Cloud OnRamp for Multicloud - Cloud and Interconnect

Table 1: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for Multicloud	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature provides a single common dashboard in Cisco SD-WAN Manager that displays unified information of accounts, gateways, and connections for both cloud and interconnect providers. This feature enhances the experience by helping you identify resources and monitor each provider's utilization.
Enhancements to Enable Connectivity to an Existing AWS Transit Gateway	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature enables you to discover and connect a cloud gateway to an existing AWS Transit Gateway created in the AWS portal.
Multiple Resource Groups and Subscriptions for Azure Cloud Gateways	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1	This feature enables tagging and discovery of vNets from Cisco SD-WAN Manager across subscriptions and tenants different from the one hosting the virtual WAN (vWAN). It also provides flexibility to use either the same or different resource groups for each region when creating a cloud gateway. Additionally, you can create cloud gateways or virtual hubs within the same virtual WAN, even if they reside in different subscriptions.

Cloud OnRamp for Multicloud

Cloud OnRamp for Multicloud functionalities on Cisco Catalyst SD-WAN Manager Release 20.16.1

The **Cloud OnRamp for Multicloud** page on Cisco SD-WAN Manager:

- Simplifies the experience for multicloud configurations.
- Provides step-by-step, intent-based connectivity deployments that helps you set up the connectivity.
- Provides an onboarding experience for Day 0 configurations and a dashboard experience for Day N configurations.

For a Cisco SD-WAN Manager instance on Cisco Catalyst SD-WAN Manager Release 20.16.1, from the onboarding page you can initially associate a provider account. Once you add an account, you can configure global settings and tags for an associated cloud account. Once you create a connection from the onboarding page, you are automatically switched to the dashboard view. From the dashboard page, click **Go to Onboarding** to go back to the onboarding page.

The **Cloud OnRamp for Multicloud** dashboard shows key utilization metrics for each configured provider:

- Number of accounts
- Number of gateways
- Number of cloud or interconnect connections
- Number of connected tags, applicable only to cloud providers
- If audit is enabled, last status of audit, applicable only to cloud providers

Cloud OnRamp for Multicloud functionalities from Cisco Catalyst SD-WAN Manager Release 20.18.1 and later release

Enhancements to enable connectivity to an existing AWS Transit Gateway

With this feature, you can discover and connect to an existing Transit Gateway that you are maintaining in the AWS portal for your cloud operations. This is done using cloud gateways deployed through Cloud OnRamp for Multicloud in Cisco SD-WAN Manager.

This feature is applicable only to the following solutions:

- Transit Gateway - VPN based
- Transit Gateway - Connect based

If the AWS cloud gateways are created with existing Transit Gateways, the connectivity from the Transit Gateway to the workload VPCs are managed on the AWS portal. For more information, see Configure Transit Gateway connections through AWS portal, on page 42.

You can connect the cloud gateways, comprising of the Cisco Catalyst 8000V, to the Transit Gateways from the Cloud router connectivity tab in the Cloud Connections page.

Multiple resource groups and subscriptions for Azure cloud gateways

All Azure networking resources belong to a resource group. 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.

From Cisco IOS XE Catalyst SD-WAN Release 26.1.1, Cisco SD-WAN Manager provides flexibility to use multiple resouce groups and subscriptions to create Azure cloud gateways. You can use either the same or different resource groups for each region when creating a cloud gateway.

You can also create cloud gateways or virtual hubs within the same virtual WAN, even if they reside in different subscriptions.

Additionally, you can discover and tag vNets from Cisco SD-WAN Manager across subscriptions and tenants different from the one hosting the virtual WAN.

Prerequisites for existing Transit Gateway connectivity

Transit Gateway in AWS portal

- In the AWS portal, create the Transit Gateway in the AWS region.
- Specify the desired value for AWS **Autonomous System Number** (ASN). Ensure that this value is not the same as Cisco Catalyst 8000V ASN, which is equal to the ASN value in global settings for AWS, plus an offset of 30
- Ensure that the **Default route table association** and the **Default route table propagation** options are not selected.
- Ensure that you select **Auto Accept of Shared Attachments**.

Global network in AWS portal

- In the AWS portal, choose **VPC**> **Network Manager** > **Global Networks** > **Create Global Network** to create a global network.

Register Transit Gateway in AWS portal

- In the AWS portal, register the Transit Gateway with global network.
- In the AWS portal, choose **VPC** > **Network Manager** > **Global Networks** > **Id** which you have created. Click the **Transit Gateway**. Click **Register Transit Gateway** and select the Transit Gateway created by you.

Route table in AWS portal

In the AWS portal, click **VPC** > **Transit Gateway Route Table** in the region where you created the Transit Gateway. Create the route table using this Transit Gateway. Adding tags is optional.

Workflow to Configure Cloud OnRamp for Multicloud

1. **Add Accounts**: Associate and manage provider accounts.
2. **Add Global Settings**: Configure and save default settings for provider services.
3. **Add VPCs/VNets Tags**: Discover and tag cloud workloads (VPCs and VNets).
4. **Add Gateway**: Create and manage cloud and interconnect gateways.
5. **Cloud Connections** and Interconnect Connections, on page 43: You can establish site-to-site, site-to-cloud, and cloud-to-cloud connectivity through the dashboard after bringing up the first gateway.

   Once you create a connection from the onboarding page, you are automatically switched to the dashboard view.

Manage Accounts

Add an AWS Cloud Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

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

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose provider as **AWS** or **AWS Gov Cloud** based on your requirement.
3. Enter the following parameters:

Field	Description
Account name	Enter the account name.
Description (Optional)	Enter the description.
Use for cloud gateway	Choose **Yes** if you want to create cloud gateway in your account, or choose **No**.
Login in to AWS with	Choose the authentication model you want to use: • **Key** • **IAM Role**

4. 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 Amazon Resource Name (ARN)** value that is available when creating an IAM role.

Choose **IAM Role** only if the controllers are deployed in AWS. If the controllers are managed by Cisco but deployed in AWS, use the **External ID**.

