

Microsoft Azure for US Government Integration

Table 1: Feature History

Feature Name	Release Information	Description
Support for the Azure for US Government Cloud with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With the integration of the Azure for US Government cloud with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, you can move and store your highly sensitive workloads in an isolated cloud that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements of the U.S. government and its customers. All of the same features that are available for the Azure integration with Virtual WAN are also available with the Azure for US Government cloud.
Configure Devices for Azure for US Government Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for Azure for US Government.

- Information About Azure for US Government Integration, on page 2
- Supported Devices for Azure for US Government, on page 2
- Prerequisites for Azure for US Government Integration, on page 3
- Restrictions for Azure for US Government Integration, on page 3
- Use Case for Azure for US Government Integration, on page 3
- Configure Azure for US Government, on page 3
- Monitor Azure for US Government Integration, on page 4

Information About Azure for US Government Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

This feature adds the Azure for US Government cloud to Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, allowing you to move and store your highly sensitive workloads in the Azure for US Government cloud.

The following are examples of highly sensitive workloads that you can store in the Azure for US Government cloud:

- Controller Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Sensitive patient medical records
- Financial data
- Law enforcement data
- Export data

The same features that are available for the Azure Virtual WAN integration are also available with the Azure for US Government integration. Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch connectivity through Azure.

For more information on the Azure for US Government cloud, see the Azure for US Government documentation.

Configure Azure for US Government as part of Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud in Cisco SD-WAN Manager.

Benefits of Azure for US Government Integration

- Allows you to store your highly sensitive workloads in the Azure for US Government cloud as part of Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud in Cisco SD-WAN Manager
- Supports the same features and workflow as for the Azure Virtual WAN integration in Cisco SD-WAN Manager
- Provides an isolated instance of Azure for storing data exclusively for U.S. government workloads
- Provides increased security with data centers and networks located in the U.S
- Limits potential access to sensitive data to only screened U.S. personnel
- Includes support for region pairing for providing geo-redundant storage

  For more information on region pairing, see the Microsoft Azure documentation.

Supported Devices for Azure for US Government

For more information on the supported devices for Azure for US Government, see Supported Azure Instances.

Prerequisites for Azure for US Government Integration

For more information on the prerequisites for Azure for US Government integration, see Prerequisites for Azure Virtual WAN Integration.

Restrictions for Azure for US Government Integration

- No support for creating a Network Virtual Appliance (NVA) from the Azure portal.
- No telemetry support for Azure for US Government.

Use Case for Azure for US Government Integration

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud with Azure for US Government cloud allows you to safely move and store your highly sensitive data in the Azure for US Government cloud. The Azure for US Government cloud is an isolated cloud dedicated to the workloads of the U.S. government and its customers.

The following are examples of sensitive data that you can store in the Azure for US Government cloud:

- Controller Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Sensitive patient medical records
- Financial data
- Law enforcement data
- Export data

Configure Azure for US Government

The workflow for configuring Azure for US Government integration is the same as the workflow as for the Azure Virtual WAN integration.

1. Associate your Azure for US Government account with Cisco SD-WAN Manager.

   For more information on associating your Azure for US Government account, see Integrate Your Azure Cloud Account.

2. Add and manage your cloud global settings.

   For more information on configuring cloud global settings for Azure for US Government, see Integrate Your Azure Cloud Account.

3. Create and manage your cloud gateways.

   For more information on creating and managing your cloud gateways, see Create and Manage Cloud Gateways.

4. Discover your host virtual network (VNets) and create tags.

   For more information on discovering host VNets and creating tags, see Discover Host VNets and Create Tags.

5. Map your VNet tags and branch network VPNs.

   For more information on mapping your VNets and branch network VPNs, see Map VNet Tags and Branch Network VPNs.

Monitor Azure for US Government Integration

For more information on monitoring the Azure for US Government integration, see Monitor Azure Virtual WAN Integration.