Cloud Infrastructure on SD-Routing Devices

First Published: 2024-03-28

Last Modified: 2024-04-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

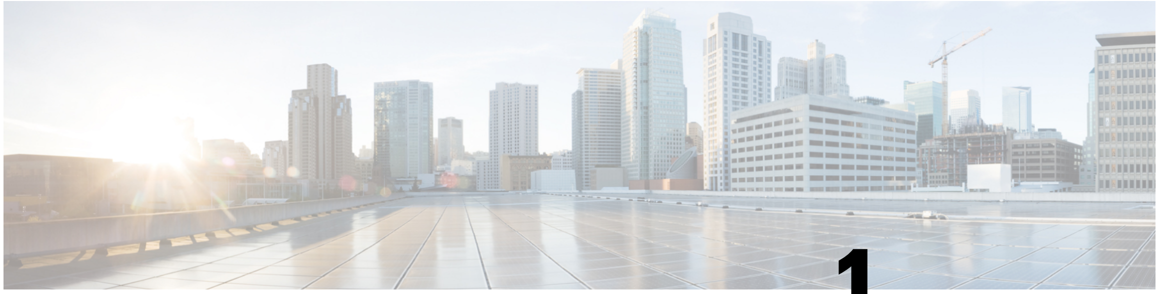
Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

- Reference Preface Map here, on page vii

Reference Preface Map here



CHAPTER 1

Overview

Cisco Catalyst SD-Routing Cloud OnRamp for Multicloud extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into the Cisco Catalyst SD-Routing devices. Using the AWS Transit Gateway (TGW), we support SD-Routing branch sites. With these capabilities, the branch devices can access the applications interfacing with cloud networks. This feature is supported from the Cisco IOS XE 17.13.1a release onwards.

Note From Cisco IOS XE 17.12.1a, the following components have been rebranded: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager** and **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**.

Information About the AWS Integration

A transit gateway is a network transit hub that you can use to interconnect your VPC and on-premises networks. You can attach a VPC, or a VPN connection to a transit gateway. It acts as a virtual router for traffic flowing between your VPC and VPN connections.

You can configure and manage Cloud OnRamp for Multicloud environments through the Cisco SD-WAN Manager controller. A configuration wizard in Cisco SD-WAN Manager automates the bring-up of the transit gateway to your public cloud account and automates the connections between public-cloud applications and the users of those applications at branches in the overlay network. This feature works with AWS virtual private clouds (VPCs) on Cisco cloud routers.

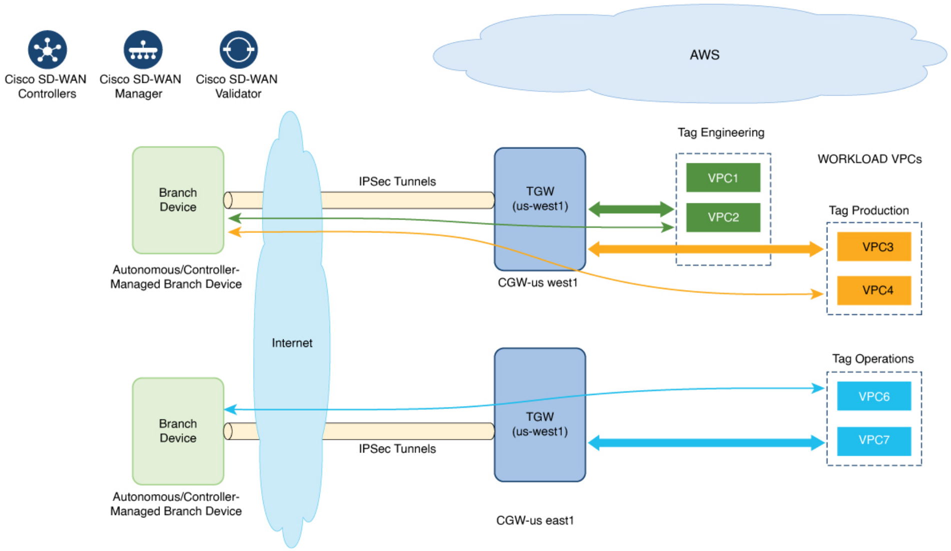
Cloud OnRamp for Multicloud supports integration with multiple AWS accounts.