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.
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 Amazon Resource Name (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]"
       }
      }
    }
  ]
}
```

5. Click **Submit**.

To view or update the account details, click **...** on the **Manage Accounts** page.

You can also remove the account if there are no associated host VPC tags or cloud gateways.

Note During the Multicloud resource cleanup process, Cisco SD-WAN Manager compares the current database to the running resources in the account using the organisation name and account detail tags. Any resources that match the tags but are not in the current database are deleted. Therefore, the AWS Multicloud resources of Cisco SD-WAN Manager can be deleted by another Cisco SD-WAN Manager if the organization name and the associated AWS account details are the same. We recommend that if you are using the same AWS account across different Cisco SD-WAN Manager overlays, ensure that you use different organization and overlay name for each Cisco SD-WAN Manager.

Add an Azure Cloud Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

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

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Azure** or **Azure Gov Cloud** based on your requirement.
3. Enter the following information:

Field	Description
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 designate the account to be used for cloud gateway creation. The option **Yes** is chosen by default. If you choose **Yes**, providing **Subscription ID** is mandatory. **Note** The subscription ID you use during account creation determines the account ID on Cisco SD-WAN Manager. Once you establish the account ID, you cannot change it.
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**.
Use for vNet discovery in all subscriptions	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 26.1.1 If you select **Yes** Cisco SD-WAN Manager discovers all the vNet's under the specified **Tenant ID**. If you select **No** Cisco SD-WAN Manager discovers the vNet's under the subscription ID.
Subscription ID	Enter the ID of the Azure subscription you want to use as part of this workflow.

Field	Description
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.

4. Click **Submit**.

Add a Google Cloud Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

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

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Google Cloud**.
3. Enter the following information:

Field	Description
Account name	Enter a name for your Google Cloud account.
Description (optional)	Enter a description for the account.
Use for cloud gateway	Choose **Yes** to create a cloud gateway in your account. The option **Yes** is chosen by default.
Billing ID (Optional)	Enter the billing ID associated with your Google Cloud service account. If you provide a billing ID, it goes through an automatic validation process. **Note** This field is visible only if you choose the **Yes** option for the **Use for Cloud Gateway** field.
Service directory lookup	Choose **Yes** to allow Cisco SD-WAN Manager to discover services or applications in the Google Service Directory associated with the Cloud Account. The option **No** is chosen by default.

Field	Description
Private key ID	Click **Upload Credential File**. You must generate this file by logging in to Google Cloud console. The private key ID may be in JSON or REST API formats. The format depends on the method of key generation. For more details, see Google Cloud documentation. For more information, see Cisco SD-WAN Cloud onRamp for Multicloud using Google Cloud Platform.

4. Click **Submit**.

Associate a Megaport Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

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

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Megaport**.
3. Configure the following:

Field	Description
Account name	Enter a name of your choice. This name is used to identify the Megaport account in workflows that define the cloud or site-to-site interconnects.
Description (Optional)	Enter a description.
User name	Enter the username of your Megaport account.
Password	Enter the password of your Megaport account.
Customer key	(Supported releases: Cisco Catalyst SD-WAN Manager Release 20.18.1 and later) Enter the API key of your Megaport account.
Customer secret	(Supported releases: Cisco Catalyst SD-WAN Manager Release 20.18.1 and later) Enter the API secret of your Megaport account.

Note

- Use of **User name** and **Password** is deprecated from Cisco Catalyst SD-WAN Manager Release 20.18.1.
- New Megaport account association authentication is via **Customer key** and **Customer secret**.
- If you upgrade Cisco SD-WAN Manager to Cisco Catalyst SD-WAN Manager Release 20.18.1 and you already have associated Megaport accounts via **User name** and **Password**, the associations continue to work. To reauthenticate, you must use an API key and secret generated for the same account, as username and password authentication is not supported.

4. Click **Submit**.

Cisco SD-WAN Manager authenticates the account and saves the account details in a database.

Associate an Equinix Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

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

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Equinix**.
3. Configure the following:

Account name	Enter a name of your choice. This name is used to identify the Equinix account in workflows that define the cloud or site-to-site interconnects.
Description (Optional)	Enter a description.
Customer key	Enter the client ID (consumer key).
Customer secret	Enter the client secret key (consumer secret).

4. Click **Submit**.

Cisco SD-WAN Manager authenticates the account and saves the account details in a database.

Global Settings

The global settings for each provider includes mandatory fields. The **Advanced layout** option provides all the advanced settings with preconfigured values. If you do not explicitly select a value in the fields that appear when you enable **Advanced layout**, preconfigured values are chosen. The **Advanced layout** option is disabled by default.

Configure Global Settings for AWS

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

   On the onboarding page, click **Add global settings**.

2. Configure the settings based on your requirements:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices. **Note** Configuration groups is not supported on AWS Branch Connect solution.

Field	Description
Cloud gateway solution	From the drop-down list choose one of the following options: • **Transit Gateway–VPN based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach. • **Transit Gateway–Connect based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS TGW Connect (GRE tunnels) approach. • **Transit Gateway–Branch-connect**—Allows connectivity of different Cisco Catalyst SD-WAN edge 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. • **Cloud WAN–VPN based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach. • **Cloud WAN–Connect based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS Connect attachments (supporting GRE tunnels) approach.

Field	Description
Reference account name	From the drop-down list choose the reference account name. Cisco SD-WAN Manager discovers the software images and instance sizes using this reference account name. **Note** You can still choose a different account, if required, at the time of a cloud gateway creation.
Reference region	From the drop-down list choose the reference region. Cisco SD-WAN Manager discovers the software images and instance sizes in this reference region under the referenced account name.
License type	Choose **BYOL** to use a bring your own license software image
	Choose **PAYG** to use a pay as you go software image. **Note** **PAYG** is supported only on Transit Gateway - VPN based and Connect based solutions.
Software image	From the drop-down list, select a software image.
Instance size	From the drop-down list choose the required size.
IP subnet pool	Enter the subnet pool address. You cannot modify the pool when a few cloud gateways are already making use of pool.
Full mesh of transit VPCs	Specifies the full mesh connectivity between TVPCs of cloud gateways in different regions to carry site to site traffic (through Cisco Catalyst 8000V).

Field	Description
Tunnel count	This field appears if you choose **Transit Gateway–Connect based (using TVPC)** from the **Cloud Gateway Solution** drop-down list. Enter the number of tunnels for a GRE/peer connection. You can configure up to 4 tunnels for each GRE/peer connection. Each tunnel supports up to 5 Gbps of traffic. **Note** For VPN based (using TVPC) solution, with TGW or Cloud WAN, there are four IPsec tunnels between the CGW and the TGW/CNE (two per C8000v). This provides a maximum aggregate throughput of ~6 Gbps, with each tunnel supporting roughly 1.5 Gbps. **Note** Changing the value of this parameter does not affect existing cloud gateways. To update the tunnel count for an existing cloud gateway, edit the cloud gateway from the **Configuration** > **Cloud OnRamp For Multicloud** > **Cloud Gateway** page.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
BGP ASN	Specifies the offset for allocation of transit gateway BGP ASNs. It is used to block routes learnt from one transit gateway (eBGP) to another. A band of 30 ASNs are reserved for transit gateway ASNs. Starting offset plus 30 will be the organization side BGP ASN. For example, if the offset is 64830, Org BGP ASN will be 64860. Acceptable start offset range is 64520 to 65500. It must be a multiple of 10.
Intra tag communication	Specifies if the communication between host VPCs under the same tag is enabled or disabled. If any tagged VPCs are already present and cloud gateways exist in those regions, then this flag cannot be changed.
Program default route in VPCs towards TGW/Core network	Specifies if the main route table of the host VPCs is programmed with default route is enabled or disabled.

Field	Description
Enable periodic audit	If you enable the 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.
Enable auto correct	If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.

Click **Save**.

Configure Global Settings for Azure and Azure Gov Cloud

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

   On the onboarding page, click **Add global settings**.

2. Configure the global settings:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices in the multicloud workflow. **Note** When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers.
Software image	Choose the software image of the WAN edge device to be used in the Azure Virtual Hub. **Note** Choose the Cisco Catalyst 8000V image based on your Cisco SD-WAN Manager release.
SKU scale	From the drop-down list, choose a scale based on your capacity requirements.

Field	Description
IP subnet pool	Specify the IP subnet pool to be used for the Azure virtual WAN hub. A subnet pool needs prefixes between /16 and /24. 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.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
BGP ASN	Specify the ASN to be used by the cloud gateway for eBGP peering with the virtual hub.
Advertise default route to Azure Virtual Hub	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
Enable periodic audit	If you enable the 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.
Enable auto correct	If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.
Push monitoring metrics to Azure	For the 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. This option is not available for Azure Gov Cloud.

Click **Save**.

Configure Global Settings for Google Cloud

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

   On the onboarding page, click **Add global settings**.

2. Configure the global settings:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices.
Software image	Choose the software image of the WAN edge device for the WAN VPC. This should be a preinstalled Cisco Catalyst 8000V instance.
Instance size	Choose an instance based on your requirements.
IP subnet pool	Specify the IP subnet pool for the SD-WAN cloud gateway in Google Cloud. This subnet pool needs prefixes between /16 and /21. **Note** The IP subnet pool cannot be modified after a cloud gateway is created.
