Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy a Cisco Cloud Services Router 1000v (Cisco CSR 1000v) instance as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway. From the Interconnect Gateway, you can create software-defined interconnects to an AWS Cloud OnRamp or another interconnect gateway in the Equinix fabric.
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix: Google Cloud and Microsoft Azure	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can create software-defined interconnects to Google Cloud VPCs, or Microsoft Azure VNets or Virtual WANs to link your branch location to the cloud resources through the Equinix fabric. You can also create, update and delete device links from Interconnect Gateway in the Equinix fabric.

Feature Name	Release Information	Description
Encrypted Multicloud Interconnects with Equinix	Cisco vManage Release 20.9.1	You can extend the Cisco Catalyst SD-WAN fabric from the Interconnect gateway in Equinix into the AWS, Google Cloud and Microsoft Azure Cloud Service Providers. You can provision a secure private Cisco Catalyst SD-WAN connection between an Interconnect Gateway and Cloud Service Providers through the Cloud OnRamp workflows in Cisco SD-WAN Manager.
Support for Cisco Catalyst 8000V Edge Software	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can deploy a Cisco Catalyst 8000v Edge Software as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway.
Addition of VPC and VNet Tags to SDCI Connections	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can modify VPC and VNet Tags and some other properties that are associated with an SDCI connection
Management of Audit in Equinix	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	The audit management helps in understanding if the interconnect cloud and provider states are in sync with the Cisco Catalyst SD-WAN Manager state. The audit process involves scanning the provider resources, interconnect gateways, and connections to the cloud. For more information, see Audit Management.

Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.

   After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* documentation in the Equinix Developer Platform Knowledge Center.

   Create billing accounts for each region in which you would like to deploy an Interconnect Gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.

2. For a connection that requires a public peering between an Interconnect Gateway and a Cloud provider, specify a public BGP peering IP address. Ensure that your organization is permitted to use the public IP address before you create the connection. Alternatively, you can allocate the public IP address for BGP peering from the Equinix portal.

3. Ensure you have UUIDs for the required number of Cisco CSR 1000v instances that you wish to deploy as Interconnect Gateways.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy Cisco Catalyst 8000v instance.

4. Ensure that Cisco SD-WAN Manager can connect to the Internet.

   As part of the configuration workflows, Cisco SD-WAN Manager connects to the Equinix portal via the Internet.

5. The Cisco SD-WAN Manager certificate must be signed by Cisco (Automated) PKI or Symantec as the root CA for Cisco SD-WAN Manager to be able interact with Equinix. We recommend using a Cisco (Automated) PKI certificate. Enterprise CA certificate is supported starting Cisco vManage Release 20.9.1.

Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

General

- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can create and edit the connections.

  Prior to Cisco Catalyst SD-WAN Manager Release 20.12.1, you cannot edit the connections. You can delete the connection and create a new connection with the desired settings.

- Interconnect gateways in the same location cannot be created or deleted at the same time.

- All interconnect and cloud operations are time bound. If an operation times out, Cisco SD-WAN Manager reports a failure. Currently, the time out values are not configurable.
- If you modify the global settings, the changes are applied to any new gateways or connections created after the modification. The changes do not affect gateways or connections created before the modification.
- If you have deployed Equinix Interconnect Gateway in Cisco IOS XE Catalyst SD-WAN Release 17.3.3 through Cisco SD-WAN Manager prior to Cisco Catalyst SD-WAN Manager Release 20.12.1, you must upgrade the Equinix Interconnect Gateway to Cisco IOS XE Catalyst SD-WAN Release 17.9.x before you upgrade Cisco SD-WAN Manager to Cisco Catalyst SD-WAN Manager Release 20.12.1.
- After you create an interconnect gateway at an Equinix location using Cisco vManage Release 20.6.1, if you upgrade Cisco SD-WAN Manager software to a later release, port 443 on the interconnect gateway is disabled. To overcome this limitation, do one of the following:
  - Enable port 443 manually.
  - Delete the existing interconnect gateway and create a new interconnect gateway after the Cisco SD-WAN Manager software upgrade.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.2, any transit gateway created as part of the multicloud workflow is not listed under the transit connections of SDCI workflow.
- Starting from Cisco vManage Release 20.9.5, you can deploy Cisco Catalyst 8000v Edge Software as the Interconnect Gateway in the Equinix fabric.

Interconnects to AWS

- While creating a connection to an AWS cloud resource, be mindful of the AWS quotas and limitations. Cisco SD-WAN Manager does not enforce all the AWS quotas and limitations.
- You cannot use cloud resources belonging to different AWS accounts as part of a single connection.
- Equinix only supports public, private, and transit VIFs over a hosted connection. Hosted VIFs are not supported.
- Attach either private VIFs or transit VIFs to a Direct Connect gateway. You cannot attach a combination of private VIFs and transit VIFs to the same Direct Connect gateway.
- From Cisco vManage Release 20.9.2 and Cisco vManage Release 20.10.1, for a transit-hosted connection, in an AWS region, you can associate only one transit gateway with a Direct Connect gateway.

  We recommend that you associate only one transit gateway with a direct connect gateway in an AWS region with Cisco vManage Release 20.9.1 and earlier releases.
- When editing interconnect transit connection, if a new transit gateway is selected without a VPC tag in the same region, connection update is discarded.
- All connections to a particular VPC must
  - peer with the same direct connect gateway
  - have the same transit gateway or virtual private gateway attachment
- For a transit VIF, the transit gateway and direct connect gateway must use different BGP ASNs.

- While creating host VPC tags, choose to use the tag with either the AWS Multi Cloud workflow or the interconnect connectivity workflow. This choice cannot be altered after the tag is created and persists till the deletion of the tag.
- A host VPC tag selected for interconnect connectivity cannot be edited after creation.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can create and edit the host VPC tag.

Interconnects to Microsoft Azure

- While creating host VNet tags, choose to use the tag with either the Microsoft Azure Multicloud workflow or the interconnect connectivity workflow. This choice cannot be altered after the tag is created and persists till the deletion of the tag.
- A host VNet tag selected for interconnect connectivity cannot be edited after creation.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can create and edit the host VNet tags.
- While creating a private-peering connection to a Microsoft Azure ExpressRoute from an interconnect gateway, you can attach to the connection only the VNets, virtual WANs, and virtual hubs that belong to the same resource group as the ExpressRoute circuit. Attaching VNets, virtual WANs, and virtual hubs from a different resource group is not a supported configuration.

