of a National Agency Check and Inquiry (NACI) verification before they are allowed access to any PCFG environment. While FedRAMP does not dictate the nationality of support staff, Pega ensures that its staff adheres to the policies of each supported Government agency, which usually has established specific rules regarding US citizenship access.

The Pega authorizing authority requires US-based – US-citizen-only support personnel, so Pega adheres to this US-citizen standard for its PCFG environments. strictly limits access to PCFG environments, and ensures that foreign nationals cannot access any PCFG environment.

Pega Cloud for Government Subscription Documentation

The Pega Cloud Subscription Documentation provides details about what is included in the Pega Cloud for Government subscription offering, with the following articles:

- The Service Level Agreement for Pega Cloud for Government
- Incident response and management for Pega Cloud for Government
- Change management for Pega Cloud for Government
- Disaster Recovery for Pega Cloud for Government
- Data backup, data restoration, and data recovery for Pega Cloud for Government
- Security standards for Pega Cloud for Government outlines the various security controls (technical and organizational, physical and environmental, network and infrastructure, and others) which are provided by Pega for clients Pega Cloud for Government deployments.
- Client responsibilities for Pega Cloud for Government describes what security responsibilities are assumed by the client for aPega Cloud for Government environment. This document includes both privacy and security controls, and data rights and responsibilities and requires clients to comply with the Pega Products and Services Acceptable Use Policy.
- Layered Distributed Denial of Service protection in Pega Cloud for Government
- Vulnerability testing policy for applications on Pega Cloud

Pega Application Support in Pega Cloud for Government

Pega Cloud® for Government provides secure Business Process Management solutions for US federal and regional government organizations.

> **Note:** This content applies only to Pega Cloud for Government environments.

Pega Cloud® for Government (PCFG) client environments are deployed on the Pega Cloud 2. A number of Pega applications and related services are approved for deployment in PCFG.

The approved Pega applications include:

- Pega Platform
- Pega Government Platform
- Pega Customer Service (the Interaction Portal – does not include Pega Customer Decision Hub™)
- Pega Call
- Pega Knowledge Management
- Pega Sales Automation (Standard Edition only)

The supporting services approved for deployment include:

- Agile Studio
- Pega Diagnostic Center™(PDC)
- Pega Robot Manager
- Deployment Manager

Connectivity features includes:

- Direct Connect
- VPN
- AWS Direct Connect
- Public VIF and Private VIF
- Internet AWS Transit Gateway
- Client-defined inbound IP address allow-list
- Pega Cloud File storage
- Near real-time log streaming to Splunk

Network services and connections

Information security is a top requirement for government services. Pega Cloud® for Government uses a range of solutions to protect client information and ensure full compliance with federal requirements.

> **Note:** This content applies only to Pega Cloud for Government environments.

Most Federal Government agencies' web services primarily focus on communication to and from citizens and others who require their services or need to provide them with information. This communication requires connectivity to the Internet.

Pega Cloud for Government supports Federal agencies that are required to use a designated Trusted Internet Connection (TIC). The TIC initiative optimizes and standardizes the security of individual external network connections to include connections to the Internet, which are currently in use by the Federal government. A TIC performs a myriad of IT security functions and is similar to a cloud access security broker (CASB).

CASBs deliver differentiated, cloud-specific capabilities that are generally not available as features in other security controls, such as web application firewalls (WAFs), secure web gateways (SWGs) and enterprise firewalls. Unlike those security products, which are premises-focused, CASBs are designed to identify and protect data that is stored in someone else's systems. CASBs provide a central location for policy and governance concurrently across multiple cloud services, for users and devices, and granular visibility into and control over user activities and sensitive data.

DoD clients require their cloud environments to have external network traffic pass through a NIPRnet Internet Access Point (IAP). An IAP performs similar functions to a TIC but it is provided by the DoD. The NIPRnet IAP is a DoD system of network boundary protections and monitoring devices through which cloud services outside the

DoD network security boundary must traverse to connect to resources inside the DoD network security boundary.

FedRAMP requires that the Cloud Service providers (CSP) like Pega connect to its networks via a FIPS 140-2 encrypted Virtual Private Network (VPN) connection; alternately, a VPN using AWS Direct Connect or Transit Gateway is also permissible. Pega is currently investigating the use of VPN technologies like PrivateLink as an additional network connectivity option.

Government and DoD Clients own the network connectivity from their Pega-provided Virtual Private Clouds (VPC) to their constituents. These clients determine what is acceptable as secure network connections. For example, Quad zero (0.0.0.0) is a perfectly acceptable short-term solution to provide the client with rapid access from Internet users to their Pega-provided VPC, particularly if it is only to the Dev/test environment.

Clients who use PCFG are encouraged to use more secure methodologies, such as encrypted VPNs, for their connections from or through the Internet. By request, Pega provides services for these clients that need more open Internet interfaces like CASB or geography IP restriction services.

Network CIDR allocations

To enforce network routing restrictions, Pega does not allow Virtual Private Cloud (VPC) networks' IP addresses to overlap, and requires that each clients' range be selected from an approved pool of dedicated PCFG CIDR ranges. Pega provisions each PCFG VPC with a network topology customized to meet and maintain a PCFG Client's environmental requirements. PCFG engages with the Client during the onboarding process to scope the appropriate CIDR range for each client's specific requirements.