AWS Branch Connect with SD-Routing Devices

When you deploy SD-Routing Cloud OnRamp through SD-Routing based branch, it should be deployed though the SD-Routing based Config group. Also, you should set the bootup license level manually through the respective CG device CLI template for the tunnel-based config to work during Cloud OnRamp connectivity.

The edge/branch devices connect to the host VPCs in the cloud over secure point-to-point tunnels. IPSec tunnels are set up between edge devices and the AWS Transit Gateway (TGW). These tunnels carry the branch

VPNs or VRFs traffic and BGP routing traffic. Using BGP, the devices and the transit gateway exchange the routing information and build routing tables.



The SD-Routing branch device can have only the default VRF. You can use this default VRF to mapping through the SD-Routing Cloud OnRamp branch connect. You cannot use any other VPN/VRF for mapping. Along with SD-Routing solcution, you can have multiple VPN mapping for SD-WAN solution. Both the Cisco SD-WAN and Cisco SD-Routing connection can co-exist.

Note A branch site can have more than one branch endpoint connecting to the cloud.

Benefits of Cloud OnRamp for SD-Routing Devices

SD-Routing Cloud OnRamp supports secure cloud connectivity for the cloud workloads deployed in AWS or Azure using SD-Routing devices through Multicloud workflows.

Prerequisites for Cloud onRamp

The following are the prerequisites for Cloud onRamp:

- The branch site should be in reachable state and the status should be In-Sync.
- The branch site should have one of these boot level licenses:
  - network-advantage
  - network-essentials
  - network-premier

  Otherwise, when you attach the site, the IPSec tunnel configurations will not get applied.
- Interface should have a public IP address assigned that is reachable from AWS TGW or Azure vHub, or NAT on the branch device. Otherwise, the tunnel will not be formed between the branch site and AWS TGW or Azure vHub.

- SD-routing branch should be deployed using or ported to Config-Group.
  - Refer to Onboarding the Existing Devices , on page 3 and Onboarding the New SD-Routing Device Using Config Group Automated Workflow, on page 4 sections to On-board or to get SD-Routing device compatible to use the Cloud onRamp feature.

Limitations

- Cloud OnRamp does not support peering between the TGWs in different regions.

Configure AWS Integration on SD-Routing Devices

This section explains the workflows to onboard the SD-Routing devices for features:

- Onboarding the existing devices:
  - Converting the existing Autonomous Device to SD-Routing device and use the Cloud onRamp feature
  - Converting the existing Non-config group based SD-Routing devices to use Cloud onRamp feature
- Onboarding new SD-Routing device using Config Group Automated Workflow

Onboarding the Existing Devices

To onboard the existing devices, perform these steps:

Step 1 To deploy or convert the existing autonomous device to SD-Routing device manually, follow the instruction provided in the section Onboarding the Devices Manually.

Or

Step 2 To deploy SD-Routing device using the Quick Connect Workflow follow the instruction provided in the section Onboarding the SD-Routing Devices Using Bootstrap.

Pre-requisities:

Step 3 To port the SD-Routing device to Configuration Group, do the following:

Note The devices from steps 1 and 2 should have following pre-requisities taken care before proceeding further:

- Log into the device using the username and password (admin/admin).
- At the command prompt, configure the **license boot level network-advantage addon dna-advantage** command.
- Save the configuration and reboot the device. Ensure that the device is in-sync under Configuration Devices in Cisco SD-WAN Manager.

a) From Cisco IOS XE Catalyst SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** > **Add CLI based Configuration Group**

b) In the **Add CLI Group** pop-up dialog box, enter the configuration group name.

c) Click the **Solution Type** drop-down list and select the solution type as **sd-routing** for the SD-Routing devices.

d) In the **Description** field, enter the description.

e) Click **Create**.