Interconnects to Google Cloud

- Each Cloud Router must use the same ASN for all its BGP sessions.

Device Links

- The fixed Bandwidth for all links in a device group can range from 50 Mbps to 10 Gbps.
- The cumulative bandwidth of all links at a given metro should not be greater than 10 Gbps.

Restrictions for Encrypted Multicloud Interconnects

Minimum supported release: Cisco vManage Release 20.9.1

Interconnects to AWS

- As per AWS requirement,
  - The minimum instance type must be x-large for Cloud Gateways.
  - A maximum of 10 Cloud Gateways can be attached to a single interconnect connection.
  - One Cloud Gateway can be connected to 30 interconnect connections.

Interconnects to Microsoft Azure

- A single Cloud Gateway can be attached to 8 different cloud interconnect connections and one interconnect connection can connect to 5 different Cloud Gateways.

- To connect to Cloud Gateways in different regions, the express route circuit must be of Premium type.
- 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.

Interconnects to Google Cloud

- Cloud Interconnect connection to Google Cloud Gateway is supported only with redundancy enabled.
- Only one Google Cloud Gateway can be attached to a single connection.
- Existing Google Cloud Gateways are not supported for cloud interconnects.
- A maximum of 5 Google Cloud Routers can be created for a combination of region and network.

Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

Table 2: Connection Configuration Limits

Description	Count
Interconnect Gateway	
Maximum number of connections (VXC) per Interconnect Gateway	20 **Note**: Aggregate VXC bandwidth should not exceed the bandwidth capacity of the Interconnect Gateway.
Interconnects to AWS	
Maximum number of VPCs per connection to AWS for a private VIF	10
Number of VPCs per connection to AWS for a transit VIF	Default: 15 Maximum: 15000
Maximum number of transit gateways per connection to AWS for a transit VIF	3
Maximum number of Direct Connect gateways per connection	1
Maximum number of VIFs (private or transit) per AWS Direct Connect gateway	Default: 30 Limit can be increased on request.
Maximum number private, public, or transit VIFs per AWS Direct Connect hosted connection	1
Maximum number of prefixes from branch location to AWS for a transit VIF	100

Description	Count
Maximum number of prefixes per AWS transit gateway from AWS to a branch location for a transit VIF	20
Interconnects to Microsoft Azure	
Maximum number of Interconnect Gateways that can connect to an ExpressRoute	2
Maximum number of VNets to which an ExpressRoute can connect	10
Maximum number of ExpressRoutes that can connect to a VNet	4
Maximum number of ExpressRoutes that can connect to a virtual hub	8 per peering location
Maximum aggregate throughput per virtual WAN ExpressRoute gateway	20 Gbps
Maximum number of VNets that can connect to a virtual hub	500 - (total number of virtual hubs in the virtual WAN)

Interconnects to AWS

- When you delete a private VIF connection to AWS, Cisco SD-WAN Manager deletes the VIF, the virtual private gateway, and the route table that were created while establishing the connection.
- When you delete a transit VIF connection, Cisco SD-WAN Manager removes any attachments and associations to a Direct Connect gateway, transit gateway, or virtual private gateway that were created while establishing the connection.
- While creating a connection to AWS, if you created a direct connect gateway or transit gateway from Cisco SD-WAN Manager, deleting the connection does not delete the gateway. You need to manage these AWS resources as required.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you have the option to delete the Direct Connect Gateway or Transit Gateway while deleting the connection.
- When you create a connection, a new route table is created and set as the Main route table for the host VPCs attached to the connection. A default route is created in the Main route table to the transit gateway and route propagation is enabled. Edit the routes and propagation as required.

  From Cisco vManage Release 20.5.1, the static routes and subnet associations required to be accessed by the interconnect should be moved to the newly created main route table by Cisco SD-WAN Manager.

Interconnects to Google Cloud

- For nonredundant connectivity, you must deploy a Google Cloud Router in each network-region and create a VLAN attachment for each Google Cloud Router.

- For redundant connectivity, you must deploy two Google Cloud Routers in each network-region and create a VLAN attachment for each Google Cloud Router.
- For use with interconnect attachments, you must set the Google ASN for the Google Cloud Routers to 16550.

Interconnects to Microsoft Azure

- Only one pair of Interconnect Gateways can connect to a particular ExpressRoute to provide a HA connection to the VNet attched to the ExpressRoute.

  To connect a second pair of Interconnect Gateways to the same vNet, do as follows: create another ExpressRoute; attach the vNet to the ExpressRoute; and connect the Interconnect Gateways to the ExpressRoute

  You can have a maximum four such ExpressRoutes connecting to a VNet, and connect each Express Route to a pair of Interconnect Gateways.
- An ExpressRoute can connect to maximum of 10 VNets. You can attach VNets to an ExpressRoute while creating connections to the ExpressRoute from Interconnect Gateways. VNets are attached based on the VNet tags you choose for the connection.

  If you choose a VNet tag that applies to more than 10 VNets or choose a combination of VNet tags so that the total number of select VNets is more than 10, interconnect creation fails.

Note Any VNets that you may have attached to the ExpressRoute from the Azure portal are also considered while determining the number VNets that you can attach to the ExpressRoute while creating the connection from the interconnect gateways.

- You can connect a VNet to either a VNet gateway or an ExpressRoute gateway. So, if you have created a private peering to a VNet through a VNet gateway, you cannot create a private peering to the same VNet through an ExpressRoute gateway, and vice-versa.
- If a VNet is connected to virtual hub in a virtual WAN, the same VNet cannot be connected to another virtual WAN.
- All the VNets in a region must connect to a single virtual hub in the same region.
- Redundant connectivity is the default and only supported configuration. You must create connections to Microsoft Azure from a pair of Interconnect Gateways in the Equinix fabric.

  When choosing a pair of Interconnect Gateways from which you wish to create the primary and secondary connections to a Microsoft Azure ExpressRoute, ensure that the Interconnect Gateways are configured to use the same BGP ASN for BGP peering.

