

Microsoft Azure Virtual WAN Integration

Table 1: Feature History

Feature Name	Release Information	Description
Automated Integration of Azure Virtual WAN and Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature enhances Cloud OnRamp integration with Microsoft Azure by allowing Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) to be deployed inside the Azure Virtual WAN Hub instead of deploying it in transit VNets. It also automates the Cisco Catalyst SD-WAN fabric connection to Azure Virtual WAN Hub through Cisco Catalyst 8000V. The connectivity between inter-region Azure Virtual WAN Hubs is also supported. In addition, you can convert the Azure virtual WAN hubs created using Cisco SD-WAN Manager into secured hubs by deploying Azure firewall inside them. However, secured virtual hubs can only be configured using the Microsoft Azure portal.
Integration of Cisco Catalyst SD-WAN and Azure Virtual WAN Hub Using Azure Portal	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	As part of the integration of Cisco Catalyst SD-WAN with Azure Virtual WAN, you can also use the Azure portal to upload bootstrap configuration files for Cisco Catalyst 8000V instances. These instances can then be used to create a virtual WAN hub using the Azure portal.
Routing Traffic Flow to a Virtual Hub Firewall or a Local Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to route Microsoft Azure Virtual WAN hub traffic to a firewall on a local branch router, or direct local branch traffic to an Azure secured virtual hub, to be subject to the security policies of the Azure Firewall Manager.
Azure Scaling, Audit, and Security of Network Virtual Appliances	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to edit the SKU scale value, and have better security for your Network Virtual Appliances (NVAs). The audit service compares the information from the Cisco SD-WAN Manager and Azure cloud databases and identifies the discrepancies.

Feature Name	Release Information	Description
Periodic Audit, Enhancement to Azure Scaling and Audit, and ExpressRoute Connection.	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	Cisco SD-WAN Manager provides an optional periodic audit every two hours. This automatic audit takes place in the background and generates a report of the discrepancies. If you enable the auto correct option, Cisco SD-WAN Manager automatically resolves any recoverable issues found during the periodic audit. You can fix the individual discrepancies generated after initiating an on-demand audit. Cisco SD-WAN Manager supports ExpressRoute connections from branch offices to NVAs through Cisco Catalyst SD-WAN tunnels. ExpressRoute connections are the private networks that offer higher reliability, fewer latencies, and faster connections for data transfer.
Support for Multiple Virtual Hubs in Each Region	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	You can create multiple virtual hubs in a single Azure region.
Added an Azure Instance Type	Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	With this feature, new instance types are added which includes 16 CPU cores and 64 GB of memory. You can deploy this type of instance for SKU scale values of 20, 40, 60, and 80.
Configure Device for Azure Integration Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for Azure integration.

- Information About Azure Virtual WAN Integration, on page 3
- Supported Devices for Azure Virtual WAN Integration, on page 11
- Prerequisites for Azure Virtual WAN Integration, on page 12
- Restrictions for Azure Virtual WAN Integration, on page 13
- Use Cases for Azure Virtual WAN Integration, on page 14
- Configure Azure Virtual WAN Integration, on page 15
- Verify Azure Virtual WAN Integration, on page 30
- Monitor Azure Virtual WAN Integration Using Cisco SD-WAN Manager, on page 31

Information About Azure Virtual WAN Integration

Azure Virtual WAN Hub Integration with Cisco Catalyst SD-WAN

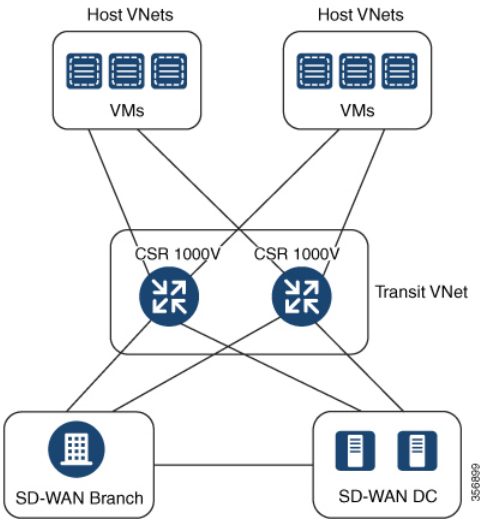
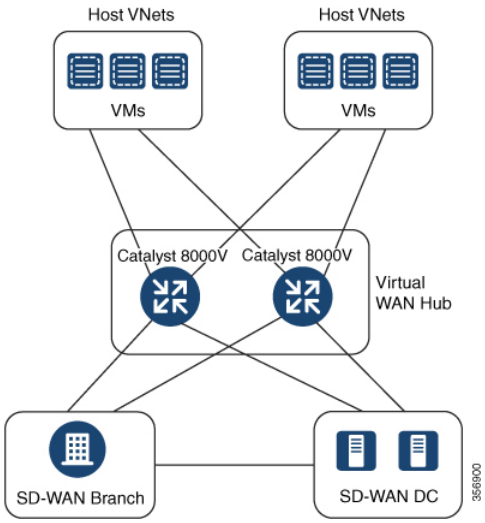
Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

The integration of the Cisco Catalyst SD-WAN solution with Azure virtual WAN enhances Cloud OnRamp for Multicloud deployments and enables configuring Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) as a network virtual appliance (NVA) in Azure Virtual WAN Hubs.

This integration simplifies the consumption model for cloud services because it eliminates the need to create a transit virtual network (VNet) and you can control your host VNet connectivity directly through the Azure Virtual WAN Hub. Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch connectivity through Microsoft Azure. It enables you to connect and configure branch devices that can communicate with Azure. Configuring Cisco Catalyst 8000V instances inside Azure virtual hubs provides higher speeds and bandwidth and overcomes the speed and bandwidth limitation of using transit VNets.

Cloud OnRamp for IaaS Versus Cloud OnRamp for Multicloud

This table lists the differences between Cloud OnRamp for IaaS and Cloud OnRamp for Multicloud in the context of Microsoft Azure Integration.

Cloud OnRamp for IaaS for Azure	Cloud OnRamp for Multicloud for Azure
	
Enables automated provisioning of transit VNets through the Cloud OnRamp for IaaS workflow in Cisco SD-WAN Manager	Enables automated provisioning of Azure virtual hubs through the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager
Cisco SD-WAN Manager automatically provisions two Cisco Cloud Services Router 1000V Series (Cisco CSR1000V) devices inside the transit VNet	Cisco SD-WAN Manager automatically provisions two Cisco Catalyst 8000V instances inside the Azure virtual hub

For information on Cloud OnRamp for IaaS with Azure and how to configure transit VNets, see Configure Cloud OnRamp for IaaS for Azure.

How Virtual WAN Hub Integration Works

The connection between the overlay network and a public-cloud application is provided by a pair of redundant Cisco Catalyst 8000V instances that are configured inside the Azure virtual WAN hub as part of the Cloud OnRamp for Multicloud workflow for Azure. Using redundant routers to form the transit offers path resiliency to the public cloud.

The Cloud OnRamp for Multicloud flow in Cisco SD-WAN Manager discovers your existing VNets in geographical cloud regions and allows you to connect select VNets to the overlay network. In such a scenario, Cloud OnRamp for Multicloud allows simple integration between legacy public-cloud connections and the Cisco Catalyst SD-WAN overlay network.

A configuration wizard in Cisco SD-WAN Manager automates the bring-up of the Azure Virtual WAN Hub to connect with your public cloud account. The wizard also automates the connections between public-cloud applications and the users of those applications at branches in the overlay network. Using tags, Cisco SD-WAN Manager enables you to map the service VPNs in your branches with specific VNets in your public cloud infrastructure.