The new configuration group page is displayed with the Feature Profiles and Associated Device tabs.

f) Click **Load Running Config from Reachable Device** from the drop-down list and select the System-IP of the device for which you want to build the configuration. You can edit the configuration based on the requirement in the Preview text box.

g) Copy the configuration that is loaded in the **Configuration Preview** text box and save it in your system as a text file.

Step 4 To add the Configuration Group on the SD-routing device, do the following:

a) From **Cisco SD-WAN Manager** menu, choose **Configuration** > **Configuration Groups** > **Add Configuration Group** > **Create SD-Routing Config** .
b) In the **Name** field, enter a name for the configuration group.
c) In the **Description** field, enter the description.
d) Click **Create SD-Routing Config**.
e) In the **Configuration Group Created** pop-up dialog box, click the **No, I will Do It Later** option.
f) From the **What's Next?** section, click **Go to Configuration Groups**.
g) Click **(…)** adjacent to the configuration group name and choose **Edit**.
h) Click on the CLI profile under Feature Profiles and select **Unconfigured**.
i) Click **Create New**.
j) Enter an unique name. Copy and paste the configuration that is saved as a text file.
k) Click **Save**.

Step 5 Click on **Associate Devices** and selct the Site ID for the SD-routing device and proceed with associtation.

Step 6 Click on the deployment status link and ensure that the deployent is successful.

Step 7 Check the following details in the **Configuration** > **Devices** page.

- Device Status - The status of the device should be In Sync
- Managed By - The respective SD-Routing Config Group created in Step 4a.

Step 8 To verify the status, use the **show sd-routing connections summary** command.

Onboarding the New SD-Routing Device Using Config Group Automated Workflow

To onboard the new SD-Routing device using Config Group automated workflow, perform these steps:

Step 1 From **Cisco SD-WAN Manager** menu, choose **Configuration** > **Configuration Groups** > **Add Configuration Group** > **Create SD-Routing Config** .

Step 2 In the **Name** field, enter a name for the configuration group.

Step 3 In the **Description** field, enter the description.

Step 4 Click **Create SD-Routing Config**.

Step 5 In the **Configuration Group Created** pop-up dialog box, click the **No, I will Do It Later** option.

Step 6 From the **What's Next?** section, click **Go to Configuration Groups**.

Step 7 Click **(…)** adjacent to the configuration group name and choose **Edit**.

Step 8 Click on the Cli profile under Feature Profiles and select **Unconfigured**.

Step 9 Click **Create New**.

Step 10 Configure the basic Configuration Group.

This example shows the minimum CLIs for the Config Group.

```
Configurations:
==============
sd-routing
organization-name CSRQA20231024
site-id 1
system-ip 4.7.8.9
vbond ip 44.226.182.48
vbond port 12346
wan-interface GigabitEthernet1
!
interface GigabitEthernet1
no shutdown
negotiation auto
ip address dhcp
exit
interface GigabitEthernet2
no shutdown
negotiation auto
ip address dhcp
exit

ip domain lookup

license boot level network-advantage addon dna-advantage
no logging console
```

Step 11 Click **Save**.

Step 12 Click on **Associate Devices** > **Associate Devices**.

Step 13 Choose **Unassigned** and select one UUID .

Step 14 Click **Save.**

Step 15 You can provision the device with the respective Sytem IP, Site ID, and Host name.

Step 16 Click **Next** .

Step 17 Click **Deploy**,

Step 18 Click on the deployment status link and ensure that the deployent is successful.

Step 19 Go to **Configuration** > **Devices** > against the uuid three dots click "generate bootstrap " enter the wan interface name (eg: GigabitEthernet1) and genreta the bootstrap

Step 20 Click **(…)** adjacent to the UUID name and click **Generate bootstrap** .