Information About Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

From Cisco SD-WAN Manager, you can deploy a Cisco Cloud Services Router 1000v (Cisco CSR 1000v) instance in the fabric of the SDCI provider Equinix and add the instance as a WAN edge device in the Cisco

SD-WAN fabric. As a WAN edge device, the Cisco CSR 1000v instance links a branch location to the Equinix fabric. In the Equinix fabric, the Cisco CSR 1000v instance acts as an interconnect gateway. From the interconnect gateway, you can create a direct Layer 2 connection (an interconnect) in the Equinix fabric to a Cloud OnRamp or another interconnect gateway. The interconnects link branch locations, or link branch locations to cloud service providers through the interconnect gateways in the Equinix fabric.

In this setup, the Cisco SD-WAN fabric acts as the overlay network, and the Equinix fabric acts as the underlay network. The Equinix fabric provides efficient, high-speed, low-latency, high-bandwidth connectivity to cloud resources in multiple global locations. We recommend that you deploy the Cisco CSR 1000v instance at an Equinix location closest to your branch location.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy Cisco Catalyst 8000v instance.

You can create the following types of connections from an interconnect gateway:

Table 3: Connection Types

Destination	Connection Types	Supported Software Releases
Amazon Web Services	• Direct-connect-private-hosted connection to AWS direct-connect-gateway from interconnect gateway • Direct-connect-public-hosted connection to AWS from interconnect gateway • Direct-connect-transit-hosted connection to AWS direct connect gateway from interconnect gateway	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Catalyst SD-WAN Release 17.3.3
Microsoft Azure	• Partner ExpressRoute Circuit - Microsoft Peering • Partner ExpressRoute Circuit - Private Peering	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Catalyst SD-WAN Release 17.3.3
Google Cloud	Partner Interconnect Attachment to a Google Cloud Router	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Release 17.3.3

Destination	Connection Types	Supported Software Releases
Interconnect Gateway	Link between Cisco Catalyst SD-WAN branch locations connected to the interconnect gateways	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Catalyst SD-WAN Release 17.3.3.

Cisco Catalyst SD-WAN Manager serves as a unified management portal and enables you to perform the following tasks:

- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, configure Cisco Catalyst 8000v instance.

  Configure and deploy the Cisco CSR 1000v instance at an Equinix location for prior to Cisco Catalyst SD-WAN Manager Release 20.12.1.

- Create cloud interconnects to public cloud resources.
- Create interconnects to link Cisco Catalyst SD-WAN branch locations through the Equinix fabric.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy a Cisco Catalyst 8000v instance as the interconnect gateway in the Equinix fabric and connect anCisco Catalyst SD-WAN branch location to the interconnect gateway. Existing Cisco CSR1000V deployments can be used to create connections.

Points to Consider

If you are upgrading from an earlier Cisco Catalyst SD-WAN Manager version to Cisco Catalyst SD-WAN Manager Release 20.12.1, to enable Cisco Catalyst 8000v:

- Re-authenticate the existing Equinix account through **Edit Account Credentials** and provide the customer key and the customer secret. You can use the same key and the secret that you used for previous versions. It internally updates the billing accounts and locations available for Cisco Catalyst 8000v. For information on editing account details, see View, Edit, or Delete an Interconnect Account.
- After the account is re-authenticated, you must update the **Global Settings** for interconnect gateways to select the Cisco Catalyst 8000v software version and other parameters for new gateways. For information on updating global settings, see Configure Global Settings for Equinix Interconnect Gateways.
- If you have deployed Equinix interconnect gateway using Cisco IOS XE Catalyst SD-WAN Release 17.3.3 via Cisco SD-WAN Manager prior to Cisco Catalyst SD-WAN Manager Release 20.12.1, the Equinix interconnect gateway must be upgraded from Cisco IOS XE Catalyst SD-WAN Release 17.3.3 to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or Cisco IOS XE Catalyst SD-WAN Release 17.9.1a before upgrading to Cisco Catalyst SD-WAN Manager Release 20.12.1.

Benefits of Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

1. Branch locations connect seamlessly to the Equinix fabric over the Cisco Catalyst SD-WAN fabric.
2. Interconnects to public cloud with assured SLAs.
3. End-to-end traffic security, segmentation, and policy through the Cisco Catalyst SD-WAN fabric.
4. Cisco SD-WAN Manager provides a single pane to manage your connectivity to any cloud.
5. End-to-end visibility across the Cisco Catalyst SD-WAN and Equinix fabric.
6. Links between Cisco Catalyst SD-WAN branch locations and between Cisco Catalyst SD-WAN branch locations and a public cloud.

Encrypted Multicloud Interconnects

Minimum supported release: Cisco vManage Release 20.9.1

You can provision a secure private Cisco Catalyst SD-WAN connection between an Interconnect Gateway and Cloud Service Providers through the Cloud OnRamp workflows in Cisco SD-WAN Manager. You can terminate the virtual cross connects from the Interconnect Gateway in the cloud interconnect provider to the existing Cloud Gateways which are created as part of the Multicloud workflow. For more information, see Cloud OnRamp for Multicloud. This feature enables support for both internet and private paths to access VPC and VNET workloads.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, encrypted multicloud interconnects supports AWS Cloud Gateway using Cloud WAN solution.

Benefits

- Provides end to end encryption from branch sites to Cloud Gateways through the cloud interconnect provider backbone.
- Supports multiple VPN segments over single virtual cross connect.
- Supports modification of VPC and VNET tags before and after the connection creation. VPN to VPC or VNET tag mapping can be performed using the Multicloud Intent Management screen.
- Route advertisements are controlled by Interconnect Gateways and Cloud Gateways to overcome prefix advertisements restrictions imposed by cloud service providers.

Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

Prerequisite Configuration

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.

After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* documentation in the Equinix Developer Platform Knowledge Center.

Also, create billing accounts for each region in which you would like to deploy an interconnect gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.

2. Associate Equinix account with Cisco SD-WAN Manager.
3. Configure global settings for interconnect gateways.
4. Create necessary network segments (see Segmentation Configuration Guide).
5. Ensure you have UUIDs for the required number of Cisco CSR 1000v instances that you wish to deploy as Interconnect Gateways.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, deploy Cisco Catalyst 8000v instance.
6. Attach Equinix Template to a Cisco CSR 1000v instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can attach Cisco Catalyst 8000v instance.
7. Create interconnect gateway at Equinix location closest to your Cisco Catalyst SD-WAN branch location.