VNet to VPN Mapping

The Intent Management workflow in Cisco SD-WAN Manager enables connectivity between Cisco SD-WAN VPNs (branch networks) and VNets, and VNets to VNets. VNets are represented by tags created under the Discover workflow for Cloud OnRamp for Multicloud. When VNets are mapped to connect them to the virtual WAN hubs, they are assigned a default route and propagate to the default label. When you create VNet tags within an Azure region, mapping is automatically created based on the other VNets and VPNs that share the same tag.

When Cisco SD-WAN Manager records the intent for connectivity, mapping is realized in cloud in regions where the cloud gateway is present. Mapping intents can be entered without cloud gateways being present in different regions. Your mapping intent is preserved and realized when a new cloud gateway or mapping change is discovered. As and when cloud gateways get instantiated or discovered in different regions, the mapping intents are realized in those regions. Similarly, tagging operations can influence the mapping in different regions as well and mappings as per the tags are realized in the cloud.

Note The VPNs selected to be mapped to VNet tags must not have overlapping IP addresses. This is because segmentation is not supported in Microsoft Azure Virtual WAN.

Inter-region Azure Hub-to-Hub connectivity is enabled by creating VNet tags and mapping them to your VPN sites. No additional configuration is required to enable inter-region hub-to-hub connectivity. VNets are associated with the Virtual WAN Hub for their respective regions. If VNets in different Azure regions share the same VNet tag, the connectivity between such VNets is automatically established and is carried out through the respective Virtual WAN Hubs that the VNets are connected to.

Components of Azure Virtual WAN Integration Workflow

A cloud gateway to connect your branches and data centers to the public cloud infrastructure is a logical object that hosts Cisco Catalyst 8000V instances. It comprises Azure Resource Groups, Azure Virtual WAN, and Azure Virtual WAN Hub.

Resource Groups

All Azure networking resources belong to a resource group and resource groups are created under Azure subscriptions. For Azure cloud gateways, Azure virtual WAN, and Azure Virtual WAN Hub are created under a resource group.

The first step to create an Azure cloud gateways is therefore to create a resource group.

After a resource group is created, you can configure Azure Virtual WAN.

Azure Virtual WAN

Azure Virtual WAN is the backbone of the Azure networking service. It's created under an existing Azure resource group. An Azure Virtual WAN can contain multiple Azure virtual hubs within it, as long as each virtual hub belongs to a different Azure region. Only one virtual hub per Azure region is supported.

After a virtual WAN has been defined under a resource group in a region, the next step is to create an Azure Virtual WAN Hub.

Azure Virtual WAN Hubs

The Azure virtual WAN Hub manages the core connectivity between your VPN sites and NVAs, and VNets. Once a virtual hub is created, the Cisco Catalyst 8000V instances can be integrated into the Azure networking service.

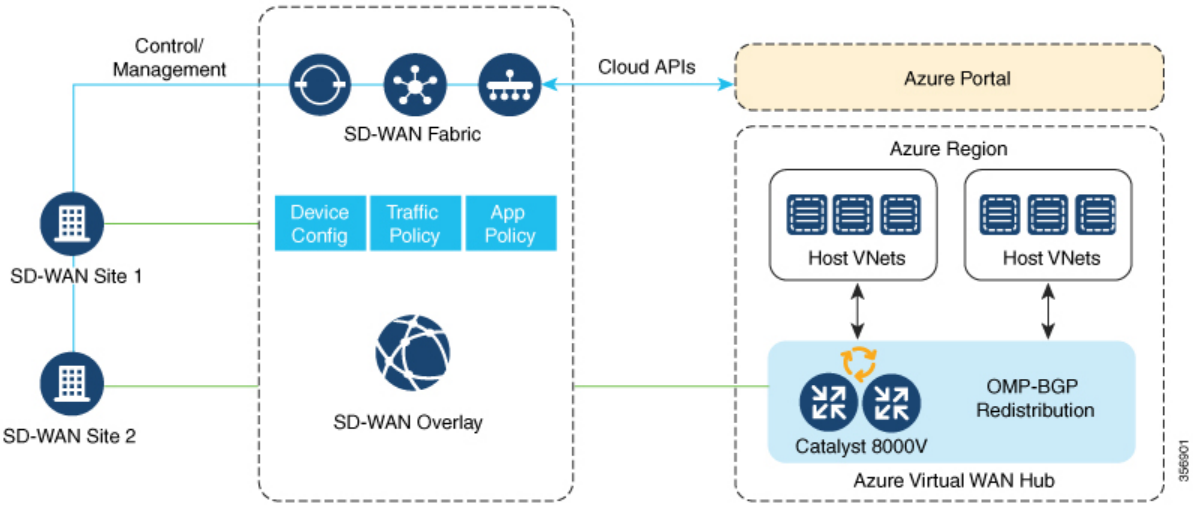
Connectivity Models

With the Integration of Azure Virtual WAN with the Cisco Catalyst SD-WAN solution, the following connectivity models are supported:

- Cisco Catalyst SD-WAN branch to Azure Host VNets within the same Azure region
- Inter-region Azure virtual hub-to-virtual hub connectivity

Cisco Catalyst SD-WAN Branch to Azure Host VNets (Single-region)

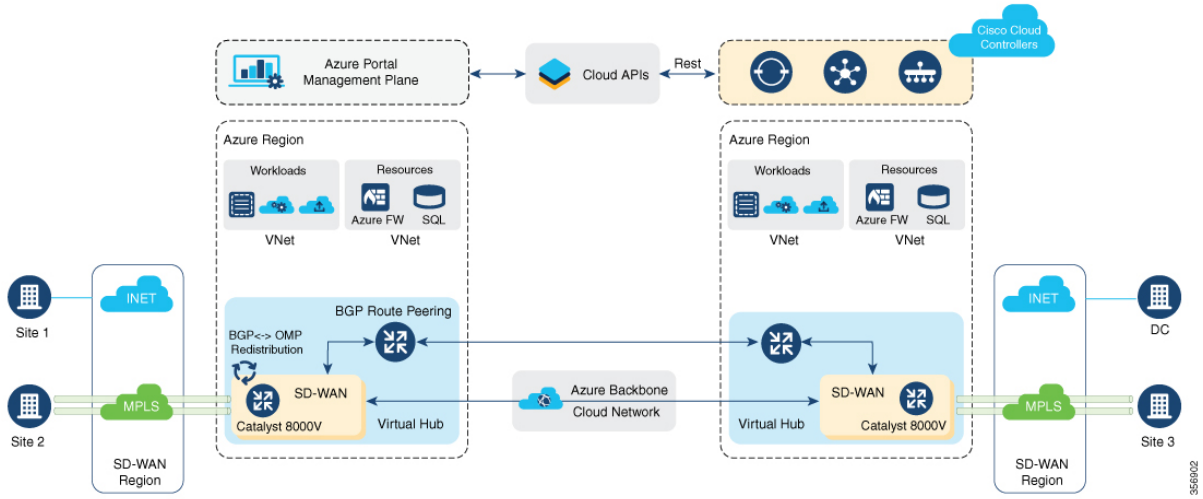
Figure 1: VNet to VNet Mapping within the Same Azure Region



In this scenario, the virtual hub is standalone and isn't connected to the virtual hubs in other Azure regions. In such cases, the VNets belong to the same region as the virtual hub, and are connected to your branch VPNs using VNet tags that are defined in Cisco SD-WAN Manager.