Step 21 In the **WAN Interface** field, enter interface name a GigabitEthernet1 and generatethe bootstrap.

Step 22 Use the bootstrap to deploy the Cisco 8000v instance against the respective AMI in AWS console and assign the public IP to the WAN interface.

Step 23 Click on the deployment status link and ensure that the deployment is successful.

Step 24 Check the following details in the **Configuration** > **Devices** page.

- Device Status - The status of the device should be In Sync
- Managed By - The respective SD-Routing Config Group created in Step 1.

Step 25 To verify the status, use the **show sd-routing connections summary** command.

Create AWS Cloud Account

To create the AWS cloud account, follow these steps:

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

Step 2 Click **Associate Cloud Account** in the Setup pane. Note the external Id from the **Associate Cloud Account** page.

Step 3 In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.

Step 4 Enter the account name in the **Cloud Account Name** field.

Step 5 (Optional) Enter the description in the **Description** field.

Step 6 In **Use for Cloud Gateway**, choose **Yes** if you want to create cloud gateway in your account, or choose **No**.

Step 7 Choose the authentication model you want to use in the field **Login in to AWS With**.

- **Key**
- **IAM Role**

If you choose the **Key** model, then provide **API Key** and **Secret Key** in the respective fileds.

Or

If you choose the **IAM Role** model, then create an IAM role with Cisco SD-WAN Manager provided **External ID**. Note the displayed external Id from the window and provide the **Role ARN** value that is available when creating an IAM role.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, to create an IAM role, you must enter the External Id provided by Cisco SD-WAN Manager into a policy by using the AWS Management Console. Do the following:

a. Attach an IAM Role to an existing Cisco SD-WAN Manager EC2 instance.

1. See the Creating an IAM role (console) topic of AWS documentation to create a policy. In the AWS **Create policy** wizard, click **JSON** and enter the following JSON policy document.

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]

}
```

2. See the Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console blog of AWS Security Blog for information about creating an IAM role and attaching it to the Cisco SD-WAN Manager EC2 instance based on the policy created in Step 1.

   Note On the **Attach permissions policy** window, choose the AWS managed policy that you created in Step 1.

Note The following set of permissions are allowed:

- AmazonEC2FullAccess
- IAMReadOnlyAccess
- AWSNetworkManagerFullAccess
- AWSResourceAccessManagerFullAccess

For more information on creating an AWS IAM Role, refer Creating an AWS IAM Role.

b. Create an IAM role on an AWS account that you want to use for the multicloud environment.

1. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require external ID** and pasting the external Id that you noted in Step 2.

2. See the Modifying a role trust policy (console) topic of AWS Documentation to change who can assume a role.

   In the **IAM Roles** window, scroll down and click the role you created in the previous step.

   In the **Summary** window, note the **Role ARN** that is displayed at the top.

   Note You can enter this role ARN value when you choose the authentication model as IAM role in Step 7.

3. After modifying the trust relationship, click **JSON** and enter the following JSON document. Save the changes.

   Note The account Id in the following JSON document belongs to the Cisco SD-WAN Manager EC2 instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
       }
      }
    }
  ]
}
```

Step 8 Click **Add**.To view or update cloud account details, click **...** on the Cloud Account Management page. You can also remove the cloud account if there are no associated host VPC tags or cloud gateways.

Configure Cloud Global Settings

To configure cloud global settings for AWS, peform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Cloud Global Settings** in the **Setup** pane. The **Cloud Global Settings** window appears.

Step 2 In the **Cloud Provider** field, choose **Amazon Web Services**.

Step 3 Click **Cloud Gateway Solution** drop-down list to choose the Transit Gateway–Branch-connect.

- **Transit Gateway–Branch-connect**—Allows connectivity of different SD-Routing devices to VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. This option uses the AWS VPN connection (IPSec) approach.

Step 4 In the **Cloud Gateway BGP ASN Offset** field, enter the value.