   For connectivity to Cloud Providers, create an interconnect gateway at the Equinix location.

   For connectivity between Cisco Catalyst SD-WAN branch locations, for each branch location, create an interconnect gateway at the closest Equinix location.

Workflow to Create Interconnect to AWS

Before you perform the following configuration procedures, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Associate AWS account with Cisco SD-WAN Manager.
2. Discover Host Private Networks to connect to AWS Virtual Private Clouds (VPCs).
3. Create one of the following types of connection:

Connection Type	Tip
Direct Connect - Public Hosted Connection	Use this connection for a link to a public AWS resource, with the link having a fixed bandwidth up to 10 Gbps.
Direct Connect - Private Hosted Connection	Use this connection for a dedicated link to AWS VPCs, with a link bandwidth up to 10 Gbps.
Direct Connect - Transit Hosted Connection	Use this connection for dedicated links up to 5,000 AWS VPCs via a transit gateway, with a link bandwidth up to 10 Gbps. You can attach up to three transit gateways to a direct connect gateway and connect to up to 15,000 VPCs.

Workflow to Link Cisco Catalyst SD-WAN Branch Locations

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

- Create an Interconnect between the interconnect gateways.

Workflow to Create Interconnect to Google Cloud

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Create the required VPC network using the Google Cloud portal.
2. Deploy Google Cloud Routers in network-regions to which you wish to connect.

   For nonredundant connectivity, using the Google Cloud portal, deploy a Google Cloud Router in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

   For redundant connectivity, using the Google Cloud portal, deploy two Google Cloud Routers in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

   Starting from Cisco vManage Release 20.9.1, you can deploy Google Cloud Routers and VLAN attachments via Cisco SD-WAN Manager interconnect workflow.
3. Associate Google Cloud account with Cisco SD-WAN Manager.
4. Create Interconnects to Google Cloud Routers from interconnect gateways.

Workflow to Create Interconnect to Microsoft Azure

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Associate Microsoft Azure account with Cisco SD-WAN Manager.
2. Discover Host Private Networks to connect to Azure Virtual Networks (VNets).
3. Create one of the following types of connection:
   - Public Peering Connection to an Azure ExpressRoute
   - Private Peering Connection to an Azure ExpressRoute

Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Equinix

Associate Equinix Account with Cisco SD-WAN Manager

Prerequisites

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.

2. After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* information in the Equinix Developer Platform Knowledge Center.
3. Create billing accounts for each region in which you would like to deploy an Interconnect Gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Associate Interconnect Account**.
4. Configure the following:

Interconnect Provider	Choose **EQUINIX**.
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).

5. Click **Add**.

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

Configure Global Settings for Equinix Interconnect Gateways

Prerequisites

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.
2. After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* information in the Equinix Developer Platform Knowledge Center.
3. Create billing accounts for each region in which you would like to deploy an Interconnect Gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.
4. Associate Equinix account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Global Settings**.

- To add global settings, click **Add**.
- To modify global settings, click **Edit**.

4. Configure the following:

Enable Configuration Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, enable this option to use configuration groups to configure devices in the multicloud workflow. This option is disabled by default. **Note** When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables it for all other multicloud and interconnect providers.
Interconnect Provider	Choose **EQUINIX**.
Software Image	Choose a Cisco CSR 1000v image. For Cisco Catalyst SD-WAN Manager Release 20.12.1, choose a Cisco Catalyst 8000v image.
Instance Size	Instance size determines the compute footprint and throughput of each Cisco CSR 1000v instance. Choose one of the following: • **Small**: 2vCPU, 4 GB DRAM, up to 1 Gbps • **Medium**: 4vCPU, 4 GB DRAM, up to 2.5 Gbps • **Large**: 6vCPU, 4 GB DRAM, up to 2.5 Gbps For Cisco Catalyst SD-WAN Manager Release 20.12.1, the instance sizes are: • **Small**: 2vCPU, 8 GB DRAM, up to 1 Gbps • **Medium**: 4vCPU, 8 GB DRAM, up to 2.5 Gbps • **Large**: 6vCPU, 16 GB DRAM, up to 2.5 Gbps • **xLarge**: 8vCPU, 16 GB DRAM, up to 2.5 Gbps
Interconnect Transit Color	Choose the color to be assigned for 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.
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.

Interconnect CGW SDWAN Color	Minimum supported release: Cisco vManage Release 20.9.1 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.

5. To save the newly added global settings, click **Save**.

   To save the modified global settings, click **Update**.

Attach Equinix Template to Cisco CSR 1000v or Cisco Catalyst 8000v Instance

Note This procedure is not required if you enabled configuration groups. In this case, skip to Create Interconnect Gateway at an Equinix Location.

Before you can deploy a Cisco CSR 1000v instance as an interconnect gateway at an Equinix location, you must attach the Equinix default template to the device. We recommend that you attach the template named *Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02.*

For Cisco Catalyst SD-WAN Manager Release 20.12.1, the default template for Cisco Catalyst 8000v is *Default_EQUINIX_ICGW_C8000V_Template_V01*.

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

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

3. Choose the **Template Type** as **Default** and find the template named *Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02.*

   For Cisco Catalyst SD-WAN Manager Release 20.12.1, choose the default *Default_EQUINIX_ICGW_C8000V_Template_V01*.
4. Click **…** and click **Attach Devices**.
5. Choose the UUID of desired Cisco CSR 1000v instance from the list of **Available Devices** and move the instance to the list of **Selected Devices**.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v instance.
6. Click **Attach**.

7. The template contains variables. To enter values for the variables in the template, click **…** and click **Edit Device Template**.
8. Enter the values for the following variables and click **Update**:
   - DNS Address (vpn_dns_primary)
   - DNS Address (vpn_dns_secondary)
   - Color (vpn_if_tunnel_color_value)
   - System IP (system-ip)
   - Site ID (site-id)
   - Hostname (host-name)
9. Click **Next**.
10. Click **Configure Devices**.