Virtual WAN Hub to Virtual WAN Hub (Inter-region)

Figure 2: Inter-region VNet-VNet Mapping Through Virtual Hubs



This image represents hub-to-hub connectivity with Azure backbone. This connectivity need not be configured separately. It's automatically achieved if VNets in different Azure regions share the same VNet tag.

Routing Traffic Flow to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

The Microsoft Azure environment includes a virtual hub that enables connectivity between Azure Virtual Network (VNet) workloads and local branch devices. The integration of Cisco Catalyst SD-WAN and the Azure environment enables the following firewall options:

- Routing outgoing internet traffic in the Azure Virtual WAN hub to a firewall on a local branch router
- Routing outgoing internet traffic from a local branch router to an Azure secured virtual hub, to be subject to the security policies of the Azure Firewall Manager.

Note An Azure secured virtual hub is an Azure Virtual WAN hub that has security and routing policy managed by the Azure Firewall Manager.

In both cases, return traffic follows the same path as outgoing internet traffic, so the same firewall policy applies to traffic in both directions.

Azure Virtual WAN Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

The multicloud audit service compares the information from the Cisco SD-WAN Manager database with the information in the Azure cloud database. This information includes Azure virtual WAN, virtual hubs, network virtual appliances, virtual networks, and VPN-to-virtual network mapping. Later, Cloud OnRamp for Multicloud compares the results, identifies the discrepancies, and displays a list of Microsoft Azure objects with and without errors.

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, the audit function incorporates the following enhancements:

- After you initiate an on-demand audit, the Cloud OnRamp for Multicloud audit service identifies and lists discrepancies between the information in the Cisco SD-WAN Manager database and the information in the Azure cloud. You can choose to fix all the discrepancies together or select a discrepancy and fix it individually. When you check a check box adjacent to an individual discrepancy, a brief explanation of the issue appears below the discrepancy.

  For more details about the audit discrepancies and resolutions, see Audit Discrepancies and Resolutions.

- You can now enable or disable periodic audits. For details, see Enable Periodic Audit.

Information About Periodic Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, Cisco SD-WAN Manager provides an optional periodic audit with an interval of two hours. This automatic audit takes place in the background and generates a report of the discrepancies. If you enable the auto correct option, Cisco SD-WAN Manager automatically resolves recoverable issues, if any, that are found during the periodic audit. For more details about the periodic audit and its resolutions, see Audit Discrepancies and Resolutions.



Note If you are upgrading the Cisco SD-WAN Manager version, the periodic audit and auto correct options are disabled by default. You can enable them from the **Cloud Global Settings** window. For details, see Add and Manage Global Cloud Settings.

Audit Discrepancies and Resolutions

The following table provides details about the audit discrepancies and resolutions for Azure.

Table 2: Examples of Azure audit discrepancies

Anomaly / Trigger	Audit Findings / Error Message	Resolution	
		On-Demand Audit Fix	Periodic Audit and Auto Correct
If the VNet is tagged in the Cisco SD-WAN Manager database, but it is not available in the Azure portal.	**Report Type**: VNet and Mapping **Details**: **VNet issue**: Cloud Virtual Network Issue: Not Found on Azure portal Name: <vnet-name>. Error received from Azure: Azure Error: ResourceNotFound Message: The resource '<vnet-name>' under resource group '<rg-name>' was not found. For more details, see https://aka.ms/ARMResourceNotFoundFix **Mapping issue**: Virtual Hub is mapped with virtual network <vnet-name> that does not exist.	The audit will remove the mapping from Cisco SD-WAN Manager. The audit will remove VNet from Cisco SD-WAN Manager.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.
If the VNet tag is removed from the Azure portal, or if a VNet tag mismatch exists between Cisco SD-WAN Manager and Azure portal.	**Report Type**: VNet **Details**: Cloud Virtual Network Issue: Tag On Cisco SD-WAN Manager is not the same as Azure portal Name: <vnet-name>.	Virtual network <vnet-name> will be tagged with <tag-name>.	Virtual network <vnet-name> will be tagged with <tag-name>.
If the storage account is not available in the Azure portal but it is available in the Cisco SD-WAN Manager database.	**Report Type**: Storage **Details**: Cloud Gateway (Storage) issue: Not Found on Azure Portal.Name: <name>, Id: <id>. A storage account is required to configure bootstrap for NVA create or edit operations. Error received from Azure: Azure Error: ResourceNotFound Message: The resource '<storage-account-name>' under resource group '<rg-name>' was not found. For more details please go to https://aka.ms/ARMResourceNotFoundFix	Storage account <storage-account-name> will be removed from Cisco SD-WAN Manager.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.

Anomaly / Trigger	Audit Findings / Error Message	Resolution	
		On-Demand Audit Fix	Periodic Audit and Auto Correct
If virtual WAN, vHub, or NVA is not available in the Azure portal.	**Report Type**: VWAN, vHub, NVA, Mapping	Audit removes virtual WAN, vHub, NVA, mapping from the Cisco SD-WAN Manager database. **Note**: Do not delete the cloud gateway manually. Deleting the cloud gateway results in a discrepancy between the cloud providers and can impact the ability to provision anything further or impact other CoR operations.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.
Mapping is found in the Cisco SD-WAN Manager database but it is not found in the Azure portal.	**Report Type**: Mapping **Details**: Mapping issue: Cloud Virtual Networks to Virtual Hub mapping issue. Mapping not found on Azure Portal with vNet <vnet-name>	Run audit-fix-sync issues to add virtual hub mapping to the Azure portal.	Audit adds virtual hub mapping to the Azure portal.
Mapping is found in the Azure portal, but it is not found in theCisco SD-WAN Manager database.	Audit shows in sync	Audit reports are in sync. To add the mapping back to the Cisco SD-WAN Manager database, add tag manually and map VNet using the Cisco SD-WAN Manager workflow.	Periodic audit reports are in sync. To add the mapping back to the Cisco SD-WAN Manager database, add tag manually and map VNet using the Cisco SD-WAN Manager workflow.
Account credentials expired	**Report Type**: VWAN, vHub, NVA, Mapping	You are required to manually update the account credentials.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You are required to manually update the account credentials.

Note Audit support for Azure was introduced in Cisco vManage Release 20.7.1.

Note Audit is not applicable for SD-Routing CoR (vHub with VPN) only deployment.

SKU Scale Value of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

You can edit the SKU scale value of a Cisco Catalyst 8000V Edge instance in Azure. In releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1, the SKU scale value is not editable. If you want to change the SKU scale value, you must delete and re-create the cloud gateway with a new SKU scale value.

You can opt for higher SKU scale values for better performance and lower values for cost-effectiveness.

For more information on how to update SKU scale values, see Configure SKU Scale Value.

Note After editing the SKU scale value, expect a network downtime of 3 to 4 minutes.

For details about the supported SKU scales, see Supported Azure Instances for Azure Virtual WAN Integration.

Security Rules Configuration of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Microsoft Azure has an option to edit the security rules of Network Virtual Appliances (NVAs). Cisco SD-WAN Manager supports the configuration of these security rules for NVAs.

Cisco Catalyst 8000V NVAs that are launched during cloud gateway creation prohibit the use of all the inbound ports, except Cisco Catalyst SD-WAN-related ports. The Security Rules Configuration of NVA feature allows you to enable a particular port as required, for example, for debugging purposes. After you add a new NVA rule to enable a port, it remains active only for two hours. Simultaneously, adding another NVA rule restarts the timer, and now all the enabled ports remain active for two hours.