BGP ASN	Specify the autonomous system number (ASN) for the cloud gateway for BGP peering. This is the starting offset for the allocation of ASNs for the cloud gateways and Google Cloud routers. Starting from the offset, 10 ASN values are reserved for allocating to the cloud gateways. **Note** This offset value cannot be modified after a cloud gateway is created.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Intra tag communication	If enabled, the VPCs with the same tag can communicate with each other.
Site-to-site communication	Enable for site-to-site transit connectivity using the Google global network.
Site-to-site tunnel encapsulation type	Choose the encapsulation from the drop-down list.

Service directory lookup capable	Enable to allow Cisco SD-WAN Manager to discover Google Service Directory applications associated with this Google account.
Network service tier	Choose one of the Google Cloud service tiers. • PREMIUM: Provides high-performing network experience using Google global network. • STANDARD: Allows control over network costs.
Enable periodic audit	If you enable the 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.
Enable auto correct	If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.

Click **Save**.

Configure Global Settings for Megaport

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

   On the onboarding page, click **Add global settings**.

2. Configure the following:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices in the multicloud workflow. This option is disabled by default.
Software image	Choose a Cisco Catalyst 8000V image.
Instance size	Instance Size determines the compute footprint and throughput of each Cisco Catalyst 8000V instance. Choose one of the following: • **Small** • **Medium** • **Large**
BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
Interconnect transit color	Select the color to assign for the connection between Interconnect Gateways. This color is restricted to prevent direct peering between branch locations. Do not assign the same color to another connection in the Cisco Catalyst SD-WAN fabric. **Note** It is recommended to use private colors. Do not use default colors.
Interconnect CGW SDWAN color	Choose the color to be used for the interface through which the Interconnect Gateway connects to the Cloud Gateway. **Note** Color assigned to an interface must be unique for the Interconnect Gateway devices and common across Cloud Interconnect providers. For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the Cloud Gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, Interconnect Gateway, and Cloud Gateway.

Click **Save**.

Configure Global Settings for Equinix

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

   On the onboarding page, click **Add global settings**.

2. Configure the following:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices in the multicloud workflow. This option is disabled by default.
Software image	Choose a Cisco Catalyst 8000V image.
Instance size	Instance Size determines the compute footprint and throughput of each Cisco Catalyst 8000V instance. Choose one of the following: • **Small** • **Medium** • **Large** • **xLarge**

Field	Description
BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
Interconnect transit color	Select the color to assign for the connection between Interconnect Gateways. This color is restricted to prevent direct peering between branch locations. Do not assign the same color to another connection in the Cisco Catalyst SD-WAN fabric. **Note** It is recommended to use private colors. Do not use default colors.
Interconnect CGW SDWAN color	Choose the color to be used for the interface through which the Interconnect Gateway connects to the Cloud Gateway. **Note** Color assigned to an interface must be unique for the Interconnect Gateway devices and common across Cloud Interconnect providers. For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the Cloud Gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, Interconnect Gateway, and Cloud Gateway.

Click **Save**.

Add VPCs/VNets Tags

After you associate an account with Cisco SD-WAN Manager, you can discover host VPCs or VNets in the regions associated with the account. You can create new tags for the discovered VPCs or VNets, or modify or delete existing tags. Tags are used to manage connectivity between the VPCs or VNets and Cisco Catalyst SD-WAN branch VPNs.

Create Tags for AWS

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

   In the onboarding page, click **Add VPC/VNet tags**. Choose the provider and click **Next**.

   Alternatively, you can navigate to the **VPC/VNet tags** page from the Cloud OnRamp for Multicloud dashboard. Click **Add tag**.

2. Enter a **Tag name**.
3. Choose a **Cloud region** from the drop-down list.
4. To use the VPC tag while creating a cloud interconnect connection to a provider, **Enable for Middle-Mile partner Interconnect Connections** . If enabled, the tag can only be used for interconnect connections and is not available for cloud gateway intent mapping.
5. Select the host VPCs from the table and view the **Selected VPCs**.
6. Click **Add**.

In the **VPC/VNet Tags** page, you can toggle between tags and VPCs. A list of discovered host VPCs and tags displays in a table with the following columns: Tag Name, Cloud Region, Account Name, Associated VPCs, and Interconnect Enabled.

For the tags, click **...** under **Action** column to:

- **Edit**: Change the selected VPCs for an existing tag.
- **Delete**: Delete the tag for the selected VPC.

Create Tags for Azure and Azure Gov Cloud

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

   In the onboarding page, click **Add VPC/VNet tags**. Choose the provider and click **Next**.

   Alternatively, you can navigate to the **VPC/VNet tags** page from the Cloud OnRamp for Multicloud dashboard. Click **Add tag**.
2. Enter a **Tag name**.
3. Choose a **Cloud region** from the drop-down list.
4. To use the VNet tag while creating a cloud interconnect connection to a provider, **Enable for Middle-Mile partner Interconnect Connections** . If enabled, the tag can only be used for interconnect connections and is not available for cloud gateway intent mapping.
5. Select the VNets from the table and view the **Selected VNets**.
6. You can choose the **Cloud gateway attachment** as **Auto** or map with an existing cloud gateway. The **Auto** option is automatically selected for **Cloud gateway attachment**.
7. Click **Add**.

In the **VPC/VNet Tags** page, you can toggle between tags and VNets. A list of discovered host VNets displays in a table with the following columns: Tag Name, Cloud Gateway Attachment, Account Name, Cloud Region, Interconnect Enabled, and VNet Name.

For the tags, click **...** under **Action** column to:

- **Edit**: Change the selected VNets for an existing tag.
- **Delete**: Delete the tag for the selected VNet.

Create Tags for Google Cloud

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

   In the onboarding page, click **Add VPC/VNet tags**. Choose the provider and click **Next**.

   Alternatively, you can navigate to the **VPC/VNet tags** page from the Cloud OnRamp for Multicloud dashboard. Click **Add tag**.
2. Enter a **Tag name**.
3. Choose a **Cloud region** from the drop-down list.
4. Select the host VPCs from the table and view the **Selected VPCs**.
5. Click **Add**.

In the **VPC/VNet Tags** page, you can toggle between tags and VPCs. A list of discovered host VPCs and tags displays in a table with the following columns: Tag Name, Cloud Region, Account Name, Associated VPCs, and Interconnect Enabled.

For the tags, click **...** under **Action** column to:

- **Edit**: Change the selected VPCs for an existing tag.
- **Delete**: Delete the tag for the selected VPC.

Note You cannot create a tag with multiple regions. To add more regions to a tag, you must first create a tag with one region and then edit the tag to add a new region.

Create and Manage Gateways

Create and Manage Cloud Gateways

Create AWS Cloud Gateway

Note You cannot create multiple AWS cloud gateways in a single region.

To create a cloud gateway, perform the following steps.

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

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.
2. Select the provider:

Field	Description
Provider	Choose **AWS** from the drop-down list.
Account name	Choose the account name from the drop-down list.
Cloud gateway name	Enter the cloud gateway name.
Description(Optional)	Enter the description.
Region	Choose the region from the drop-down list.
Transit gateway	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Select one of the options: • **Create new**: Creates a new Transit Gateway and a transit VPC with a pair of virtual routers. • **Connect later/skip connection**: Creates transit VPC with a pair of virtual routers without creating a new Transit Gateway or any attachments to an existing one. You can later attach this cloud gateway to an existing Transit Gateway using SD-WAN Manager, or manually. You can either bring up attachments to the Transit Gateway through the Edit Gateway page, or through the Cloud router connectivity tab on the Cloud Connections page, once the cloud gateway is associated with an existing Transit Gateway from the Edit Gateway page. • **Use existing**: Creates a transit VPC of virtual routers. You can select an existing Transit Gateway which was created in the AWS portal. Click **Add attachments** to connect the virtual routers in the transit VPC to the Transit Gateway and associate the SD-WAN Manager VPN to the Transit Gateway route table that you have created from the AWS portal. If you choose **Connect later/skip connection** or **Use existing**, to connect the Transit Gateway with the workload VPC , see Configure Transit Gateway connections through AWS portal, on page 42.

Note If you are using an existing Transit gateway and want to create a cloud gateway using **Create new**, then perform these steps to avoid creating two separate Global Networks—one for the existing Transit Gateway and one for the new Transit Gateway:

a. Create a new cloud gateway.

b. Deregister Transit Gateway from the AWS Global Network manually created in the AWS portal.

c. Register the Transit Gateway (deregistered in step b) with the Global Network created by Cisco SD-WAN Manager.

It is recommended to disable audit if you are using the existing and new Transit Gateways together. You must also disable auto-correct option.

Click **Next**.

3. Configure the site parameters:

Field	Description
SSH key (Optional)	Choose the SSH Key from the drop-down list.
Site name	Choose a site for which you want to create the cloud gateway.
Configuration group	**Note** When you enable configuration groups, it is enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers. If you have enabled the **Enable Configuration Group** option in the AWS global settings, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • 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.

Field	Description
Chassis number	Associate a pair of chassis to the configuration group.
Instance settings	
License type	Choose a licensing option: • **BYOL** for bring your own license. • **PAYG** for pay as you go.
Software image	From the drop-down menu, choose a software image. **Note** The software image options are determined by the selection of **BYOL** or **PAYG**.
Instance size	From the drop-down list, choose the required size. Pick the size of the WAN edge based on the capacity needs.
IP subnet pool	Enter the subnet pool address. Subnet pool is used for transit VPC creation, needs between /16 to /24.System allocates /27 per transit VPC 8 subnet(s).
Tunnel count	This field appears if you choose **Transit Gateway–Connect based (using TVPC)** from the **Cloud Gateway Solution** drop-down list in the global settings for AWS. Enter the number of tunnels for a VPN connection.
This option is available only when Multi-Region Fabric is enabled. **Multi-Region Fabric Settings**	
MRF role	Choose **Border** or **Edge**.

Click **Next**.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

   Most of the parameters are auto-populated based on your eariler selections. Click the edit icon for each chassis number to modify the following:

   - **System IP**
   - **Host name**
   - **WAN region**
   - **TLOC color**

- **Username**
- **User password**

Click **Next**.

5. Verify all the configuration parameters and click **Deploy**.