Create Interconnect Gateway at an Equinix Location

Deploy a Cisco CSR 1000v instance as the interconnect gateway at the desired Equinix location. We recommend that you deploy the Cisco CSR 1000v instance at an Equinix location closest to your branch location.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy a Cisco Catalyst 8000v instance.

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. If you did not enable configuration groups, attach the Equinix template to the Cisco CSR 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach the template to the Cisco Catalyst 8000v instance.
4. If you enabled configuration groups, ensure that you configure device parameters for devices that are associated with the configuration group.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Create Interconnect Gateway**.
4. Configure the following:

Interconnect Provider	Choose **EQUINIX**.
Gateway Name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.

Account Name	Choose an Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose the Equinix location where the Cisco CSR 1000v instance must be deployed. Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v instance.
Billing Account ID	Choose the appropriate billing account for the location.
Site Name	Choose the site. Starting Cisco vManage Release 20.10.1, Site Name field is available.
Configuration Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for interconnect gateways, perform one of these actions: • Choose a configuration group. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow. 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 have been created in Cisco Catalyst SD-WAN. The configuration groups in this drop-down list include the options that are needed for this provider. • If you create the Equinix Interconnect Gateway by using a configuration group, using SSH from Cisco SD-WAN Manager works only when the interconnect gateway is Cisco Catalyst 8000v 17.13 or later.
UUID	Choose the UUID of a Cisco CSR 1000v instance that has the Equinix default template attached. **Note** When a site name is selected, UUID field is auto-populated with the UUID associated with the site name. Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v 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.

5. Click **Add**.

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

Note Before proceeding further, verify that the **Device Status** column for the interconnect gateway shows **In Sync** and the certificate is successfully installed.

Create Interconnect to AWS

Associate AWS Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud**.
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Amazon Web Services**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.
Log in to AWS with	Choose **Key** or **IAM Role**.
Role ARN	Enter the API/Secret Key or the Role ARN.

5. Click **Add**.

Cisco SD-WAN Manager uses the API/Secret Key or the Role ARN to authenticate the user account with AWS as part of the API workflow to create connections to AWS.

Discover Host Private Networks and Tag AWS VPCs

A number of host VPCs can be grouped together using a tag. VPCs under the same tag are considered as a singular unit. Tag the AWS VPCs to which you wish to create software-defined cloud interconnects from an interconnect gateway.

Prerequisite

Associate AWS Account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Amazon Web Services**.

   The available host VPCs are discovered and listed in a table.

   The host VPC table includes the following columns:

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

5. Select the VPCs that you wish to tag using the check boxes in the left-most column.
6. Click **Tag Actions**.

   You can perform the following actions:

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

7. Click **Add Tag** and configure the following:

Tag Name	Enter a name for the tag that links the selected VPCs.
Region	List of regions that correspond to the selected VPCs. Click **X** to omit a region and associated VPCs from the tag.
Selected VPCs	List of VPC IDs of the selected host VPCs. Click **X** to omit a VPC from the tag.

(Cisco vManage Release 20.8.1 and earlier) Enable for Interconnect Connectivity (From Cisco vManage Release 20.9.1) Enable for SDCI partner Interconnect Connections	To use the VPC tag while creating a cloud interconnect connection to AWS, check the check box. If enabled, the tag can only be used for cloud interconnect connections and is not available for Multicloud Gateway Intent Mapping. If you do not check the check box, you cannot use the VPC tag to create a cloud interconnect connection. **Note** Do not enable this setting when you use cloud gateways to connect VPC workloads. You cannot edit this setting when the tag is in use by a connection.

8. Click **Add**.

On the **Discover Host Private Networks** page, the VPCs you selected earlier are tagged and the tag name is shown in the **Host VPC Tag** column. If you chose to use the VPC tag for software-defined cloud interconnects, the **Interconnect Enabled** column reads **Yes**.

Create Direct Connect Public Hosted Connection to AWS from Interconnect Gateway

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Attach Equinix Template to Cisco CSR 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
6. Create interconnect gateway at an Equinix Location.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the direct connect connection must be created.
7. Click **Add Connection**.

8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

9. Configure the following and click **Next**:

Equinix Hosted Connection VIF Type	Choose **Public**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.
Interconnect IP Address	Enter the public IP Address (CIDR) to be used as the BGP Peer ID of the interconnect gateway.
Amazon IP Address	Enter the public IP Address (CIDR) to be used as the AWS BGP Peer ID.
Prefixes	Enter the summary AWS addresses and prefixes you wish to advertise to the branch location.
Segment	Choose the segment ID for this connection.

10. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Private Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.

5. Discover Host Private Networks and tag AWS VPCs.
6. Attach Equinix template to Cisco CSR1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
7. Create Interconnect Gateway at an Equinix Location.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

9. Configure the following and click **Next**:

Equinix Hosted Connection VIF Type	Choose **Private**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.

Direct Connect Gateway	**a.** Click the Refresh button to fetch the Direct Connect gateways associated with the selected AWS account. **b.** Choose the direct connect gateway to which the direct connect connection must be created. Alternatively, create a new direct connect gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.

Settings	Choose one of the following:
	• **Global**:
	  • BGP peering IP address is picked from an internally reserved /16 subnet (198.18.0.0/16).
	  • BGP ASN is picked from the Global Settings.
	• **Custom**:
	  • Enter a custom /30 CIDR IP address for BGP peering.
	  • Enter custom BGP ASN for peering.
	Note You can specify a custom BGP ASN only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.

Attachment	Cisco vManage Release 20.8.1 and earlier: Choose **VPC**. **Segment**: Choose the segment ID for this connection. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection.
	Cisco vManage Release 20.9.1 and later: Choose one of the following: • **VPC** **Segment**: Choose the segment ID for this connection. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection. • **Cloud Gateway** **Cloud Gateways**: Choose the cloud gateways to attach to this connection. If the drop-down is empty, you must first create the cloud gateway using the multicloud workflows. For a single connection, AWS supports up to 10 cloud gateways. Each cloud gateway can be connected to 30 interconnect connections.

10. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Transit Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and Tag AWS VPCs.
6. Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.

   Attach Equinix Template to Cisco CSR 1000v Instance for versions prior to Cisco Catalyst SD-WAN Manager Release 20.12.1.