Step 5 Choose the **Intra Tag Communication**. The options are **Enabled** or **Disabled**

Step 6 Choose the **Program Default Route in VPCs towards TGW/Core**. The options are **Enabled** or **Disabled**.

Step 7 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.

Step 8 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.

Step 9 Click **Add** or **Update**.

Discover Host Private Networks

You can discover host VPCs in all the accounts across all the respective regions of the account that are available. When the **Host VPC Discovery** is invoked, the discovery of the VPCs is performed without any cache.

To discover the host private networks, peform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Host Private Networks** under **Discover**. The **Discover Host Private Networks** window appears with the list of available VPCs.

The host VPC table includes the following columns:

- Cloud Region
- Account Name
- Host VPC Name
- Host VPC Tag
- Account ID
- Host VPC ID

Click a column to sort the VPCs, as required.

Step 2 Click the **Region** drop-down list to select the VPCs based on particular region.

Step 3 Click **Tag Actions** to perform the following actions:

- **Add Tag** - group the selected VPCs and tag them together.
- **Edit Tag** - migrate the selected VPCs from one tag to another.
- **Delete Tag** - remove the tag for the selected VPCs.

A number of host VPCs can be grouped under a tag. All VPCs under the same tag are considered as a singular unit.

Create a Cloud Gateway

Cloud gateway is an instantiation of Transit VPC (TVPC)and transit gateway in the cloud. To create a cloud gateway, perform the following steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Create Cloud Gateway** under **Manage**. The **Manage Cloud Gateway - Create** window appears.

Step 2 In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.

Step 3 In the **Cloud Gateway Name** field, enter the cloud gateway name.

Step 4 (Optional) In the **Description**, enter the description.

Step 5 Choose the account name from the **Account Name** drop-down list.

Step 6 Choose the region from the **Region** drop-down list.

Step 7 Click **Add** to create a new cloud gateway.

Attaching Sites

To attach sites to a cloud gateway, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** > **Gateway Management** under **Manage**. The **Cloud Gateway** window appears. A table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.

For each of the cloud gateways, you can view, delete, or attach more sites.

Step 2 For the desired cloud gateway, click **(…)** and choose **Cloud Gateway**.

Step 3 Click **Attach SD-Routing**.

Step 4 Click **Attach Sites**.

Step 5 Click **Next**. The **Attach Sites - Select Sites** window appears. The table shows the sites with the selected WAN interface.

Step 6 Choose one or more sites from **Available Sites** and move them to **Selected Sites**.

Step 7 Click **Next**.

Step 8 On the **Attach Sites - Site Configuration** window, enter the **Tunnel Count**. The tunnel count ranges from 1 to 8 and each tunnel gives a bandwidth of 2.5 Gbps.

Step 9 On **Attach Sites - Select Interface** window, enter the details of the Interface . This interface is used to form the tunnel to TGW.

Step 10 For the **Accelerated VPN** option, choose **Enabled** or **Disabled**. AWS Global Accelerator helps in optimized connectivity to the cloud.

Step 11 For the **Use selected interface as Preferred Path** option, chose **Enabled** or **Disabled**. Multicloud workflow will configure the selected WAN interface as the default path.

Step 12 Click **Next**.

Step 13 Click **Save and Exit**. If the configuration is successful, you see a message that indicates that the branch devices are successfully attached.

Step 14 To verify the status of the device, use the **show running config** command.

Step 15 To view the status of the configuration, from the Cisco SD-WAN Manager menu, choose **Configuration**> **Configuration Groups**> **Feature Profile** and click **View Details**.

Detaching Sites

To detach sites to a cloud gateway, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** >**Cloud Gateways**. A table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.

Step 2 For the desired cloud gateway, click **...** and choose **Cloud Gateway**.

Step 3 Click **Attach SD-Routing**.

Step 4 Choose one or more sites from **Available Sites** and click **Detach Sites**.