Note

- Security rules of NVAs are not configurable when the cloud gateway operations are in progress.
- The source IP address for Azure can only have /30, /31, or /32 as suffixes. Examples of the source IP address for Azure are 192.0.2.0/30, 192.0.2.0/31, 192.0.2.0/32.

Information About Azure ExpressRoute Connection to NVA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, Cisco SD-WAN Manager supports ExpressRoute connections from branch offices to NVAs through SD-WAN tunnels. Express route connections are private networks that offer high reliability, few latencies, and fast connections for data transfer.

For further details about Azure ExpressRoute Connection to NVA, see Alternative Azure Designs.

Information about Multiple Virtual Hubs in Each Region

Minimum supported release: Cisco vManage Release 20.11.1

Note This feature is supported on both Azure Cloud and Azure Government Cloud.

For organizations with thousands of sites connected to Azure in a single region, Microsoft supports creation of multiple cloud gateways, and up to eight virtual hubs for a single region.

For Cisco vManage Release 20.10.1 and earlier releases, the Azure Virtual WAN solution supports only a single virtual hub in a single region. From Cisco vManage Release 20.11.1, the solution supports multiple virtual hubs in each region.

The cloud gateway attachment to a virtual network is based on a load balancing algorithm. When you add a tag to the cloud gateway attachment, you can choose **Auto** which distributes the VNets based on the load balancing algorithm. When you create a new cloud gateway, you can choose to redistribute VNets to load balance the existing VNets among all the cloud gateways. You can only reassign VNets across cloud gateways when you choose the **Auto** VNet tag. You cannot reassign the dedicated VNet tags that are attached to cloud gateways.

Supported Devices for Azure Virtual WAN Integration

Supported Azure Instances

Azure virtual WAN integration supports the following Cisco Catalyst 8000V instances.

Table 3: SKU Scale Value and Azure Instance Types

SKU Scale Value	Instance Resources	Number of Instances	Supported From
2	2 CPU cores and 7 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a
4	4 CPU cores and 14 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

SKU Scale Value	Instance Resources	Number of Instances	Supported From
10	8 CPU cores and 32 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a
20	16 CPU cores and 64 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a
40	16 CPU cores and 64 GB memory	3	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a
60	16 CPU cores and 64 GB memory	4	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a
80	16 CPU cores and 64 GB memory	5	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

Note The Azure instance type for a specific SKU Scale is determined by Azure when you create the cloud gateway. To find out which instance type has been allocated, use the **show platform software system all** command in the CLI session of the Cisco Catalyst 8000V cloud gateway and look for the Instance Type field under Cloud Metadata.

Prerequisites for Azure Virtual WAN Integration

Prerequisites for Routing Traffic to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

Cisco Cloud OnRamp for Multicloud has been configured to operate together with a Microsoft Azure environment. See Microsoft Azure Virtual WAN Integration.

Prerequisites for Azure SKU Scaling, Audit, and Security Rules of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

- Cisco Cloud OnRamp for Multicloud must be configured to operate together with a Microsoft Azure environment. See Microsoft Azure Virtual WAN Integration.
- Azure cloud account details.
- Subscription to Azure Marketplace.

- Cisco SD-WAN Manager must be connected to the internet and must be able to communicate with Microsoft Azure to authenticate your Azure account.
- Cloud gateway must be operational.

Restrictions for Azure Virtual WAN Integration

Restrictions for Azure Virtual WAN Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

- Azure Virtual WAN hub architecture doesn't support segmentation.
- The VPNs you select for mapping to the VNets should not have overlapping IP address spaces.
- Because of VNet tagging, all the VPNs and VNets are visible to all the other VPNs and VNets.
- Only one virtual hub can be configured for each Azure region and for each resource group.
- Only one resource group is permitted on Cisco SD-WAN Manager.
- For inter-region hub-to-hub connectivity, all the virtual hubs must be part of the same Azure Virtual WAN.
- IPv6 is not supported.
- Azure virtual WAN hubs don't support trace route.
- Branches connected to the virtual WAN hub can only be assigned to the default route table of the virtual WAN hub.
- If no virtual WAN hub is created or discovered in an Azure region through Cisco SD-WAN Manager, the VNets in that region don't get mapped using VNet tags.
- For deploying the Cisco Catalyst 8000V Network Virtual Appliances (NVAs) in the Azure WAN hub, it is supported under one resource group and virtual WAN. You can not deploy Cisco Catalyst 8000V in different resource groups. After the Cisco Catalyst 8000V NVA deployment, by default is associated to that resource group and virtual WAN for subsequent deployments.

Restrictions for Routing Traffic to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

Routing local traffic to an Azure secure virtual hub operating with the Azure Firewall Manager may involve additional operating charges for your Azure environment. Check the terms of your Azure service.

Restrictions for Azure SKU Scaling, Audit, and Security Rules of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

- The multicloud audit service cannot run while a cloud gateway is being created, edited, or deleted.
- The ability to change the SKU scale values and the audit feature, and the ability to open ports temporarily apply only to cloud gateways that are created in Cisco SD-WAN Manager using the multicloud. These features do not apply to the Network Virtual Appliances created directly on the Azure portal.

Restrictions for Multiple Virtual Hub per Region

Minimum supported release: Cisco vManage Release 20.11.1

A maximum of 8 virtual hubs can be created per region.

Use Cases for Azure Virtual WAN Integration

Use Cases for Routing Traffic Flow to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

- Routing traffic to a secured virtual hub or to a local firewall may be useful where it is desirable to apply the same firewall policy to all of the Azure-based and local internet traffic, using either an Azure-based firewall or a local firewall.
- Routing local traffic to a secured virtual hub may be useful if you do not want to set up a firewall on a local branch device.
- Routing Azure traffic to a local firewall may be useful if you do not want to set up a firewall in the Azure environment.

Use Cases for Azure SKU Scaling

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

You can configure the SKU Scale value for either better performance or better cost effectiveness of cloud gateway services. If the CPU load is above 75 percent, then you can configure a higher SKU Scale value, and if the CPU load is below 25 percent, you can configure a lower SKU Scale value.

Use Cases for Azure Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

If you are facing any connectivity or networking issues, then initiate an audit. The information provided by Azure audit helps in troubleshooting the networking issues.

Use Cases for Security Rules of NVAs

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Security rules configuration of NVAs allows you to enable a particular port.

Configure Azure Virtual WAN Integration

Configure Azure Virtual WAN Hubs

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

Use the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager to create Azure virtual WAN hubs to connect your Cisco Catalyst SD-WAN branches to the applications in your private networks or Host VNets. To configure an Azure virtual WAN hub, perform the following tasks in the order specified.

Configuration Prerequisites

You need the following to be able to configure Azure virtual WAN hubs using Cisco SD-WAN Manager.

- Azure cloud account details.
- Subscription to Azure Marketplace.
- Cisco SD-WAN Manager must have two Cisco Catalyst 8000V licenses that are free to use for creating the Azure Cloud Gateway.
- Cisco SD-WAN Manager must be connected to the Internet and must be able to communicate with Microsoft Azure to authenticate your Azure account.

Integrate Your Azure Cloud Account

Associate your Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Setup**, click **Associate Cloud Account**.
3. In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.
4. Enter the requested information:

Field	Description
Cloud Account Name	Enter a name for your Azure subscription.