Note Creating cloud gateways for AWS Cloud WAN can take over an hour depending on the resources deployed. The first deployment in a region may fail due to AWS's resource verification and validation processes in that region.

You cannot create cloud gateways in regions that do not support AWS Cloud WAN. For information about currently supported regions, see the AWS documentation.

You cannot edit a configuration group created in a multicloud workflow outside of a multicloud workflow.

Create Cloud Gateway for Azure and Azure Gov Cloud

Creation of cloud gateways involves the instantiation or discovery of Azure Virtual WAN Hub and creation of two or more 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.

To create a cloud gateway, perform the following steps.

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

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. Select the provider:

Field	Description
Provider	Choose **Azure** from the drop-down list.
Account name	Choose your Azure account name from the drop-down list.

Field	Description
Cloud gateway name	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 **Azure Virtual WAN** and **Azure Virtual WAN Hub** fields.
Description (Optional)	Enter a description for the cloud gateway.
Region	Choose an Azure region from the drop-down list.

Cisco Catalyst SD-WAN Manager Release 20.18.2 and earlier:

Field	Description
Resource group	Perform one of these actions: • Choose a resource group from the drop-down list • Choose **Create New**. For more information, see Create resource groups. **Note** If you choose to create a new resource group, you also need to create a new Azure virtual WAN and an Azure virtual WAN hub.
Azure Virtual WAN	Perform one of these actions: • Choose an Azure Virtual WAN from the drop-down list. • Click **Create New** to create a new Azure Virtual WAN.
Azure Virtual WAN Hub	Perform one of these actions: • Choose an Azure Virtual WAN Hub from the drop-down list. • Click **Create New** to create a new Azure virtual WAN hub.

From Cisco IOS XE Catalyst SD-WAN Release 26.1.1:

Field	Description
Create Azure virtual WAN hub in a different resource group	If you enable this option, you can select other subscriptions and resource groups in which you can create the Virtual hub and Network Virtual Appliance (NVA).
Azure virtual WAN hub account name	Choose an Azure account from the drop-down list. Only accounts within the same Tenant ID as the virtual WAN are displayed in the drop-down list All the gateways must be within the same tenant ID, but can span across multiple subscriptions.
Azure virtual WAN hub resource group	Perform one of these actions: • Choose a resource group from the drop-down list. The resource groups are discovered based on the account you select. • Click **Create New** to create a new resource group.

Click **Next**.

3. Configure the site parameters:

Field	Description
Solution type	Choose one of the solution type from the drop-down list: • **vHub with NVA** • **vHub with VPN** **Note** You cannot configure both the VPN and NVA solutions in the same region. Also, you cannot configure more than one VPN Gateway in the same region.

If you choose **vHub with NVA** configure the following parameters:

Field	Description
Site name	From the drop-down list, choose a site for which you want to create the interconnect gateway or click **Create New**. If you click **Create New**, configure the site settings in the slide-in pane. You can create a new site only if you have enabled configuration groups in the global settings. Configure the following and click **Save**: • **Name** • **Description** (optional) • **Site ID** (optional) • **Country** (optional) • **Address** (optional) • **City** (optional) • **State** (optional) • **Zip code** (optional)
Configuration group	If you have enabled the **Enable Configuration Group** option in the Azure global settings, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • 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.
Chassis number	Associate the number of chassis based on your requirement to the configuration group.
Instance settings	
Software image	This field is auto-populated with the configurations from the global settings. You can modify this field based on your requirements.

Field	Description
IP subnet pool	This field is auto-populated with the configurations from the global settings. You can modify this field based on your requirements.
SKU scale	This field is auto-populated with the configurations from the global settings. You can modify this field based on your requirements.
This option is available only when Multi-Region Fabric is enabled. **Multi-Region Fabric Settings**	
MRF role	Choose **Border** or **Edge**.

Click **Next** to proceed to step 3.

If you choose **vHub with VPN** configure the following parameters:

Note You can create only one gateway for VPN solution in one region.

Field	Description
SKU scale	This field is auto-populated with the configurations from the global settings when you onboard the virtual hubs with Cisco Catalyst 8000V created on Cisco SD-WAN Manager. You can modify this field based on your requirements.
IP subnet pool	This field is auto-populated with the configurations from the global settings when you onboard the virtual hubs with Cisco Catalyst 8000V created on Cisco SD-WAN Manager. You can modify this field based on your requirements.

Click **Next** to proceed to step 4.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

   Most of the parameters are auto-populated based on your eariler selections. Click the edit icon for each chassis number to modify the following:

   - **System IP**
   - **Host name**
   - **WAN region** (This option is available only when Multi-Region Fabric is enabled.)
   - **TLOC color**
   - **Username**

- **User password**

Click **Next**.

5. Review the connection summary. Click **Deploy**.

Note It can take up to 40 minutes for your Azure Virtual WAN hub to be created and for the Cisco SD-WAN Manager 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 SD-WAN devices.

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

Note You cannot edit configuration groups created by multicloud workflows outside of multicloud workflows.

Create Google Cloud Gateways

When the first cloud gateway is created, three reserved VPCs are instantiated—WAN transit VPC, site-to-site transit VPC, and site-to-cloud transit VPC. Cisco Catalyst 8000V instances that are instantiated as part of the cloud gateway are anchored to the VPCs.

Note You cannot use the same configuration group for more than one cloud gateway in Google Cloud and AWS. Use different configuration groups for each cloud gateway in Google Cloud and AWS.

To create a cloud gateway, perform the following steps:

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

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. Enter the provider details:

Field	Description
Provider	Choose **Google Cloud** from the drop-down list.
Account name	Chose your Google Cloud account name from the drop-down list.
Cloud gateway name	Enter a name for your cloud gateway. **Note** Ensure that the name is in lower case letters. See the Google Cloud documentation for information about Naming resources and Naming convention.
Region	Choose a Google region from the drop-down list.
Description (Optional)	Enter a description.
Involved in site-to-site communication	If the cloud gateway will participate in site-to-site communication, click **Yes**. If the cloud gateway will not participate in site-to-site communication, click **No**. **Note** This field is enabled for configuration only when **Site-to-site Communication** is enabled in the global settings. When **Site-to-site Communication** is disabled in the global settings, this field is dimmed.

   Click **Next**.

3. Configure the site parameters:

Field	Description
NHM region (This option is available only when Multi-Region Fabric is enabled.)	From the drop-down list, choose a network health monitoring (NHM) region for which you want to create the gateway.
Site name	From the drop-down list, choose a site for which you want to create the cloud gateway.

Field	Description
Configuration group	**Note** When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers. If you have enabled the **Enable Configuration Group** option in the Google Cloud global settings, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • 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.
Chassis number	You can associate between 2 and 8 chassis to the configuration group
Instance settings	
Software image	From the drop-down menu, choose a software image.
Instance size	From the drop-down list, choose the required size. Pick the size of the WAN edge based on the capacity needs.
IP subnet pool	Enter the subnet pool address. Subnet pool is used for transit VPC creation, needs between /16 to /24.System allocates /27 per transit VPC 8 subnet(s).
Network service tier	Choose one of the Google Cloud network service tiers from the drop-down list. • **PREMIUM**: Provides high-performing network experience using Google Cloud global network. • **STANDARD**: Allows control over network costs.

Field	Description
This option is available only when Multi-Region Fabric is enabled. **Multi-Region Fabric Settings**	
MRF role	Choose **Border** or **Edge**.

Click **Next**.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

   Most of the parameters are auto-populated based on your eariler selections. Click the edit icon for each chassis number to modify the following:

   - **System IP**
   - **Host name**
   - **WAN region** (This option is available only when Multi-Region Fabric is enabled.)
   - **TLOC color**
   - **Username**
   - **User password**

   Click **Next**.

5. Click **Deploy**.

View, edit, or delete a cloud gateway

Procedure

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

Step 2 Click **Gateway Management** on the Cloud OnRamp for Multicloud dashboard.

Existing cloud gateway details are summarized in a table.

Step 3 In the table, click **…** for the desired cloud gateway.

- To view more information about the cloud gateway, click **View**.
- To delete the cloud gateway, click **Delete** and confirm that you wish to delete the gateway.
- To edit the cloud gateway, click **Edit**. You can edit the tunnel count of the cloud gateway

  From Cisco Catalyst SD-WAN Manager Release 20.18.1, when you connect to an existing Transit Gateway, you can create VPN attachments and update the tunnel count when you edit an AWS cloud gateway.

  To disconnect the Transit Gateway connections and to connect later click **Disconnect**.

  To connect a transit VPC including a pair of virtual routers with an existing Transit Gateway, click **Use existing**. You can discover a Transit Gateway from the cloud gateway's region and attach chosen VPN(s) with Transit Gateways

routing tables. You can also add attachments in Cloud Connections page. For more information, see Cloud router connectivity.

Create and Manage Interconnect Gateways

Create a Gateway at a Megaport Location

Deploy a Cisco Catalyst 8000V instance as the interconnect gateway at the desired Megaport location. We recommend that you deploy the Cisco Catalyst 8000V instance at the Megaport location closest to your branch location.

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

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. To view the Interconnect Gateway licenses purchased through Cisco, that are associated with the account, click **Check available licenses**.

   Configure the following provider parameters:

Field	Description
Provider	Choose **Megaport**.
Account name	Choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
Interconnect gateway name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.

3. Configure the site parameters:

Field	Description
Location	Choose the Megaport PoP location where the Cisco 8000v instance must be deployed.

Field	Description
Provider license type	• **Prepaid**: Choose a prepaid license type to create the interconnect gateway. • **PayG**: Choose a pay-as-you-go (PAYG) license type to create the interconnect gateway. **Note** When using a Megaport account with Cisco billing, specify if you want to use a prepaid MVE license, or PAYG license where you are billed for each month. The selection must be done at the time of gateway creation and cannot be changed later. Appropriate prepaid or PAYG license should be purchased beforehand.