The **Are you sure you want to detach sites from cloud gateway?** window appears.

Step 5 Click **OK**.

The sites attached to a cloud gateway are detached.

Step 6 To view the status of the configuration, from the Cisco SD-WAN Manager menu, choose **Configuration**> **Configuration Groups**> **Feature Profile** and click **View Details**.

Editing a Site

To edit a site, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** >**Cloud Gateways**. A table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.

Step 2 For the desired cloud gateway, click **...** and choose **Cloud Gateway**.

Step 3 Click **Edit Site Details**.

Step 4 In the Edit Site Details dialog box, enter the tunnel count.

Step 5 Enable or disable the **Accelerated VPN** field. By default, this field is **Enabled**.

Step 6 Enable or disable the **Use Select Interface as Preferred path** field. By default, this field is **Enabled**.

Step 7 Click **Submit**.

Intent Management - Connectivity

Mapping workflow in Cisco SD-WAN Manager enables connectivity between Cisco Catalyst SD-Routing VPNs (segment) and VPCs, and VPCs to VPCs. VPCs are represented based on the tags.

Note The SD-Routing branch device can have only the Default VRF. You can use this default VRF to mapping through the SD-Routing Cloud OnRamp branch connect. You cannot use any other VPN/VRF for mapping. Along with SD-Routing solution, you can have multiple VPN mapping for SD-WAN solution. Both the Cisco SD-WAN and Cisco SD-Routing connection can co-exist.

When the system records the intent for connectivity, mapping is realized in cloud in regions where cloud gateway is present. Mapping intents can be entered without cloud gateways being present in different regions. The user mapping intent is preserved and realized when a new cloud gateway or mapping change is discovered. As and when cloud gateways get instantiated 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.

In the Cloud OnRamp for Multicloud dashboard, click **Connectivity** under **Management**. The **Intent Management - Connectivity** window appears. The window displays the connectivity status with the following legends:

- Blank - Editable
- Grey color - System Defined
- Blue color - Intent Defined
- Green color - Intent Realized
- Red color - Intent Realized With Errors

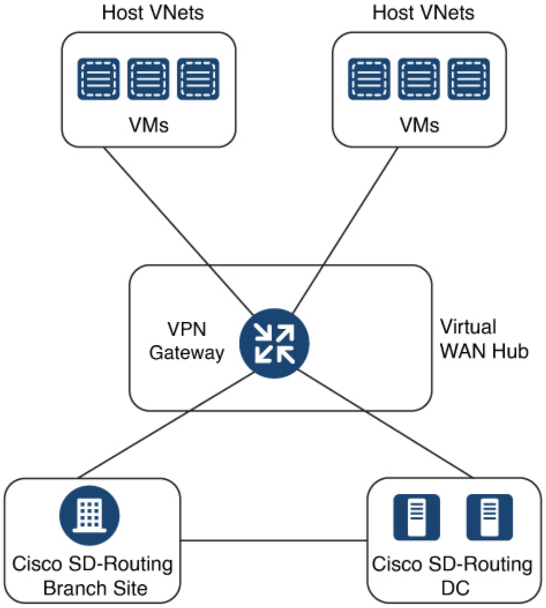
On the **Connectivity** window, you can:

- View the changes in connectivity as required.
- Filter and sort.
- Define the connectivity independent of cloud gateways in different regions.
- Realize the connectivity in regions wherever cloud gateways are present.

Azure Virtual WAN Hub Integration with Cisco SD-Routing

The integration of the Cisco Catalyst SD-Routing solution with Azure virtual WAN enhances Cloud OnRamp for Multicloud deployments and enables configuring Cisco VPN Gateway as a network virtual appliance 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-cloud connectivity through Microsoft Azure. It enables you to connect and configure SD-Routing branch devices that can communicate with Azure. Configuring VPN Gateway inside Azure virtual hubs provides higher speeds and bandwidth and overcomes the speed and bandwidth limitation of using transit VNets.