Field	Description
Description (optional)	Enter a description for the account. This field is optional.
Use for Cloud Gateway	Choose **Yes** to create a cloud gateway in your account. The option **No** is chosen by default.
Tenant ID	Enter the ID of your Azure Active Directory (AD). To find the tenant ID, go to your Azure Active Directory and click **Properties**.
Subscription ID	Enter the ID of the Azure subscription you want to use as part of this workflow.
Client ID	Enter your existing Azure application ID. See Azure documentation for more information on how to register an application in Azure AD, get the client ID and secret key, and more.
Secret Key	Enter the password associated with the client ID.

5. Click **Add**.



Note If you are using multiple Azure subscriptions to discover the VNets or to create cloud gateways, you must add all the subscriptions that are under the same tenant as different Azure Accounts in **Cloud OnRamp for Multicloud Set up** > **Associate Cloud Account**.

Add and Manage Global Cloud Settings

1. On the **Cloud OnRamp for Multicloud** window, click **Cloud Global Settings** in the Setup area.
2. In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.
3. To edit global settings, click **Edit**.
4. To add global settings, click **Add**.
5. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enable the **Enable Configuration Group** option to use configuration groups to configure devices in the multicloud workflow.
6. In the **Software Image** field, choose the software image of the WAN edge device to be used in the Azure Virtual Hub. This should be a preinstalled Cisco Catalyst 8000V image.



Note Choose the Cisco Catalyst 8000V image based on your Cisco SD-WAN Manager release. For Cisco SD-WAN Manager Release 20.n, choose the Cisco Catalyst 8000V image for Cisco IOS XE Release 17.n or earlier. For example, for Cisco SD-WAN Manager Release 20.5, you can choose an image corresponding to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a or Cisco IOS XE Catalyst SD-WAN Release 17.5.1a. If a software image corresponding to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later is available among the preinstalled images, do not select such an image because it is not compatible with your Cisco SD-WAN Manager release.

7. In the **SKU Scale** field, from the drop-down list, choose a scale based on your capacity requirements.
8. In the **IP Subnet Pool** field, specify the IP subnet pool to be used for the Azure virtual WAN hub. A subnet pool needs prefixes between /16 and /24. You can use /16 prefix in the global settings and then overwrite the settings with /24 when you create a cloud gateway.



Note **IP Subnet Pool** from the global settings is used only when a virtual hub is not deployed in a given region. When a virtual hub is deployed in a region, this field is auto-populated from cloud and you cannot edit the values.

A single /24 subnet pool is able to support one cloud gateway only. You cannot modify the pool if other cloud gateways are already using the pool. Overlapping subnets are not allowed.

The IP subnet pool is meant for all Azure Virtual WAN Hubs inside an Azure Virtual WAN, one /24 prefix per Virtual WAN Hub. Ensure that you allocate enough /24 subnets for all the Virtual WAN Hubs you plan to create within the Virtual WAN. If a Virtual WAN Hub is already created in Microsoft Azure, you can discover it through Cisco SD-WAN Manager and use the existing subnet pool for the discovered hub.

9. In the **Autonomous System Number** field, specify the ASN to be used by the cloud gateway for eBGP peering with the virtual hub.



Attention This value cannot be modified after a cloud gateway has been created.

10. For the **Push Monitoring Metrics to Azure** field, choose **Enabled** or **Disabled**. If you choose **Enabled**, the cloud gateway metrics associated with your Azure subscription are sent to the Microsoft Azure Monitoring Service portal periodically. These metrics are sent in a format prescribed by Microsoft Azure for all NVA vendors.



Important

- There is a separate cost associated with using the Azure Monitor Service for processing and monitoring the data sent through Cisco SD-WAN Manager. Refer to Microsoft Azure documentation for information on billing and conditions of use.
- It is the responsibility of managed service providers to provide notice to and obtain any necessary legal rights and permissions from end users regarding the collection and processing of their telemetry data.

11. From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, you can enable or disable the **Advertise Default route to Azure Virtual Hub** field. By default, this field is **Disabled**. If you click **Enabled**, the internet traffic from the virtual network is redirected through Cisco Catalyst SD-WAN branches.
12. From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, you can enable or disable the **Enable Periodic Audit** field by clicking **Enabled** or **Disabled**.

    If you the enable periodic audit, Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background, and a discrepancies report is generated.
13. From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, you can enable or disable the **Enable Auto Correct** field by clicking **Enabled** or **Disabled**. If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.
14. Click **Add** or **Update**.

Create and Manage Cloud Gateways

Creation of cloud gateways involves the instantiation or discovery of Azure Virtual WAN Hub and two Cisco Catalyst 8000V instances within the hub.

Note If you have used the Azure portal to provision Cisco Catalyst 8000V instances, and created an Azure Virtual WAN and Azure Virtual WAN Hub using the Azure portal, you can also discover them using the procedure below.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Manage**, click **Create Cloud Gateway**.
3. In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.
4. In the **Cloud Gateway Name** field, enter the name of your cloud gateway.

Note If you have created an Azure Virtual WAN Hub using the Azure portal, ensure that you enter the exact virtual hub name in this field. This ensures that the resources associated with the hub are discovered. The associated Azure Virtual WAN and Azure Virtual WAN Hub then become available for you to choose from in the **Virtual WAN** and **Virtual Hub** fields. The associated NVAs also autopopulate in the **UUID** field.

5. (Optional) In the **Description** field, enter a description for the cloud gateway.
6. In the **Account Name** field, choose your Azure account name from the drop-down list.
7. In the **Region** field, choose an Azure region from the drop-down list.
8. (From Cisco Catalyst SD-WAN Manager Release 20.13.1, applies only if you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for Azure cloud gateway) From the **Configuration Group** drop-down list, perform one of these actions:
   - Choose a configuration group.

- To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list.

The configuration group that you choose is used to configure devices in the multicloud workflow.



Note The **Configuration Group** drop-down list includes only configuration groups that you create as described in this step. It does not include other configuration groups that have been created in Cisco Catalyst SD-WAN. The configuration groups in this drop-down list include the options that are needed for this provider.

For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups.

9. In the **Resource Group** field, either choose a resource group from the drop-down list, or choose **Create New**.



Note If you choose to create a new Resource Group, you would also need to create a new Azure Virtual WAN and an Azure Virtual WAN hub in the next two fields.

10. In the **Virtual WAN** field, choose an Azure Virtual WAN from the drop-down list. Alternatively, click **Create New** to create a new Azure Virtual WAN.

11. In the **Virtual HUB** field, choose an Azure Virtual WAN Hub from the drop-down list. Alternatively, click **Create New** to create a new Azure Virtual WAN Hub.

    (Minimum supported release: Cisco vManage Release 20.11.1) When you select the **Region**, **Resource Group**, and **Virtual WAN**, the **Azure Virtual WAN Hub** field displays **Create a new vHub using Cloud Gateway Name**. From the drop-down list, select the discovered virtual hubs.

    The virtual hubs are discovered on Cisco SD-WAN Manager in two ways:

    - Virtual hubs with Network Virtual Appliances (NVAs) created on the Azure portal.
    - Virtual hubs created in the Azure portal and discovered by Cisco SD-WAN Manager. You can then add the NVAs to the virtual hubs in Cisco SD-WAN Manager.