7. Create Interconnect Gateway at an Equinix Location.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the direct connect connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

9. Configure the following and click **Next**:

Equinix Hosted Connection VIF Type	Choose **Transit**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.
Direct Connect Gateway	**a.** Click the Refresh button to fetch the direct connect gateways associated with the selected AWS account. **b.** Choose the Direct Connect Gateway to which the direct connect connection must be created. Alternatively, create a new Direct Connect Gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.

Settings	Choose one of the following:
	• **Global**:
	  • BGP peering IP address is picked from an internally reserved /16 subnet (198.18.0.0/16).
	  • BGP ASN is picked from the Global Settings.
	• **Custom**:
	  a. Enter a custom /30 CIDR IP address for BGP peering.
	  b. Enter custom BGP ASN for peering.
	  Note You can specify a custom BGP ASN only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.

Segment	Choose the segment ID for this connection.
Attachment	Choose **Transit Gateway**. **Transit Gateway**: **a.** Click the Refresh button to fetch the transit gateways associated with the selected AWS account. **b.** Choose the transit gateway to which the direct connect connection must be created. Alternatively, create a new transit gateway by clicking **Add New Transit Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Select **AWS Region**. **d.** Click **Save**. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection. **Allowed Prefixes**: **a.** Click **Add Prefixes**. **b.** Enter the IPv4 CIDR prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard.

10. Review the connection summary.

- To create the connection, click **Save**.
- To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Interconnects to Google Cloud

Associate Google Cloud Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud** .
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Google Cloud**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.
Private Key ID	Click **Upload Credential File**. You must generate this file by logging in to the Google Cloud console. The private key ID may be in the JSON or the REST API format. The format depends on the method of key generation. For more details, see Google Cloud documentation.

5. Click **Add**.

Cisco SD-WAN Manager uses the Private Key ID to authenticate the user account with Google Cloud as part of the workflow to create connections to Google Cloud.

Create Interconnect to Google Cloud Routers from Interconnect Gateways

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Deploy Google Cloud Routers in network-regions to which you wish to connect.

   For nonredundant connectivity, on the Google Cloud console, deploy a Google Cloud Router in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

   For redundant connectivity, on the Google Cloud console, deploy two Google Cloud Routers in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

Starting from Cisco vManage Release 20.9.1, you can create the Google Cloud Routers and VLAN attachments fromCisco SD-WAN Manager during connection creation.

Note For use with interconnect attachments, you must set the Google ASN for the Google Cloud Routers to 16550.

3. Associate Equinix Account with Cisco SD-WAN Manager.
4. Configure Global Settings for Interconnect Gateways.
5. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
6. Create Interconnect Gateway at a Equinix Location closest to your Cisco Catalyst SD-WAN branch location.

   For redundant connectivity to Google Cloud, create a pair of interconnect gateways in the Equinix fabric. For nonredundant connectivity, deploy an interconnect gateway at a Equinix location.
7. Create necessary network segments (see Segmentation Configuration Guide).
8. Associate Google Cloud Account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Google Cloud**.
Google Account	Choose a Google account by the account name entered while associating the Google account details with Cisco SD-WAN Manager.
Attachment	Minimum supported release: Cisco vManage Release 20.9.1 Choose **Shared VPC** to attach a Google Cloud Router and Google Cloud Interconnect to the connection..

Region	Minimum supported release: Cisco vManage Release 20.9.1 Choose a Google Cloud region.
VPC Network	Minimum supported release: Cisco vManage Release 20.9.1 Choose the VPC network to deploy this connection.

Redundancy	For Cisco vManage Release 20.8.1 and earlier: Choose **Enable** if you want to create connections with redundancy. **Primary Google Cloud Interconnect Attachment:** • Click the refresh symbol next to the **Primary Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*. **Secondary Google Cloud Interconnect Attachment:** • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*. The secondary interconnect attachment options are determined based on the region and network to which the primary interconnect attachment belongs. If you do not have an unused interconnect attachment in the same region and network as the primary interconnect attachment, the drop-down list is empty and indicates that you must create a redundant interconnect attachment on the Google Cloud portal. Choose **Disable** if you want to create the connection without redundancy. **Google Cloud Interconnect Attachment**: • Click the refresh symbol next to the **Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*.

	For Cisco vManage Release 20.9.1 and later: **Google Cloud Router**: • Click the refresh symbol next to the **Google Cloud Router** drop-down list. • Choose a Google Cloud router or click **Add New Google Cloud Router**. If you clicked **Add New Google Cloud Router**, configure the router settings in the **Add Google Cloud Router** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Cloud Router Name: Enter a unique Google Cloud router name. **Note** Google Cloud routers are always created with a BGP ASN of 16550, MTU of 1500 and with default routing enabled. **Google Cloud Interconnect Attachment**: • Click the refresh symbol next to the **Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment or click **Add New Google Cloud Interconnect Attachment**. If you clicked **Add New Google Cloud Interconnect Attachment**, configure the router settings in the **Add Google Cloud Interconnect Attachment** 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. • IC 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.

9. Configure the following settings for the primary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the primary VLAN attachment.

Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

10. If you enabled redundancy in Step 8, configure the following settings for the secondary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the secondary VLAN attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary VLAN attachment.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which a connection must be established to the secondary VLAN attachment.

11. Configure the following and click **Next**:

Settings	Choose **Auto-generated** or **Custom**. • **Auto-generated:** The Interconnect BGP ASN is selected by the system • **Custom**: Specify Interconnect BGP ASN of your choice for peering with the interconnect VLAN attachments. **Note** You can specify a custom BGP ASN only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. BGP peering IP addresses for interconnects to Google Cloud Routers are auto-assigned by Google from the subnet (169.254.0.0/16). The IP addresses cannot be configured from Cisco SD-WAN Manager.
Segment	Choose a segment ID for this connection.

12. Review the connection summary.
    - To create the connection, click **Save**.
    - 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 **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

What to do Next: On the Google Cloud console, manage the routes advertised from the Google Cloud Routers towards the interconnect gateway via BGP.

Create Interconnect Connection to a Cloud Gateway In Google Cloud

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Associate Equinix Account with Cisco SD-WAN Manager.
3. Configure Global Settings for interconnect gateways.
4. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v instance.
5. Create Interconnect Gateway at a Equinix Location closest to your Cisco Catalyst SD-WAN branch location.