Internet bandwidth (IP transit) in Mbps	Choose the IP transit bandwidth value.
WAN region	This option is available only when Multi-Region Fabric is enabled. From the drop-down list, choose a WAN region for which you want to create the interconnect gateway.
Site name	From the drop-down list, choose a site for which you want to create the interconnect gateway or click **Create New**. If you click **Create New**, configure the site settings in the slide-in pane. You can create a new site only if you have enabled configuration groups in the global settings. Configure the following and click **Save**: • **Name** • **Description** (optional) • **Site ID** (optional) • **Country** (optional) • **Address** (optional) • **City** (optional) • **State** (optional) • **Zip code** (optional)

Field	Description
Configuration group	If you enabled the **Enable Configuration Group** in global settings for interconnect gateways, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • 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. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups. **Note** It does not include other configuration groups that are created in Cisco SD-WAN Manager. The configuration groups in this drop-down list include the options that are needed for this provider.
Chassis number	Choose the chassis number of a Cisco Catalyst 8000v instance that has the Megaport default template attached. If the configuration group is enabled, Cisco Catalyst 8000v chassis numbers do not require the Megaport template to be attached. **Note** The chassis numbers are auto-populated when you choose a site from the **Site Name** drop-down list.
Instance settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect global settings. • **Custom**: Choose a specific instance size and software image for this gateway.
MRF role	This option is available only when Multi-Region Fabric is enabled. Choose a router role: **Border** or **Edge**.
Transport gateway	This option is available only when Multi-Region Fabric is enabled. Choose **Enabled** or **Disabled**.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

The system IP address is not auto-populated for the interconnect connections. Click the edit icon for the chassis number to modify the following:

- **System IP**
- **Host name**
- **Color**
- **Username**
- **User password**

Click **Next**.

5. Click **Deploy**.

When the configuration task is successful, the interconnect gateway is listed in the **Gateway Management** page.

Create a Gateway at a Equinix Location

Deploy a Cisco Catalyst 8000V instance as the interconnect gateway at the desired Equinix location. We recommend that you deploy the Cisco Catalyst 8000V instance at the Equinix location closest to your branch location.

If a subscription for Equinix SKUs is purchased through Cisco and the account is associated to the subscription via the Equinix portal, then all network edges brought up by the Cisco SD-WAN Controller, along with the IP transit associated with those network edges, device link groups, and all virtual connections originating from those network edges, is billed by Cisco. Otherwise, these component SKUs are billed directly by Equinix.

To create an interconnect gateway, perform the following steps:

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

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. Configure the following provider parameters:

Field	Description
Provider	Choose **Equinix**.
Account name	Choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
Gateway name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.

3. Configure the site parameters.

Field	Description
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose the Equinix metro location where the Cisco 8000v instance must be deployed.
Billing Account ID	Choose the appropriate billing account for the location.
WAN region	This option is available only when Multi-Region Fabric is enabled. From the drop-down list, choose a WAN region for which you want to create the interconnect gateway.
Site name	From the drop-down list, choose a site for which you want to create the interconnect gateway or click **Create New**. If you click **Create New**, configure the site settings in the slide-in pane. You can create a new site only if you have enabled configuration groups in the global settings. Configure the following and click **Save**: • **Name** • **Description** (optional) • **Site ID** (optional) • **Country** (optional) • **Address** (optional) • **City** (optional) • **State** (optional) • **Zip code** (optional)

Field	Description
Configuration group	If you enabled the **Enable Configuration Group** in global settings for interconnect gateways, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • 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. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups. **Note** The **Configuration Group** drop-down list includes only configuration groups that you create from this drop-down list. It does not include other configuration groups that are created in Cisco SD-WAN Manager. The configuration groups in this drop-down list include the options that are needed for this provider.
Chassis number	Choose the chassis number of a Cisco Catalyst 8000v instance that has the Equinix default template attached. If the configuration group is enabled, Cisco Catalyst 8000v chassis numbers do not require the Equinix template to be attached. **Note** The chassis numbers are auto-populated when you choose a site from the **Site Name** drop-down list.
Instance settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect global settings. • **Custom**: Choose a specific instance size and software image for this gateway.
MRF role	This option is available only when Multi-Region Fabric is enabled. Choose a router role: **Border** or **Edge**.
Transport gateway	This option is available only when Multi-Region Fabric is enabled. Choose **Enabled** or **Disabled**.

4. This step is applicable only when you enable configuration groups.

Configure the device parameters:

The system IP address is not auto-populated for the interconnect connections. Click the edit icon for the chassis number to modify the following:

- **System IP**
- **Host name**
- **DNS Address (vpn_dns_primary)**
- **DNS Address (vpn_dns_secondary)**
- **Color**
- **Username**
- **User password**

Click **Next**.

5. Click **Deploy**.

When the configuration task is successful, the interconnect gateway is listed in the **Gateway Management** page.

Cloud Connections

VPC connectivity

In the Cloud OnRamp for Multicloud onboarding page, click **Add connections** and choose the provider. Alternatively, you can create connectivity by clicking **Edit** on the intent management page for the selected cloud provider from the **Cloud Connections** tab in the dashboard view.

When the system records your intent for connectivity, it maps the intent in regions where a cloud gateway is present. This means that the VPC is reachable for VPNs that have a green color status.You can enter mapping intents even if cloud gateways are not present in certain regions. The system preserves and realizes your mapping intent when it discovers a new cloud gateway or mapping change. As cloud gateways are instantiated in different regions, the system realizes the mapping intents in those regions. Similarly, tagging operations can influence the mapping in different regions, and the system realizes mappings according to the tags in the cloud.

The **Cloud Connections** page displays the connectivity status with the following legends:

- Blank - Editable
- Grey color - System Defined
- Blue color - Intent Defined

  Expressed intent between two tags or a VPN and a tag. Connectivity is not realized until a VPC in a tag and cloud gateway have regional overlap.

- Green color - Intent Realized

  All tagged VPCS/VNets have connectivity to a cloud gateway.

- Orange Color: Intent Partially Realized

A combination of blue and green. Not all regions with tagged VPCs/VNets have connectivity.

- Red color - Intent Realized With Errors

  Cisco Catalyst SD-WAN attempted connectivity but found errors.

Note Cisco Catalyst SD-WAN supports only those cloud connections that have regions where Cisco Catalyst 8000V deployed.

Cloud router connectivity

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

The cloud router connectivity tab is only available for cloud gateways that need connectivity to existing Transit Gateways.

From cloud router connectivity tab, you can manage connectivity between cloud gateways, and between Cisco Catalyst 8000V Transit VPCs and the Transit Gateway. The matrix displays the connectivity status between the VPNs and the cloud gateways (implicitly the Transit Gateways) they are attached to. Click any of the cells in the matrix displayed to get detailed information on the status.

Click **Edit** on cloud router connectivity page. Select any cell in the matrix and click **Add attachments** to update the routing table on the Transit Gateway that you want to connect to. Click **Save** on the routing table as well as the main matrix view to save the changes.

Once the Cisco Catalyst 8000V VPNs are connected to the Transit Gateway using VPN attachments over desired Transit Gateway route tables, to establish connectivity between Transit Gateway and VPC, see Configure Transit Gateway connections through AWS portal, on page 42.

Configure Transit Gateway connections through AWS portal

When you create an AWS cloud gateway, in the Transit Gateway field if you choose **Use Existing** or **Connect later/skip connection**, use this procedure to connect the cloud gateway to the Transit Gateways in the AWS portal.

Before you begin

Procedure

Step 1 Verify the VPN tunnel status.

a) From the AWS portal, click **Virtual Private Network (VPN)** > **Site-to-Site VPN connections** to navigate to the region in which the cloud gateway is created in Cisco SD-WAN Manager.

b) Select the VPN ID associated to the Transit Gateway ID and verify that the tunnel active.

Step 2 Create the Transit Gateway attachment.

a) Select the **Attachment Type** as **VPC** from the drop-down menu.

b) Select the VPC from the **VPC ID** drop-down list to attach the Transit gateway on Cisco SD-WAN Manager.

c) Click **Create the transit gateway attachment**.

Step 3 Create propagation with host VPC attachment in route table.

a) From the AWS portal, click **Virtual Private Cloud** > **Transit Gateways** > **Transit Gateway Route Table**.
b) Select the route table that was used to create the cloud gateway in Cisco SD-WAN Manager.
c) Select the propagation tab and click **Create propagation** to add the host VPC attachment.
d) Add the VPC attachment from Step 2 to the propagation. click on **Add Propagation**.
Verify the propagation is successful by checking the routes on selection of the route table.

Step 4 Create a new route table to associate the host VPC and propagate the VPN connections.

Step 5 Select the host VPC and **Add Route** by selecting routes through the Transit Gateway attachment to the main route table of the host VPC.

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.

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. In **Cloud Connections** page, choose **Azure** or **Azure Gov Cloud** and click **Rebalance VNets**
2. In the **Region** field, choose a region from the drop-down list.
3. In the **Tag Name** field, choose a tag from the drop-down list.
4. Click **Save**.

Interconnect Connections

Interconnect connections that are created in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier releases are automatically mapped into the middle-mile netwroks, multicloud networks, and the virtual networks workflows.

The connection names of the multicloud networks and virtual networks are in the following format:

AWS:

- Private connections: AWS-<Name of DxGW> ::<UUID of DGW>
- Public connections: AWS_PUBLIC_CONNECTION::<Account ID>

Azure connections: AZURE-<ERC Name>-<Auth Key>

Google Cloud:

- Private connections: GCP <Region>::<Name of Google Cloud Route>r::<Name of Attachment>

Middle-Mile Networks

This section helps you create a middle-mile fabric between Interconnect gateways or a virtual connection from an Interconnect gateway to a cloud provider's on-ramp location.

Create Middle-Mile Networks to AWS

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.

2. Configure the intent:

Field	Description
Destination	From the drop-down list, choose **Cloud-AWS**.
Connection source	Choose an interconnect gateway from the drop-down list.
Cloud gateway connection	Enable to extend the SD-WAN fabric to a cloud gateway.

   Click **Next**.

3. **Connect to AWS**:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.
Cloud access type	Choose one of the following: • **Public Services** • **Private Workloads**

   If you choose **Public Services**:

Field	Description
Cross-connect type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Hosted VIF** A virtual interface (VIF) in AWS is a connection that allows access to AWS services. • **Hosted Connection** This is the default option if **Advanced layout** option is not enabled. **Note** Equinix only supports public, private, and transit VIFs over a hosted connection. Hosted VIFs are not supported.
VPN segment	Choose the segment ID for this connection.
Cloud OnRamp location	Select the AWS on-ramp connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Select or enter AWS account	Select an AWS account or enter an AWS account ID details to establish an interconnect connection.
Account ID	Enter the AWS account ID. This option is available only if you select **Enter AWS account ID** in the **Select or enter AWS account** field.
Interconnect IP address	Enter the source BGP peering subnet public IP address for the interconnect gateway.
Amazon IP address	Enter a public IP address for AWS BGP peer.
Prefixes to be advertised to AWS	Enter prefixes to advertise to AWS.
(Optional) **Source BGP ASN**	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. Enter an ASN supported by your provider.

If you choose **Private Workloads**:

Field	Description
Cross-connect type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Hosted VIF** • **Hosted Connection** This is the default option if **Advanced layout** option is not enabled.
Virtual network association type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Direct to VPC** • **Transit Gateway** This is the default option if **Advanced layout** option is not enabled.
VPN segment	Choose the segment ID for this connection.
Cloud OnRamp location	Select the AWS on-ramp connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Select or enter AWS account	Select an AWS account or enter an AWS account ID details to establish an interconnect connection.
Account ID	Enter the AWS account ID. This option is available only if you select **Enter AWS account ID** in the **Select or enter AWS account** field.
Direct connect gateway BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and direct connect gateway in your cloud provider. Check with you provider for the supported ranges.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP Peering IP** • **Destination BGP Peering IP** • **Source BGP ASN**

Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Middle-Mile Networks** page.

Create Middle-Mile Networks to Azure

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.

2. Configure the intent:

   :

Field	Description
Destination	From the drop-down list, choose **Cloud-Azure**. **Note** Make sure to create the necessary Express Route circuit in the appropriate region before proceeding. You can create these resources using the **Multicloud Networks** page or directly in the cloud provider.
Cloud gateway connection	Enable to extend the SD-WAN fabric to a cloud gateway.
Primary connection source	Choose a primary interconnect gateway from the drop-down list.
Secondary connection source	Choose a secondary interconnect gateway from the drop-down list.

   Click **Next**.

3. **Connect to Azure**:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.

Field	Description
Cloud access type	Choose one of the following: • **Microsoft Services** • **Private Workloads**

If you choose **Microsoft Services**:

Field	Description
VPN segment	Choose the segment ID for this connection.
Select account or enter express-route circuit	Select an Azure account or enter an express route circuit key.
Azure express-route circuit	Click on the refresh button to get the latest list from cloud provider. Select the Azure Express Route circuit from the drop-down list. This option is available only if you select **Enter an express-route circuit** in the **Select account or enter express-route circuit** field.
Primary cloud OnRamp location	The primary Azure connection location field is auto-populated based on the Azure Express Route circuit selection. You cannot modify this field.
Secondary cloud OnRamp location	The selection Azure connection location field is auto-populated based on the Azure Express Route circuit selection. You cannot modify this field.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Primary connection peering IP addresses	
Interconnect IP address	Enter the public IP Address to be used as the source BGP peering subnet ID for the interconnect gateway.
Azure IP address	Enter the public IP Address to be used as the destination BGP peering for the interconnect gateway.
Secondary connection peering IP addresses	
Interconnect IP address	Enter the public IP Address to be used as the source BGP peering subnet ID for the interconnect gateway.

Field	Description
Azure IP address	Enter the public IP Address to be used as the destination BGP peering for the interconnect gateway.
Prefixes to be advertised to Azure	Enter prefixes to advertise to Azure.
Source BGP ASN This field is available only if you enable **Advanced layout** option.	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

If you choose **Private Workloads**:

Field	Description
Virtual network association type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Direct to VNets** • **Virtual WAN and vHubs** This is the default option if **Advanced layout** option is not enabled.
VPN segment	Choose the segment ID for this connection.
Select account or enter express-route circuit	Select an Azure account or enter an express route circuit key.
Azure express-route circuit	Click on the refresh button to get the latest list from cloud provider. Enter the details of Azure Express Route circuit. This option is available only if you select **Enter an express-route circuit** in the **Select account or enter express-route circuit** field.
Primary cloud OnRamp location	The primary Azure connection location field is auto-populated based on the Azure express route circuit selection. You cannot modify this field.
Secondary cloud OnRamp location	The secondary Azure connection location field is auto-populated based on the Azure express route circuit selection. You cannot modify this field.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.

Field	Description
Connection peering settings This field is available only if you enable **Advanced layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Primary connection peering IP addresses** • **Interconnect IP address** • **Azure IP address** • **Secondary connection peering IP addresses** • **Interconnect IP address** • **Azure IP address** • **Source BGP ASN**

Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Middle-Mile Networks** page.

Create Middle-Mile Networks to Google Cloud

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.

2. Configure the intent:

Field	Description
Destination	From the drop-down list, choose **Cloud-Google**. **Note** Make sure to create the necessary Google Cloud router and Interconnect attachment in the appropriate region before proceeding. You can create these resources using the **Multicloud Networks** page or directly in the cloud provider.
Cloud gateway connection	Enable to extend the SD-WAN fabric to a cloud gateway. If you enable, enter the following details: • **Primary connection source** • **Secondary connection source**
Redundancy	Choose **Enable** if you want to create connections with redundancy. Enter the following details: • **Primary connection source** • **Secondary connection source** Choose **Disable** if you want to create the connection without redundancy. Enter the following details: • **Connection Source**

Click **Next**.

3. Configure a connection to Google Cloud:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.
VPN segment	Choose the segment ID for this connection.
Select account or enter pairing key for attachment	Select an account or enter a pairing key for the attachment.

If you choose to select an account when redundancy is enabled:

Field	Description
Google region	Choose a Google Cloud connection location.
VPC network	Choose the VPC network to deploy this connection.
Primary Connection	

Field	Description
Cloud router	• Click the refresh symbol next to the **Cloud Router** drop-down list. • Choose a Google Cloud router.
Google interconnect attachment	Choose the desired interconnect attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Secondary Connection	
Cloud router	• Click the refresh symbol next to the **Cloud Router** drop-down list. • Choose a Google Cloud router.
Google interconnect attachment	Choose the desired interconnect attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you choose to select an account when redundancy is disabled:

Field	Description
Google region	Choose a Google Cloud connection location.
VPC network	Choose the VPC network to deploy this connection.
Connection	
Cloud router	• Click the refresh symbol next to the **Cloud Router** drop-down list. • Choose a Google Cloud router.

Field	Description
Google interconnect attachment	Choose the desired interconnect attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you choose to enter a pairing key for the attachment when redundancy is enabled:

Field	Description
Primary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Secondary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you choose to enter a pairing key for the attachment when redundancy is disabled:

Field	Description
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you enable cloud gateway connection to extend the SD-WAN fabric to a cloud gateway through the middle-mile networks.

Field	Description
Connection name	Enter a unique name for the connection.
Select account or enter pairing key for attachment	Select an account or enter a pairing key for the attachment.
Google Cloud Gateway	Choose the Google Cloud gateway you wish to attach to this connection.
Primary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Secondary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.

Field	Description
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

   When you save the connection configuration, a configuration task is launched and creates the interconnects between the Interconnect Gateway and the interconnect attachments of the Google Cloud routers.

   When the task is successful, the connections are listed on the **Middle-Mile Networks** page. You can also view the connection details on the Google Cloud console.

When you connect an Interconnect gateway to Google Cloud using Middle-Mile Networks, Cisco SD-WAN Manager does not automatically set up the connection. The connection is set up in Multicloud Networks.

However, since a pairing key based connection is not applicable to Multicloud Networks, you have to set up the connection manually. Perform the following steps in your Google Cloud environment:

1. Activate and set up the Autonomous System Number (ASN) for the Interconnect attachment. This number identifies your network to Google Cloud.
2. Get the Cloud Router's IP address and the peer BGP IP address. These addresses are needed for routing traffic.
3. Set up a VRF instance. This keeps the routing information of the connection separate.
4. Configure the VRF BGP settings under the Interconnect Gateway using the appropriate interface. This enables your network and Google Cloud to share routing information.

Create Interconnect Between Interconnect Gateways

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.

2. Configure the intent:

Field	Description
Destination	From the drop-down list, choose **Device Connect**.
Connection source	Select an interconnect gateway from the drop-down list.

Click **Next**.

3. Configure the device connections:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.
Connection destination	Choose a destination interconnect gateway.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source IP Address and Prefix** • **Destination IP Address and Prefix**

   Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Middle-Mile Networks** page.

Device Links