12. (Minimum release: Cisco Catalyst SD-WAN Manager Release 20.13.1) From the **Solution Type** drop-down list, choose a virtual appliance that you want to deploy:

    - Choose **vHub with NVA** to create a network virtual appliance (NVA) in vHub with Catalyst 8000V instances. Choose this option to deploy Cisco SD-WAN devices in controller mode.
    - Choose **vHub with VPN** to create a VPN gateway in vHub, which is a bridge for on-premises devices to enter cloud resources. Choose this option to deploy Cisco SD-Routing devices in autonomous mode.

13. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.

14. In the **Settings** field, choose one of the following:

- **Default** - The default values of IP subnet pool, image version, and SKU Scale size are retrieved from global settings.
- **Customized** - you can override the global settings with this option. This option is applicable only for the newly created cloud gateway.

(Minimum supported release: Cisco vManage Release 20.10.1)

In the **Instance Setting** area, the following fields are auto-populated with the configurations from the global settings only when you onboard the virtual hubs with Cisco Catalyst 8000V created on Azure portal to Cisco SD-WAN Manager:

- **Software Image**
- **SKU Scale**
- **IP Subnet Pool**
- **UUID (specify 2)**



Note When the cloud gateways are onboarded on Cisco SD-WAN Manager, without the NVAs, the **IP Subnet Pool** and **UUID (specify 2)** fields are auto-populated.

Routers in NVA get IP addresses over DHCP in the Azure portal. Cisco SD-WAN Manager learns the IP addresses assigned to the routers via API's.

You can override the global settings by selecting the options in the drop-down list.

15. From Cisco Catalyst SD-WAN Manager Release 20.13.1, applies only if you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for Azure cloud gateway) In the **Configuration Group**, choose the name of the configuration group that is to be used to create the cloud gateway, or create a new configuration group.

(

16. In the **UUID (specify 2)** field, choose two Cisco Catalyst 8000V licenses from the drop-down list.



Note From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

17. (Minimum release: Cisco vManage Release 20.10.1) In the **Multi-Region Fabric Settings** area, for **MRF Role**, choose **Border** or **Edge**.

    This option is available only when Multi-Region Fabric is enabled.

18. Click **Add**.



Note It can take up to 40 minutes for your Azure Virtual WAN hub to be created and for the Cisco Catalyst 8000V instances to be provisioned inside the virtual hub.

Note Once the creation of the Azure Virtual WAN Hub is complete, you have the option to convert it into a secured Azure Virtual WAN Hub. However, this configuration can only be completed through the Microsoft Azure portal. See Microsoft Azure documentation for more information.

Note You can simultaneously create Azure cloud gateways in different regions.

- Before creating multiple cloud gateways in different regions, create the resource group, virtual WAN, and storage account for the first cloud gateway.
- Before creating multiple cloud gateways in the same region, create the virtual hub for the first cloud gateway in the region.
- You need to have blob access to create a storage account in Azure for the Cloud OnRamp for Multicloud. Blob access is required while creating cloud gateways and modifying scale operations on the Cisco Catalyst 8000V devices.

Note The Cloud OnRamp for Multicloud workflow supports up to eight virtual hubs in each Azure region. You can deploy two cloud gateway Network Virtual Appliances (NVAs) in each virtual hub.

Discover Host VNets and Create Tags

After you create an Azure virtual hub, you can discover your host VNets in the region of the virtual hub.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Discover** workflow, click **Host Private Networks**.
3. In the **Cloud Provider** field, choose **Microsoft Azure**.

   A list of your host VNets displays in a table with the following columns: Cloud Region, Account Name, VNET Tag, Cloud Gateway Attachment, Account ID, Resource Group, and VNet Name.
4. Click the **Tag Actions** drop-down list to choose any of the following:
   - **Add Tag:** Create a tag for a VNet or a group of VNets.

     (Minimum supported release: Cisco vManage Release 20.11.1) You can choose the **Cloud Gateway Attachment** as **Auto** or map with an existing cloud gateway.
   - **Edit Tag:** Change the existing tag of a selected VNet.

     (Minimum supported release: Cisco vManage Release 20.11.1) You can choose the **Cloud Gateway Attachment** from the **Edit Tag**. The **Auto** option is automatically selected, if you choose not to make a selection or if the cloud gateway is not yet created in that region. The **Auto** option is based on a load balancing algorithm. For VNets with the **Auto** option selected, the cloud gateway attachments are selected during mapping and not when the tag is created.
   - **Delete Tag:** Delete the tag for the selected VNet.

Map VNets Tags and Branch Network VPNs

To enable VNet to VPN mapping, you select a set of VNets in one or multiple Azure regions and define a tag. You then select the service VPNs that you want to map the VNets to using the same tags. Only a single set of VNets can be mapped to a single set of branch offices. All selected VNets are visible to all selected VPNs and vice versa. One service VPN can be mapped to a single or multiple tags. Multiple VNets could have the same tag. Mapping is automatically realized when a cloud gateway exists in the same region or when tagging operations take place.

Note The VPNs selected to be mapped to VNet tags must not have overlapping IP addresses. This is because segmentation is not supported in Microsoft Azure Virtual WAN.

To edit the VNet-VPN mapping for your Cisco Catalyst SD-WAN networks, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under, **Intent Management** click **Connectivity**.
3. To define the intent, click **Edit**.
4. Choose the cells that correspond to a VPN and the VNet tags associated with it, and click **Save**.

The **Intent Management - Connectivity** window displays the connectivity status between the branch VPNs and the VNet tags they are mapped to. A legend is available at the top of the screen to help you understand the various statuses. Click any of the cells in the matrix displayed to get a more detailed status information, such as, Mapped, Unmapped, and Outstanding mapping.

Rebalance VNets

Minimum supported release: Cisco vManage Release 20.11.1

You can choose to redistribute VNets to load balance the existing VNets among all the cloud gateways in a region for a given tag at any time. You can reassign only the VNets with **Auto** option selected across cloud gateways. The VNets assignment is based on a load-balancing algorithm. As the rebalancing involves detachment and re-attachments of VNETs to cloud gateways, traffic disruption may occur. After rebalancing the VNets, you can view the revised mapping of VNETs to cloud gateways on the tagging page.

Note You cannot rebalance VNets when:

- Create, edit, or delete of Cloud gateway is in progress.
- Mapping of VNets is in progress.
- Audit is in progress.

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Cloud OnRamp for Multicloud**.
2. In **Intent Management** workflow, click **Rebalance VNETS (Azure/GovCloud)**
3. In the **Cloud Provider** field, choose **Microsoft Azure**.

4. In the **Region** field, choose an Azure region from the drop-down list.
5. In the **Tag Name** field, choose a tag from the drop-down list.
6. Click **Rebalance**.

Configure an Azure Virtual WAN Hub Through the Azure Portal

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

Note The end-to-end configuration of Azure virtual WAN hub can be done using Cisco SD-WAN Manager. Alternatively, you can use the Azure portal to create resource groups, virtual WAN, and virtual WAN hub, and then return to Cisco SD-WAN Manager to discover the infrastructure you created using the Azure portal, and then create VNet tags and map them to your service VPNs.

Configuration Workflow

Task	Description
Task 1	From the Cisco SD-WAN Manager menu, select two Cisco Catalyst 8000V instances that are free to use for the Azure virtual WAN hub. Next, generate and download a bootstrap configuration file for these instances.
Task 2	In the Azure portal, create a managed identity and a custom role with the necessary permissions. Assign the role to the managed identity in the resource group.
Task 3	In the Azure portal, create a virtual WAN hub and associate the Cisco Catalyst 8000V instances with the virtual WAN hub you create.
Task 4	In the Azure portal, create NVAs for Cisco Catalyst 8000V using the bootstrap configuration file generated in Cisco SD-WAN Manager.
Task 5	In Cisco SD-WAN Manager, discover the infrastructure you created in the Azure portal. As part of this discovery, the NVAs created in the Azure Virtual WAN Hub are brought up.
Task 6	In Cisco SD-WAN Manager, configure connectivity between the host VNets and service VPNs by mapping VNet tags.