   For redundant connectivity to Google Cloud, create a pair of interconnect gateways in the Equinix fabric. For nonredundant connectivity, deploy an interconnect gateway at a Equinix location.
6. Create necessary network segments (see Segmentation Configuration Guide).
7. Associate Google Cloud Account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Google Cloud**.
Google Account	Choose a Google account by the account name entered while associating the Google account details with Cisco SD-WAN Manager.
Attachment	Choose **Cloud Gateway** to connect to a Cloud Gateway. **Cloud Gateways**: You can select only one Cloud Gateway from the drop-down list.

9. Configure the following and click **Next**:

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

10. Configure the following settings for the primary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the primary VLAN attachment.

Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

11. If you enabled redundancy in Step 8, configure the following settings for the secondary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the secondary VLAN attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary VLAN attachment.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which a connection must be established to the secondary VLAN attachment.

12. Configure the following and click **Next**:

Settings	Choose **Auto-generated** or **Custom**. • **Auto-generated:** The Interconnect BGP ASN is selected by the system • **Custom**: Specify Interconnect BGP ASN of your choice for peering with the interconnect VLAN attachments. **Note** You can specify a custom BGP ASN only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. BGP peering IP addresses for interconnects to Google Cloud Routers are auto-assigned by Google from the subnet (169.254.0.0/16). The IP addresses cannot be configured from Cisco SD-WAN Manager.
Segment	Choose a segment ID for this connection.

13. Review the connection summary.
    - To create the connection, click **Save**.
    - 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 **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

What to do Next: On the Google Cloud console, manage the routes advertised from the Google Cloud Routers towards the interconnect gateway via BGP.

Create Interconnects to Microsoft Azure

Associate Microsoft Azure Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud** .
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Microsoft Azure**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.
Tenant ID	Enter the ID of your Azure Active Directory (AD). **Tip** To find the tenant ID, go to your Azure Active Directory and click **Properties**.
Subscription ID	Enter the ID of the Azure subscription you want to use.
Client ID	Enter your existing Azure application ID. See Azure documentation for more information on how to register an application in Azure AD, get the client ID and secret key, and more.
Secret Key	Enter the password associated with the client ID.

5. Click **Add**.

Discover Host Private Networks and Tag Microsoft Azure VNets

Tag the Microsoft Azure VNets to which you wish to create software-defined cloud interconnects from an interconnect gateway. Azure VNets grouped using the same VNet tag are considered a singular unit.

Prerequisite

Associate Microsoft Azure Account with Cisco SD-WAN Manager.

Add a Tag

Group VNets and tag them together.

Note VNets belonging to different resource groups cannot be used together.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Choose the Azure VNets that you wish to tag by checking the corresponding check boxes.
6. Click **Tag Actions**.
7. Click **Add Tag** and configure the following:

Field	Description
Tag Name	Enter a name for the tag.
Region	If you selected VNets before clicking **Add Tag**, this field shows the list of regions that correspond to the selected VNets. • If you did not select VNets before clicking **Add Tag** or wish to select more regions, choose regions from the drop-down list. • Click **X** to omit a region and associated VNets from the tag.
Selected VNets	If you selected VNets before clicking **Add Tag**, this field shows the list of VNet IDs of the selected host VNets. • If you did not select VNets before clicking **Add Tag** or wish to select more VNets, choose VNets from the drop-down list. • Click **X** to omit a VNet from the tag.
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	To use the VNets tag while creating interconnect connections to Microsoft Azure, check the check box. If enabled for interconnect connetions, the tag cannot be used in the Microsoft Azure Multicloud workflow. If not enabled for interconnect connections, the tag can only be used with Microsoft Azure Multicloud workflow. **Note** Do not enable this setting when you use Cloud Gateways to connect VNet workloads.

8. Click **Add**.

On the **Host Private Networks** page, the Azure vNets you selected earlier are tagged and the tag name is shown in the **VNET Tag** column. If you chose to use the vNet tag for cloud interconnects, the **Interconnect Enabled** column reads **Yes**.

Edit a Tag

Add VNets to or remove VNets from an existing tag.

From Cisco vManage Release 20.10.1, edit a VNet tag associated with an interconnect connection subject to the following conditions:

- If only one VNet is associated with a VNet tag, you cannot remove the VNet from the tag. To remove the VNet from the tag, delete the interconnect connection and then edit the tag.
- For a private-peering connection with a virtual WAN attachment, the VNets you wish to associate with the tag must be from the same regions as the VNets already associated with the tag.

  To attach VNets from a new region to the private-peering connection, do the following:

  1. Create a new tag for the region and associate required VNets.
  2. Edit the private-peering connection and attach the VNet tag to the connection.

- For a private-peering connection with a VNet attachment, you can associate VNets from a new region to the tag while editing the tag.

Note In Cisco vManage Release 20.9.1 and earlier releases, you cannot edit a VNet tag that is associated with an interconnect connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Edit Tag** and modify the following as required:

Field	Description
Tag Name	From the drop-down list, choose a tag name.
Region	This field shows the list of regions that correspond to the VNets associated with the tag. • Choose additional regions from the drop-down list. • Click **X** to omit a region and associated VNets from the tag.
Selected VNets	This field shows the list of VNets associated with the tag. • Choose additional VNets from the drop-down list. • Click **X** to omit a VNet from the tag.

Field	Description
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	(Read only) Indicates whether the VNet is configured to be used while configuring interconnect connections or for Multicloud Gateway intent mapping.

7. Click **Update**.

Delete a Tag

Remove a tag that groups together VNets.

Note You cannot delete a VNet tag while the tag is associated with an interconnect connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Delete Tag**.
7. **Tag Name**: From the drop-down list, choose a tag name.
8. Click **Delete**.

Create Microsoft-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.

6. Create Interconnect Gateways at Equinix Location.

   For connectivity to Microsoft Azure, create a pair of interconnect gateways in the Equinix fabric. Redundant connectivity is the default and only supported configuration.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: Choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: Choose the Interconnect Gateway from which the connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Microsoft Azure**.
Azure Account	Choose a Microsoft Azure account by the account name entered while associating the account details with Cisco SD-WAN Manager.