Integration with AWS Transit Gateway

Pega Cloud® for Government can be seamlessly integrated into the AWS Transit Gateway, which simplifies your network setup and improves connectivity by providing a secure central hub for your VPCs and on-premises networks.

> **Note:** This content applies only to Pega Cloud for Government environments.

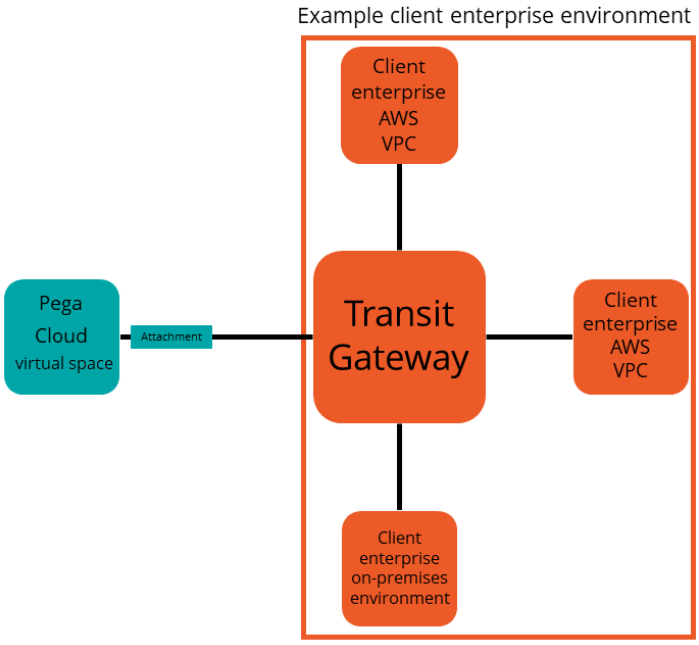
Pega Cloud for Government (PCFG) supports the integration of a client AWS Transit Gateway with your FedRAMP-compliant environments.

If your enterprise uses the Transit Gateway as a secure, centralized hub to route, provision, and monitor your enterprise network topology, it can now include all of your networking connections with your Pega Cloud environments. The Transit Gateway centralizes your external connections to your Pega Cloud for Governmentenvironments in a monitored and secure private network.

Although Pega Cloud for Government does not provide the Transit Gateway as a service, PCFG can integrate a client who subscribes to the AWS Transit Gateway. You can integrate your Pega Cloud for Government VPCs, and any PCFG VPN service, with your Transit Gateway, as you would with any other AWS for Government VPC or VPN.

After you subscribe to the AWS Transit Gateway service through your AWS for Government account, you can request that Pega Cloud for Government provide the information you need to integrate your service with your Pega Cloud® environments.

The following illustration provides a model of how your Pega Cloud for Government VPC integrates with your AWS Transit Gateway Service.



Integration with Transit Gateway

Integrating your FedRAMP-compliant Pega Cloud environments with your Transit Gateway can simplify your enterprise network topology by providing the following benefits:

- Eliminating the need for complicated peering connections, especially in larger topologies, to let multiple environments communicate with one another.
- Removing the requirement for multiple VPN connections between each of your AWS VPCs, including your Pega VPC, and on-premises environments.
- Limiting traffic between your Pega Cloud environment and other VPCs.
- Scaling your enterprise network topology to your Pega Cloud networking demands.
- Responding to spikes in network traffic more resiliently through multiple interoperable VPCs.

Integrating Pega Cloud for Government with AWS Transit Gateway

Before you begin:

- Ensure that you can access your AWS Resource Access Manager (RAM) to create a resource share for Pega Cloud® for Government.
- Set up a management account with sharing enabled for AWS organizations in order to create the Transit Gateway resource share. For more information about subscribing to AWS Transit Gateway, see the AWS Transit Gateway landing page.

1. Request a new service by selecting **New request** in My Support Portal, or by contacting Pega Support with a request to integrate your Transit Gateway with your Pega Cloud environments. For more information, see My Support Portal Frequently Asked Questions.
2. Update your Transit Gateway service by allowing Pega Cloud for Government to access your Transit Gateway:
   a. In the AWS RAM console, create a resource share.
   b. From the response to the request, or the information from the call with your Pega representative, note the AWS account number Pega Cloud for Government shares with you.
   c. In your RAM console, in the **Principals** section, enter the AWS account number that you receive from Pega Cloud for Government in response to your service request.
   d. Select **Create resource share**.

Note: You can use the *create-resource-share* AWS API to enter the account number. For additional information on how to create a resource share through the RAM console or by using the API, see the AWS Resource Management Documentation.

3. After you create a resource share of your Transit Gateway, Pega Cloud for Government creates a Transit Gateway VPC attachment to your Pega Cloud VPC.
4. If you do not select auto-accept shares, accept the share by performing the following steps:
    a. In your RAM console, select the **Shared with me: Resource shares**.
    b. On the **Pending** resource share page, add your Pega Cloud environment by selecting **Accept Resource Share**.

    For additional information on receiving a resource share, see the AWS Resource Access Manager documentation.

Result:

You integrated the Pega Cloud for Government VPC and VPN service into your Transit Gateway, and can now utilize the Transit Gateway to connect your FedRAMP-compliant Pega Cloud VPC to the rest of your enterprise network topology.