Note Any configuration done using the Azure portal is out of scope of this document. However, we've provided links to Azure documentation to help you complete the configuration using the Azure portal.

Task 1. Generate Bootstrap Configuration for Cisco Catalyst 8000V

Prerequisite: You must have licenses available in Cisco SD-WAN Manager for two Cisco Catalyst 8000V instances before proceeding with the next steps.

To generate bootstrap configuration for Cisco Catalyst 8000V using configuration groups, ensure that you have enabled the **Enable Configuration Group** option in the Azure global settings and follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.
3. In the **Configuration groups** field, create a new configuration group by choosing **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**.
4. Once you create the configuration group, click **Cancel** to abort the cloud gateway creation workflow.
5. Associate the Cisco Catalyst 8000V devices to the configuration group that you created in Step 3. For more information see, Add Devices to a Configuration Group.
6. Deploy a Configuration Group.
7. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
8. Locate the devices you updated and for each of the devices, click **...**. Choose **Generate Bootstrap Configuration** from the options.
9. On the **Generate Bootstrap Configuration** dialog box, deselect **Include Default Root Certificate** , and click **OK**.

   You can see the **Include Default Root Certificate** option only if you have an enterprise certificate for Cisco SD-WAN Manager.
10. On the dialog box, click **Download**.

To generate bootstrap configuration for Cisco Catalyst 8000V using templates, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

3. From the **Template Type** drop-down list, choose **Default**.

   A list of default templates is displayed.
4. For the desired row in **Default_Azure_vWAN_C8000V_Template_V01**, click **...** and choose **Attach Devices**.
5. From the list of **Available Devices**, choose two Cisco Catalyst 8000V instances and click **Attach**.

   On the next screen, you'll see the devices that you attached to the device template.
6. On the Device Templates screen, for each of the device rows, click **...** and choose **Update Device Template**.

7. For each of the devices, enter the requested information: Host Name, System IP, and Site ID. Click **Update**.
8. Click **Next**. On the **Configure Devices** dialog box, check the check-box and click **OK**.

   The **Task View** screen opens. It takes a few minutes for the device information to be updated. When the status column shows the status as **Done - Complete**, it indicates that the device information has been updated.
9. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
10. Locate the devices you updated and for each of the devices, click **...**. Choose **Generate Bootstrap Configuration** from the options.
11. On the **Generate Bootstrap Configuration** dialog box, deselect **Include Default Root Certificate** , and click **OK**.
12. On the dialog box, click **Download**.

Task 2. Create a Managed Identity and a Custom Role

In the Azure portal, complete the following:

1. Create managed identities.
2. Create a custom role.
3. Assign the custom role to the managed identity for a resource group hosting the virtual WAN Hub.

Task 3. Create Azure Virtual WAN Hub

The steps in this section are performed in the Azure portal. We have provided links to Azure documentation for completing these step. You need an Azure subscription and login credentials to perform the steps in this section.

In the Azure portal, complete the following:

1. Create resource groups.
2. Create a virtual WAN.
3. Create a virtual WAN hub.

Next step: In the virtual hub, create a Network Virtual Appliance (NVA) for your Cisco Catalyst 8000V instances. The procedure to create NVAs may differ for various NVA partners. Therefore, we've provided information specific to Cisco Catalyst 8000V in the next section.

Task 4. Create NVA for Cisco Catalyst 8000V

1. In the Azure portal, search for **Cisco Cloud vWAN Application** in the search box and click the result under Marketplace.
2. The **Cisco Cloud vWAN Application** page opens. Click **Create**.

   Enter the requested details and click **Next: Cisco SD-WAN Cloud Gateway**.
3. Click **NVA Application Settings**.
   a. Click **Add**.

b. Check the check box to select the managed identity created in Task 2.

4. Enter the requested details. The details you enter on this screen are similar to the Cloud Global Settings screen in Cisco SD-WAN Manager.
   a. **Virtual WAN:** Choose the virtual WAN your created from the drop-down list.
   b. **Virtual WAN Hubs:** When you choose a virtual WAN, all the virtual hubs in that WAN are shown in the drop-down list. Choose the virtual WAN hub you want to use for this procedure.
   c. **Scale Unit:**
   d. **Cisco Version:** Enter the software version for the Cisco Catalyst 8000V instances.
   e. **BGP ASN to peer with Azure Router Service:** This is the number that the NVA uses.
   f. **Cisco SDWAN Cloud Gateway Name:** Enter a name for the cloud gateway.
   g. **Upload the Bootstrap configuration File that was generated:** Using this field, navigate to the bootstrap configuration files you downloaded for Cisco Catalyst 8000V from Cisco SD-WAN Manager.



Note Ensure that you select both the bootstrap configuration files at this step.

5. Click **Next** and retain the default values.
6. Check the check box to agree to the terms and conditions. Click **Create**.

   When the deployment is complete, two Cisco Catalyst 8000V instances are provisioned inside the virtual hub. When they come up, they are also connected to Cisco SD-WAN Manager.

In Cisco SD-WAN Manager, on the main dashboard, click the upward arrow next to Devices. If your deployment through the Azure portal is successful, you'll see the two Cisco Catalyst 8000V instances show as reachable.

Task 5. Discover NVAs in Cisco SD-WAN Manager

Prerequisite: To discover NVAs in Cisco SD-WAN Manager, your Azure account should be added in Cisco SD-WAN Manager. If you haven't already associated your Azure account with Cisco SD-WAN Manager, see Integrate Your Azure Cloud Account, on page 15.

To discover your NVAs or the Cisco Catalyst 8000V you configured using the Azure portal, follow the steps outlined in Create and Manage Cloud Gateways, on page 18.

Task 6. Configure Connectivity Between VNets and VPNs

To configure VNet to VPN tagging, you first need to discover the host VNets in your Azure regions and create tags and then map these tags to connect the VNets and your branch networks or VPNs.

Configure Routing of Traffic Flow to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

Route Local Outgoing Traffic Flow to an Azure Secured Virtual Hub

Before You Begin

- Configure integration of your Azure Virtual WAN hub with Cisco Catalyst SD-WAN. For information about this, see Azure Virtual WAN Hub Integration with Cisco SD-WAN.
- Configure a firewall in the Azure environment, including the desired firewall policy.

Route Local Outgoing Traffic Flow to an Azure Secured Virtual Hub

To configure a branch router to route outgoing internet traffic to an Azure secured virtual hub, perform these steps.

1. On the local branch router, verify that the branch router does not have a static default route configured for direct internet access (DIA) from the branch.

   On the local branch router, use the **show ip route vrf** *vrf-number* command to verify that the static default route is not configured for the service side VPN.

2. On the local branch router, use the **show ip route vrf** *vrf-number* command to verify that internet traffic from the local branch router has been routed to the Azure firewall using the VRF that you have configured for communication between the local branch router and Azure. In the command output, look for the IP addresses associated with the default route, which is represented as 0.0.0.0. The IP addresses must correspond to the cloud gateways operating in the Azure hub where the Azure firewall is enabled.