How Virtual WAN Hub Integration Works

The connection between the SD-Routing branches and a public-cloud application is provided by an Azure VPN Gateway that is configured inside the Azure Virtual WAN hub as part of Cloud OnRamp for Multicloud SD-Routing workflow for Azure.

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-Routing 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-Routing Manager enables you to map the service default-VRF 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-Routing default VRF (branch networks) and VNets, and VNets to VNets. You can enable both SD-Routing and SD-WAN connectivity mapping. When you enable the SD-WAN VPN, the SD-Routing VRF gets enabled by default. VNets are represented by tags created under the Discover workflow for Cloud OnRamp for Multicloud. 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.

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 Azure Virtual Hub VPN Gateways. It comprises Azure Resource Groups, Azure Virtual WAN, Azure VPN Gateway, 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 default VRF sites and VPN Gateways and VNets. Once a virtual hub is created, the VPN Gateway can be integrated into the Azure networking service.

Prerequisites for Azure

- Minimum supported releases: Cisco IOS XE Catalyst SD-Routing Release 17.13.1.
- 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.

Limitations for Azure SD-Routing Cloud OnRamp

- Only one VPN gateway can be created for each region. However, you can create multiple NVA based cloud gateways in a single region.
- Only one resource group is permitted on the Cisco SD-WAN Manager.
- We cannot have a combination of VPN gateway and NVA based Cloud gateways in the same region.

- Audit cannot be executed when you have only VPN gateways. Audit can be executed only when you have at least one NVA based cloud gateway.

Configure Azure Virtual WAN Hubs for SD-Routing

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

Associate your Account with Cisco SD-WAN Manager

To associate your account with Cisco SD-WAN Manager, perform these steps:

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

Step 2 Under **Setup**, click **Associate Cloud Account**.

Step 3 In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.

Step 4 Enter the requested information:

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

Step 5 Click **Add**.

Add and Manage Global Cloud Settings

To add and manage the global cloud settings, perform these steps:

Step 1 On the **Cloud OnRamp for Multicloud** window, click **Cloud Global Settings** in the Setup area.

Step 2 In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.

Step 3 To edit global settings, click **Edit**.

Step 4 To add global settings, click **Add**.

Step 5 In the **Software Image** field, choose the software image of the WAN edge device to be used in the Azure Virtual Hub.

Step 6 In the **SKU Scale** field, from the drop-down list, choose a scale based on your capacity requirements.

Step 7 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.

Step 8 In the **Autonomous System Number** field, specify the ASN to be used by the cloud gateway for eBGP peering with the virtual hub.

Step 9 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.

Step 10 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.

Step 11 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.

Step 12 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.

Step 13 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 VPN Gateways within the hub.

To create and manage the cloud gateways, perform these steps:

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

Step 2 Under **Manage**, click **Create Cloud Gateway**

Step 3 In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.

Step 4 In the **Cloud Gateway Name** field, enter the name of your cloud gateway.

Step 5 (Optional) In the **Description** field, enter a description for the cloud gateway.

Step 6 In the **Account Name** field, choose your Azure account name from the drop-down list.

Note . You can have only one Azure account.

Step 7 In the **Region** field, choose an Azure region from the drop-down list.

Note You have only one VPN gateway in a region. When you have a VPN gateway in a region, you cannot have a NVA gateway in the same region.

Step 8 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 have to delete all the existing cloud gateways. Also, you need to create a new Azure Virtual WAN and a Azure Virtual WAN hub in the next two fields.

Step 9 In the **Virtual WAN** field, choose a Azure Virtual WAN from the drop-down list. Alternatively, click **Create New** to create a new Azure Virtual WAN.

Step 10 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.

Step 11 In the **Solution Type** field, choose a Cisco vHub With VPN from the drop-down list.

Step 12 In the **SKU Scale Unit Size** field, choose SKU scale unit size from the drop-down list.

Step 13 Click **Add**. to deploy the VPN gateway.