Device link groups create a full-mesh network between two or more edge devices. Device links connects all the edge devices, that are part of a group, together to create a WAN. All the device links in a mesh share the same bandwidth between the edge devices.

Note

- Only one device link is supported per Equinix account.
- Point to point connection cannot be formed between interconnect gateways belonging to a device link group.

Add Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Click **Middle-Mile Networks**.
4. Select **Device Links**.
5. Click **Add Device Link**.
6. Configure the following parameters:

Field	Description
Account name	Choose an account from the drop down menu. This is the Equinix account that has been associated to Cisco SD-WAN Manager through Account Association.
Device link name	Enter a name for the device link.
Bandwidth	Choose the bandwidth from the drop down menu. **Note** The maximum bandwidth supported by Equinix is 10000 Mbps per metro.
Subnet (Optional)	Enter the subnet. **Note** • Provide IP subnets for interconnect gateway device link interface. • The subnet should be in 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 range. • The subnet should not conflict with 172.31.251.0/21. • The subnet should not conflict with other connections. • If you do not enter the subnet, 198.19.0.0/16 is used by default.

Field	Description
Gateway name	Select the gateways from the drop down menu. Select at least two gateway names.

7. Click **Next** to preview the summary.
   - To create the device link, click **Submit**.
   - To modify the parameters, click **Back**.

Update Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Click **Middle-Mile Networks**.
4. Click **Device Links**.
5. Existing device links are summarized in a table.
6. In the table, find the desired link and click **...**.
7. To edit the device link, click **Edit**.
8. In the **Edit Device Link** page, you can only update the **Bandwidth** and **Gateway Name** to add or remove gateways.

Note Bandwidth and Gateway Name are the only two parameter that can be edited.

When adding or removing devices, at least two devices should be present in the device link.

The maximum bandwidth supported by Equinix is 10000 Mbps per metro.

9. Click **Save**.

Delete Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Click **Middle-Mile Networks**.
4. Click **Device Links**.
5. Existing device links are summarized in a table.
6. In the table, find the desired link and click **...**.
7. To delete a device link, click **Delete** and confirm that you wish to delete the device link.

Multicloud Networks

This section helps you create cloud network resources, such as Direct Connect Gateways, ExpressRoute Circuits, or Google Cloud Routers. These resources are essential for connecting middle-mile network connections to your cloud workloads (VPCs/VNets).

Ensure that both Cloud Gateways and Interconnect Gateways use the same configuration method, either templates or configuration groups.

Create Multicloud Networks to AWS

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Multicloud Networks**.

2. Configure the cloud intent:

Field	Description
Cloud type	From the drop-down list, choose **AWS**.
Cloud access type	Choose one of the following: • **Public services** • **Private workloads**

3. If you choose **Public services** make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Direct connect gateway account	Choose a direct connect gateway account from the drop-down list.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose the middle-mile network connection from the drop-down list. Only middle-mile network connections matching the direct gateway's BGP ASN are displayed in the drop-down list.

If you choose **Private workloads** make the following configurations:

Field	Description
Virtual network association type This field is available only if you enable **Advanced Layout** option.	Choose one of the following: • **Direct to VPC** • **Transit gateway** This is the default option if **Advanced layout** option is not enabled. • **Cloud gateway connection**

Field	Description
Connection name	Enter a unique name for the connection.
Direct connect gateway account	Choose a direct connect gateway account from the drop-down list.
Direct connect gateway	Click on the refresh button first. Choose a direct connect gateway from the drop-down list. Alternatively, create a new **Direct Connect Gateway** by clicking **Create New**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**. From Cisco Catalyst SD-WAN Manager Release 20.16.1, AWS Direct Connect Gateways are shared only by connections having the same virtual network association type (Direct to VPC, Transit Gateway or Cloud Gateway). When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.16.1 or later releases, ensure that the AWS Cloud Gateway connections and Private VPC connections do not share the same Direct Connect Gateway. Delete any connections that share the same Direct Connect Gateway if they are not of the same virtual network connection type.
Connectivity configuration	• **Interconnect attachments** • **Gateway Associations** This option is applicable to virtual network association type **Transit Gateway** and **Cloud gateway connection**.
If you choose **Interconnect attachments**:	

Field	Description
Middle-mile network connections	Choose the middle-mile network connection from the drop-down list. Only middle-mile network connections matching the direct gateway's BGP ASN which are of the same type as current multicloud networks connection are displayed in the drop-down list.
If you choose **Gateway Associations** and if you choose **Cloud gateway connection**:	
+ AWS region(s)	Click to add AWS regions.
AWS region	Select the AWS on-ramp connection location.
Cloud gateway	Click on the refresh button first. Choose a cloud gateway for the selected region from the drop-down list.
If you choose **Transit gateway**	
+ AWS region(s)	Click to add AWS regions.
AWS region	Select the AWS on-ramp connection location.
Transit gateway	Click on the refresh button first. Select transit gateway associated to the AWS account. Alternatively, create a new **Transit gateway** by clicking **Add New**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.
Prefixes	Enter the IPv4 prefixes for the selected gateway.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Multicloud Networks** page.

Create Multicloud Networks to Azure

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Multicloud Networks**.

2. Configure the cloud intent:

Field	Description
Cloud type	From the drop-down list, choose **Azure**.
Cloud access type	Choose one of the following: • **Microsoft services** • **Private workloads**

3. If you choose **Microsoft services** make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Express route circuit account	Choose an Azure account from the drop-down list to establish an interconnect connection.
Express route circuit	Click on the refresh button first. Choose an express route to attach an interconnect connection or click **Add New**. If you clicked **Add New**, configure the express route settings and click **Save**: • **Resource Group**: Choose a resource group associated with the Microsoft Azure account. • **Region**: Choose an Azure region. • **Instance Name**: Enter a name for the ExpressRoute instance. • **Provider**: Choose Megaport. • **Peering Location**: Choose an ExpressRoute location. • **Bandwidth**: Choose the bandwidth of the ExpressRoute circuit. • **SKU**: Choose the **Premium** or the **Standard** SKU. • **Billing Model**: Choose **Metered** billing or **Unlimited**.
Connectivity configurations	Choose **Interconnect attachments**.
Middle-mile network connections	Choose the interconnect circuits from the drop-down list. Only middle-mile network connections that are applicable are displayed in the drop-down list.

If you choose **Private workloads** make the following configurations:

Field	Description
Virtual network association type This field is available only if you enable **Advanced Layout** option.	Choose one of the following: • **Direct to VNets** • **Virtual WAN** This is the default option if **Advanced layout** option is not enabled. • **Cloud gateway connection**

Field	Description
Connection name	Enter a unique name for the connection.
Express route circuit account	Choose an Azure account from the drop-down list to establish an interconnect connection.
Express route circuit	Click on the refresh button first. Choose an express route to attach an interconnect connection or click **Add New**. If you clicked **Add New**, configure the express route settings and click **Save**: • **Resource Group**: Choose a resource group associated with the Microsoft Azure account. • **Region**: Choose an Azure region. • **Instance Name**: Enter a name for the ExpressRoute instance. • **Provider**: Choose Megaport. • **Peering Location**: Choose an ExpressRoute location. • **Bandwidth**: Choose the bandwidth of the ExpressRoute circuit. • **SKU**: Choose the **Premium** or the **Standard** SKU. • **Billing Model**: Choose **Metered** billing or **Unlimited**.
Connectivity configurations	Choose one of the following: • **Interconnect attachments** • **Gateway Associations**

Field	Description
Middle-mile network connections	Choose the interconnect circuits from the drop-down list. Only middle-mile network connections that are applicable are displayed in the drop-down list.
If you choose **Gateway Associations**:	
Azure virtual WAN This field is available only if you enable **Advanced Layout** option and choose **Virtual WAN**.	Choose or add a new virtual WAN.
+ Add virtual hub(s)	Click to add Azure virtual hubs.
Azure region	Select the Azure connection location.
Virtual hub	Click on the refresh button first. Choose a virtual hub for the selected region from the drop-down list.
These fields are available only if you enable **Advanced Layout** option and choose **Cloud gateway connection**.	
+ Add Cloud Gateways	Click to add cloud gateways.
Azure region	Select the Azure connection location.
Cloud gateway	Click on the refresh button first. Choose a cloud gateway for the selected region from the drop-down list.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Multicloud Networks** page.

Create Multicloud Networks to Google Cloud

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Multicloud Networks**.

2. Configure the cloud intent:

Field	Description
Cloud type	From the drop-down list, choose **Google Cloud**.

Field	Description
Virtual network association type	Choose one of the following: • **Shared VPC** • **Cloud gateway connections**
Redundancy	Choose **Enable** if you want to create connections with redundancy. Choose **Disable** if you want to create the connection without redundancy.

3. If you choose **Shared VPC** and **Enable** redundancy make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Google account	Choose a Google Cloud account to establish an interconnect connection from the drop-down list.
Google region	Select the Google Cloud connection location.
VPC network	Choose the VPC network to deploy this connection.
Primary Google Cloud router	Select a primary Google Cloud router or create a new one for the partner interconnect connection. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Google Cloud Router: Enter a unique Google Cloud router name.

Field	Description
Primary Google Cloud interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Secondary Google Cloud router	Select a secondary Google Cloud router or create a new one for the partner interconnect connection. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Google Cloud Router: Enter a unique Google Cloud router name.

Field	Description
Secondary Google Cloud interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose a middle-mile network connections to connect to the Google Cloud.

If you choose **Shared VPC** and **Disable** redundancy make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Google account	Choose a Google account to establish an interconnect connection from the drop-down list.
Google region	Select the Google cloud connection location.
VPC network	Choose the VPC network to deploy this connection.

Field	Description
Google cloud router	Select a Google Cloud router or create a new one for the partner interconnect connection. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Google Cloud Router: Enter a unique Google Cloud router name.