   The following example uses VRF 100. In the example, only a portion of the command output is shown. The IP addresses that correspond to the cloud gateways operating in the Azure hub are 209.165.201.1 and 209.165.201.2.

   ```
   Device# show ip route vrf 100

   ...
   m*    0.0.0.0/0 [251/0] via 209.165.201.1, 21:06:00, Sdwan-system-intf
                   [251/0] via 209.165.201.2, 21:06:00, Sdwan-system-intf
   ...
   ```

3. In the Azure environment, configure internet traffic to be routed through the Azure firewall.

Route Azure Outgoing Traffic Flow to a Local Branch Router

Before You Begin

- Configure integration of your Azure Virtual WAN hub with Cisco Catalyst SD-WAN. For information about this, see Azure Virtual WAN Hub Integration with Cisco SD-WAN.
- Configure a firewall on the local branch router, including the desired firewall policy.

Route Azure Outgoing Traffic Flow to a Local Branch Router

To configure Azure to route outgoing internet traffic to a local branch router firewall, perform these steps.

1. In Cisco SD-WAN Manager, use the CLI template for the local branch router to add the following commands to the configuration. This advertises the local router as the default route for the Azure

environment, causing the Azure virtual network to route its outgoing internet traffic to the branch router. Note that 0.0.0.0 represents the default route.

```
address-family ipv4 vrf branch-router-vpn-id
   advertise connected
   advertise static
   advertise network 0.0.0.0/0
```

Only traffic in the specified VPN is directed to the branch router. For information about how VPNs map the connectivity between Cisco Catalyst SD-WAN and Azure, see How Virtual WAN Hub Integration Works.

The following example directs Azure traffic in VPN 100 to the branch router:

```
address-family ipv4 vrf 100
   advertise connected
   advertise static
   advertise network 0.0.0.0/0
```

2. In the Azure environment, verify that the traffic is routed to the local branch router. View the routing table and verify that the following appears:

   Prefix: 0.0.0.0/0
   Next Hop Type: VPN_S2S_GATEWAY

Configure SKU Scale Value

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to configure SKU Scale value:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Cloud Gateways** with a table displaying the list of cloud gateways with cloud account name, ID, cloud type, and other information, is displayed.
3. Click **...** adjacent to the corresponding cloud gateway, and choose **Edit**.
4. From the **SKU Scale** drop-down list, choose a value. .

Note Only SKU Scale values **2**, **4**, and **10** are supported.

5. Click **Update**.

Initiate On-Demand Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

This is a user-invoked audit. Follow these steps to initiate an on-demand audit:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

2. Click **Audit** under **Intent Management**.
3. For the **Cloud Provider** drop-down list, choose **Microsoft Azure**.

   The window displays the status for various Microsoft Azure objects. If the status is **In Sync** for any of the objects, it means the object is free from errors. If the status of an object is **Out of Sync**, it means that there are discrepancies between the object details available on Cisco SD-WAN Manager and the details available on the Azure database.
4. If the status is **Out of Sync** for any of the objects, click **Fix Sync issues**. This option resolves recoverable errors, if any, and opens a window that displays the status activity log.

   If the status of an object still shows **Out of Sync**, it means that it is an error that requires manual intervention.

Note The multicloud audit service does not run while other cloud operations are in progress.

Enable Periodic Audit

The following steps describe the procedure to enable periodic audit:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Setup** area, click **Cloud Global Settings**.
3. To enable or disable the **Enable Periodic Audit** field, click **Enabled** or **Disabled**.

   If you click **Enabled**, Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background, and a discrepancies report is generated.

   For examples on audit discrepancies and resolutions, see Examples of Audit Discrepancies.
4. Click **Update**.

Configure Security Rules of NVAs

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to configure security rules for NVA:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Create Cloud Gateways** window with a table displaying the list of cloud gateways with cloud account name, ID, cloud type, and other information is displayed.
3. Click **...** adjacent to the corresponding cloud gateway, and choose **Add/Edit Security Rules**.

   The **Add/Edit Security Rules** window is displayed.

   a. To add a new security rule, click **Add Security Rule** and provide the following details:

Table 4: Parameters Table

Parameter	Description
Port Number	Provide the port range.
IPv4 Source Address	Provide the IP address.

b. Click **Add**.

c. (Optional) To edit a security rule, click the pencil icon.

d. (Optional) To delete a security rule, click the delete icon.

4. Click **Update**.

Note All the security rules are active only for two hours.

Verify Azure Virtual WAN Integration

View, Edit, or Delete a Cloud Gateway

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Cloud OnRamp for Multicloud**.
2. Click **Cloud**.
3. Under **Manage**, click **Gateway Management**.

   Existing cloud gateway details are summarized in a table.
4. In the table, click **…** for the desired Cloud Gateway.
   - To view more information about the cloud gateway, click **View**.
   - To edit the cloud gateway description, click **Edit**.
   - To delete the cloud gateway, click **Delete** and confirm that you wish to delete the gateway.

     (Minimum supported release: Cisco vManage Release 20.11.1) If you delete a cloud gateway, the attached VNets move to other selected cloud gateways in the same region based on a load balancing algorithm and the VNets are marked as **Auto**.

Verify Azure SKU Scale Value Update

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to verify the Azure SKU scale value update:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Create Cloud Gateways** window is displayed. A table displays the list of cloud gateways with cloud account name, ID, cloud type, and other information.
3. Click **...** adjacent to the corresponding cloud gateway, and choose **View**.

   The changed SKU value appears on the **View Cloud Gateway** window.

Verify Security Rule for Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to verify a security rule created for NVA:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Create Cloud Gateways** window with a table displaying the list of cloud gateways with cloud account name, ID, cloud type, and other information is displayed.
3. For the desired cloud gateway, click **...** and choose **Add/Edit Security Rules**.

   The **Add/Edit Security Rules** window is displayed along with one of the following statuses of the updated security:

   - **Successful**
   - **In-progress: Check the status after sometime.**
   - **Failed: Recreate the security rule.**

Monitor Azure Virtual WAN Integration Using Cisco SD-WAN Manager

Monitor Azure Virtual WAN Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

NVA Connectivity

When you create a new cloud gateway, you can verify the creation and reachability of the Cisco Catalyst 8000V instances provisioned inside the Azure virtual WAN hub. To view whether these instances are configured successfully and are reachable, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

Cisco SD-WAN Manager Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

2. Under **WAN Edge**, click the upward arrow next to the number displayed. The number represents the WAN Edge devices available.
3. In the table that displays in the pop-up window, look for the Cisco Catalyst 8000V instances you chose while creating a cloud gateway. If your cloud gateway configuration was successful, the instances should appear in the table and show as reachable.

Monitor NVA Data Using Microsoft Azure Monitor Service

In Cisco SD-WAN Manager, you can enable sending metrics to the Azure portal using the **Cloud OnRamp for Multicloud** > **Cloud Global Settings** window.

If you enable the **Push Monitoring Metrics to Azure** option, data about all the Cloud Gateways associated with the Azure account, that you have integrated with Cisco SD-WAN Manager, is sent to the Azure Monitor service.

For details about the Azure Monitoring service, see Azure documentation.



Important

- There is a separate cost associated with using the Azure Monitor Service for processing and monitoring the data sent through Cisco SD-WAN Manager. Refer to Microsoft Azure documentation for information on billing and conditions of use.
- It is the responsibility of managed service providers to provide notice to and obtain any necessary legal rights and permissions from end users regarding the collection and processing of their telemetry data.