Attaching a Site

To attach sites to a cloud gateway, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** >**Cloud Gateways**. A table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.

For each of the cloud gateways, you can view, delete, or attach more sites.

Step 2 For the desired cloud gateway, click **...** and choose **Cloud Gateway**.

Step 3 Click **Attach SD-Routing**.

Step 4 Click **Attach Sites**.

Step 5 Click **Next**. The **Attach Sites - Select Sites** window appears. The table shows the sites with the selected WAN interface.

Step 6 Choose one or more sites from **Available Sites** and move them to **Selected Sites**.

Step 7 Click **Next**.

Step 8 On the **Attach Sites - Site Configuration** window, enter the **Tunnel Count**. The tunnel count is 1 and it gives a bandwidth of 2.5 Gbps.

Step 9 For the **Use selected interface as Preferred Path** option, chose **Enabled** or **Disabled**. Multicloud workflow will configure the selected WAN interface as the default path.

Step 10 Click **Next**.

Step 11 Click **Save and Exit**. If the configuration is successful, you see a message that indicates that the branch devices are successfully attached.

Step 12 To verify the status of the device, use the **show running cofig** command.

Step 13 To view the status of the configuration, from the Cisco SD-WAN Manager menu, choose **Configuration**> **Configuration Groups**> **Feature Profile** and click **View Details**.

Detaching Sites

To detach sites to a cloud gateway, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** >**Cloud Gateways**. A table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.

Step 2 For the desired cloud gateway, click **...** and choose **Cloud Gateway**.

Step 3 Click **Attach SD-Routing**.

Step 4 Choose one or more sites from **Available Sites** and click **Detach Sites**.

The **Are you sure you want to detach sites from cloud gateway?** window appears.

Step 5 Click **OK**.

The sites attached to a cloud gateway are detached.

Step 6 To view the status of the configuration, from the Cisco SD-WAN Manager menu, choose **Configuration**> **Configuration Groups**> **Feature Profile** and click **View Details**.

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. To discover the host VNets and create tags, perform these steps:

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

Step 2 In the **Discover** workflow, click **Host Private Networks**.

Step 3 In the **Cloud Provider** field, choose **Microsoft Azure**.

Step 4 Click the **Tag Actions** drop-down list to choose any of the following:

ul

- **Add Tag:** Create a tag for a VNet or a group of VNets.
- **Edit Tag:** Change the existing tag of a selected VNet.
- **Delete Tag:** Delete the tag for the selected VNet.

Map VNets Tags and Branch Network VRF

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

Before you begin

To enable VNet to VRF mapping, you select a set of VNets in one or multiple Azure regions and define a tag. You then select the default VRF 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.

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

Step 2 Under, **Intent Management** click **Connectivity**.

Step 3 To define the intent, click **Edit**.

Step 4 Choose the cells that correspond to a VRF and the VNet tags associated with it, and click **Save**.

The **Intent Management - Connectivity** window displays the connectivity status between the branch VRF 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

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.

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

Step 2 In **Intent Management** workflow, click **Rebalance VNETS (Azure)**.

Step 3 In the **Cloud Provider** field, choose **Microsoft Azure**.

Step 4 In the **Region** field, choose an Azure region from the drop-down list.

Note For the Cisco 17.13.1a release, you can have only one VPN gateway for a region.

Step 5 In the **Tag Name** field, choose a tag from the drop-down list.

Step 6 Click **Rebalance**.

Feature Information for Cisco SD-Routing Cloud OnRamp for Multicloud

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco SD-Routing Cloud OnRamp for Multicloud

Feature Name	Releases	Feature Information
Cisco SD-Routing Cloud OnRamp for Multicloud	Cisco IOS XE Release 17.13.1a	Cisco SD-Routing Cloud OnRamp for Multicloud extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into the Cisco Catalyst SD-Routing devices. With these capabilities, the devices can access the applications hosted in the cloud.