Google interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose a middle-mile network connections to connect to the Google Cloud.

If you choose **Cloud gateway connections** make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.

Field	Description
Google account	Choose a Google Cloud account to establish an interconnect connection from the drop-down list.
Google Cloud gateway	Choose the Google Cloud gateway you wish to attach to this connection.
Primary Google Cloud router	This field is auto-populated based on the selection of the Google Cloud gateway. You cannot modify this field.
Primary Google interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Secondary Google Cloud router (Optional)	This field is auto-populated based on the selection of the Google Cloud gateway. You cannot modify this field.

Field	Description
Secondary Google interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose a middle-mile network connections to connect to the Google Cloud.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Multicloud Networks** page.

Virtual Networks

This section helps you to associate multicloud network connections with your cloud workloads (VPCs/VNets).

Create Virtual Networks to AWS

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Virtual Networks**.
2. Configure cloud infrastructure connectivity:

Field	Description
Connection name	Enter a unique name for the connection.
Cloud	Select AWS as the cloud provider.
Cloud account	Select an AWS account from the drop-down list.
Virtual Network Tag Association	
Virtual network tag(s)	Choose VPC tags to identify VPCs for which traffic must be routed through this connection. See Create Tags for AWS, on page 20.
Multicloud network connection	Choose a multicloud network connection.

Click **Next**.

3. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Virtual Networks** page.

Create Virtual Networks to Microsoft Azure

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

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Virtual Networks**.

2. Configure cloud infrastructure connectivity:

Field	Description
Connection name	Enter a unique name for the connection.
Cloud	Select Azure as the cloud provider.
Cloud account	Select an Azure account from the drop-down list.
Virtual Network Tag Association	
Virtual network tag(s)	Choose VNet tags to identify VNets for which traffic must be routed through this connection. See, Create Tags for Azure and Azure Gov Cloud , on page 21.
Multicloud network connection	Choose a multicloud network connection.

Click **Next**.

3. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Virtual Networks** page.

View, Edit, or Delete Connections

View Connection Properties

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Based on your requirements, click **Middle-Mile Networks**, **Multicloud Networks**, or **Virtual Networks**.

   Existing connections are summarized in a table.
4. To view more information about a connection, click **...** for the desired connection and click **View**.

Edit Connection Configuration

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Based on your requirements, click **Middle-Mile Networks**, **Multicloud Networks**, or **Virtual Networks**.

   Existing connections are summarized in a table.
4. To modify connection configuration, click **...** for the desired connection and click **Edit**.

   Along with these editable parameters, Cisco SD-WAN Manager also displays read-only properties about the connection.

Note You can modify the properties of active connections only.

5. To apply the changes, click **Update** or **Save**.

Delete Connection

Note

- When you delete a connection to AWS, Cisco SD-WAN Manager deletes only the VIF, the virtual private gateway, and the route table that were created while establishing the connection.

  To delete cloud resources created during AWS virtual interface connection:

  1. Edit the Multicloud networks connection and delete the attachment.
  2. Delete the correspondent middle-mile networks connection to detach the cross connect.
  3. Delete the Multicloud networks connection.

- While creating a connection to AWS, if you created a direct connect gateway or a transit gateway, you can optionally delete the direct connect gateway and transit gateway.
- When you delete a connection to Azure, Cisco SD-WAN Manager deletes any ExpressRoutes, VNet gateways, ExpressRoute gateways, and virtual hubs created for the connection only if these elements are not used in other connections. Azure Virtual WAN cannot be deleted when you delete a connection.

  When you delete a GCP connection, you can optionally select to delete the Google Cloud Router, or manage these resources as required.

- Express-routes cannot be deleted until they are detached from the middle-mile cross connection. If you want to delete an express-route:

  1. Edit the multicloud metworks connection and delete both the primary and secondary attachments.
  2. Delete the correspondent middle-mile networks connection to detach the cross connect from the express-route.
  3. Delete the multicloud networks connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Based on your requirements, click **Middle-Mile Networks**, **Multicloud Networks**, or **Virtual Networks**.

   Existing connections are summarized in a table.
4. To delete a connection, click **...** for the desired connection and click **Delete**. Confirm that you wish to delete the connection.

Audit

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. In the dashboard page, click **Audit**.
3. Perform one of the following:
   - Select the public cloud provider and click **Run audit**

- or, select the interconnect providers, choose **Interconnect Connections**, **Destination type**, and **Cloud Provider**, and click **Submit**.

  When you choose Equinix you can also choose **Device links** for audit.

The window displays the status for various instances. 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 instance details available on Cisco SD-WAN Manager and the details available on the provider database.

4. If the status of an instance shows **Out of Sync**, it means that it is an error that requires manual intervention or a review and rerun of the audit to fix the error.

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

AWS audit-reported anomalies and fixes

Table 2: Examples of AWS audit discrepancies

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Transit Gateway Attachment with Resource Type as **VPC** in AWS (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details**: Mapping issue Connectivity element was missing from response: [srcType:VPC ID dstType: <C8kv-device1-UUID]> Connectivity element was missing from response: [srcType: <C8kv-device1-UUID >dstType: VPCID]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the applicable solution type.
Missing site-to-site VPN Attachment (Transit Gateway Attachment Type VPN) in AWS	Transit Gateway–VPN based (using TVPC) / Cloud WAN–VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: Mapping **Details**: Mapping issue vpnAttachSpec with tunnelId: <C8kv-device1-UUID >:<VPNID> was missing from the cloud.	Yes, audit-fix workflow - 1 is triggered.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Transit Gateway Attachment > VPC Attachment in secondary AWS account (Applicable when CGW and workload hosts are in different accounts) (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:VPC src: VPC1-Account1 dstType: VPC2 dst: VPC2] Connectivity element was missing from response: [srcType:VPC src: vpc-1 dstType: <C8kv-device1-UUID>]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the solution type.
Missing Transit Gateway Attachment with resource type as **Connect** in AWS	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC)	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:<C8kv-device1-UUID> dstType:VPC dst:VPCID] Connectivity element was missing from response: [srcType: C8kv-device2-UUID> dstType:VPC dst:VPCID]	Yes, audit-fix workflow - 2 is triggered.
Missing Host VPC (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: HOSTVPC **Details:** Host Vpc issue: <VPC ID> Hostvpc: <VPC ID> Tag mismatch- [<TAG NAME>! =] Hostvpc: <VPC ID> Couldn't find in the cloud.	Yes, audit will remove the missing VPC from tag(s) and from discovered VPC list.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing TGW	Transit Gateway–VPN based (using TVPC) / Cloud WAN VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TGW **Details:** Cloud Gateway (TGW) issue: TGW missing from the cloud. Name: <TGW Name>, region: <Region>. Please recreate the Cloud Gateway	Not fixable
Missing C8kv	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC) / Transit Gateway–VPN based (using TVPC) / Cloud WAN – VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TVPC **Details:** Cloud Gateway (TVPC) issue. Name: <CGW Name>, Id:<TVPC Id>. Please recreate the Cloud Gateway.	Not fixable
Invalid credentials	All	Could not perform audit at this time. Please retry after 10 minutes. Audit Failure.	Not fixable

Note Network connectivity disturbance is expected when the audit-fix (on-demand or periodic) is in progress, as the fix workflow deletes and recreates attachments and mappings in all the regions.

Note VPCs referred to are those discovered and tagged by Cisco SD-WAN Manager. “Missing” is defined in the context of the Cisco SD-WAN Manager’s database/knowledge.

Note Audit-fix performs the same steps in both on-demand (that is, clicking the **Fix Sync Issues** button) and periodic audit scenarios.

Note Audit-fix deletes all out-of-band attachments (VPC, TGW-peering, and Connect) to TGW or CloudWAN that users have manually created or mapped outside of CoR workflow, if any exist.

Azure audit-reported anomalies and resolutions

Table 3: 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.

GCP audit-reported anomalies and fixes

Table 4: Examples of GCP audit discrepancies

Anomaly / Trigger	Audit Findings / Error Message
Missing Network Connectivity Center (NCC) spokes	**Report Type**: NCC_HUB **Details**: Spoke <spoke-name> in region <region-id> is missing.
Missing NCC Hubs	**Report Type:** NCC_HUB **Details:** NCC Hub: <Hub Name> not found.
Missing Google cloud routers (GCRs) - primary, secondary, or both	**Report Type:** GCR **Details**: <GCR Name> not found.
Missing site-to-cloud peering of VPCs mapped to VPNs in Cisco SD-WAN Manager	**Report Type**: MAPPING **Details**: Connectivity element was missing from response: [srcType:V dstType:VPC dst:<dst-vpc-id>]
Missing VPC peering of VPCs that are mapped to other VPCs in Cisco SD-WAN Manager	**Report Type:** MAPPING **Details:** Connectivity element was missing from response: [srcType: dstType:VPC dst:<dst-vpc-id>]
Missing custom routes	**Report Type:** Mapping **Details:** Connectivity element was missing from response: [srcType: src:<C8Kv-Device-UUID>::<vpn-id> dstType:VPC dst:<vpc-id>]
Missing Border Gateway protocol (BGP) sessions	**Report Type**: MAPPING **Details**: BGP session is missing in GCR
Stale BGP sessions	**Report Type**: MAPPING **Details**: Stale prefixes found in BGP Sessions
Removal of a cloud gateway or any of its components	**Report Type:** CGW_ROUTER **Details:** CGW Router: [<CGW Instance name> <region-id>] Couldr cloud (Irrecoverable error, user intervention needed to fix things in cl

Anomaly / Trigger	Audit Findings / Error Message
Issues with host VPCs with overlapping CIDRs	**Mapping Failure**: Additional details: Overlapping subnets part of mappi Mapping: VPN:<vpn id> --> <s2c vpc name, vpc-id, vpc-subnet> / <vpc na **Report Type**: Mapping **Details**: vpnAttachSpec with tunnelId: <c8kv uuid>::<vpn id> was miss
Issues with site-to-site VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2S_VPC] not found in cloud (Irrecoverabl needed to fix things in cloud).
Issues with site-to-cloud VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2C_VPC] not found in cloud (Irrecoverabl needed to fix things in cloud).
Issues with WAN VPCs	**Report Type:** TVPC **Details:**TVPC: [<s2c-vpc-id> WAN_VPC] not found in cloud (Irrecoverab needed to fix things in cloud).
Invalid GCP Credentials	**Report Type:** Account **Details:** Invalid GCP Credentials found for account Id <acc-id>

Note Audit-fix performs the same steps in both on-demand fix (that is, clicking the **Fix Sync Issues** button) and periodic audit followed by auto-correct.