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following 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 **Equinix**. • Peering Location: Click the Refresh button to update the list of available locations. 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**.

9. Configure the following settings for the primary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

10. Configure the following settings for the secondary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	The bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which the secondary connection must be established.

11. Configure the following and click **Next**:

Deployment Type	Choose **Public**.
Primary IPv4 Subnet	Enter a /30 CIDR public IP address for BGP peering from the primary interconnect gateway. Before creating the connection, ensure that your organization is permitted to use the public IPv4 address.
Secondary IPv4 Subnet	Enter a /30 CIDR public IP address for BGP peering from the secondary interconnect gateway. Before creating the connection, ensure that your organization is permitted to use the public IPv4 address.
BGP Advertise Prefix	Enter the summary addresses and prefixes you wish to advertise to the interconnect gateway.
Segment	Choose a segment ID for this connection.

12. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched. This task creates the following resources:

- virtual cross connects in the Equinix fabric between the interconnect gateways and the ExpressRoute
- Microsoft Azure public/private peerings for ExpressRoute circuits
- a vNet gateway, if a vNet gateway does not exist for a vNet
- connections between the ExpressRoute and the vNet gateways

When the task is successful, the connections are listed on the **Interconnect Connectivity** page.

You can also view the connection details on the Microsoft Azure portal.

Create Private-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag Microsoft Azure VNets.
6. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
7. Create Interconnect Gateways at Equinix Location.

   For connectivity to Microsoft Azure, create a pair of interconnect gateways in the Equinix fabric. Redundant connectivity is the default and only supported configuration.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the direct connect connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Microsoft Azure**.
Azure Account	Choose a Microsoft Azure account by the account name entered while associating the account details with Cisco SD-WAN Manager.

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following 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 **Equinix**. • Peering Location: Click the Refresh button to update the list of available locations. 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**.

9. Configure the following settings for the primary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

10. Configure the following settings for the secondary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	The bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which the secondary connection must be established.

11. Configure the following and click **Next**:

Deployment Type	Choose **Private**.
BGP-Peering Settings	Choose **Auto-generated** or **Custom**. **Auto-generated**: The interconnect BGP ASN, and the primary and secondary IPv4 subnets are selected by the system. The IPv4 subnets are selected from an internally reserved /16 subnet (198.18.0.0/16). **Custom**: **Note** You can specify a custom BGP ASN and custom IPv4 subnets only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. • **BGP ASN**: Specify an ASN of your choice for the primary and secondary peering with the ExpressRoute. • **Primary IPv4 Subnet**: Enter a /30 CIDR IP address for BGP peering with the primary interconnect gateway. • **Secondary IPv4 Subnet**: Enter a /30 CIDR IP address for BGP peering with the secondary interconnect gateway.
Attachment	Choose one of the following: • **vNet**: Attach VNets to the connection using VNet tags. • **vWAN**: Attach virtual WAN to the connection and choose VNets from the regions of the virtual WAN using VNet tags. • Minimum supported release: Cisco vManage Release 20.9.1 **Cloud Gateway**: Attach cloud gateways to the connection. You can select upto 5 cloud gateways per connection.
VNet Settings	**VNet Tags**: Choose VNet tags to identify VNets for which traffic must be routed through this connection.

virtual WAN Settings	**vWAN**: Choose or add a new virtual WAN. **Note** You can choose the virtual WAN to be attached only for the first connection to Microsoft Azure from an interconnect gateway for the selected resource group of the ExpressRoute Circuit. The same virtual WAN is attached to any subsequent connection in the same resource group to which you choose to attach a virtual WAN. Starting from Cisco vManage Release 20.8.1, Cisco SD-WAN Manager supports one virtual WAN per Microsoft Azure resource group per Microsoft Azure account. Once that vWAN is chosen and used as part of a virtual WAN connection, subsequent virtual WAN connections to the same Microsoft Azure resource group use the same virtual Wan. The Microsoft Azure resource group is determined for the connection when the ExpressRoute Circuit is selected for it. All other Microsoft Azure resources belonging to the connection must be in the same Microsoft Azure resource group as that of the selected ExpressRoute Circuit. **vNet**: Choose VNet tags to identify VNets for which traffic must be routed through this connection. Cisco SD-WAN Manager finds VNets based on the chosen VNet Tags, and identifies the regions to which the VNets belong. For the chosen virtual WAN and the identified regions, Cisco SD-WAN Manager finds and lists the available virtual hubs for verification. For regions where a virtual hub does not exist, you must specify the name and address-prefix to add a virtual hub. **vHub Settings**: **Note** From Cisco Catalyst SD-WAN Manager Release 20.12.1, if multiple Azure Virtual WAN hubs are there in a region, you can select a particular Azure Virtual WAN hub for that region. Once you choose the Azure Virtual WAN hub, all subsequent connections created for Azure Virtual WAN uses the same Azure Virtual WAN hub. **a.** Click **Add Settings**. Or, if you're modifying the configuration, click **Edit Settings**. **b.** Review the virtual hub name and address-prefix for applicable regions. If a virtual hub does not exist in a region, enter the virtual hub name and address-prefix to be used for the region. **Note** Ensure that the virtual hub address-prefix that you enter does not overlap with the address-prefixes of any VNets. **c.** To apply changes, click **Save**. To discard changes, click **Cancel**.
Segment	Choose a segment ID for this connection.

12. Review the connection summary.

- To create the connection, click **Save**.
- To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched.

For VNet attachmment, the configuration task creates the following resources:

- virtual cross connects in the Equinix fabric between the interconnect gateways and the ExpressRoute
- Microsoft Azure public/private peerings for the ExpressRoute circuits
- a vNet gateway, if a vNet gateway does not exist for a vNet
- connections between the ExpressRoute and the vNet gateways

For virtual WAN attachment, the configuration task creates the following resources:

- virtual cross connects in the Equinix fabric between the interconnect gateways and the ExpressRoute
- Microsoft Azure public/private peerings for the ExpressRoute circuits
- necessary virtual hubs
- connections between vNets and virtual hubs
- an ExpressRoute Gateway for each virtual hub, if necessary
- connections between the ExpressRoute Gateway and ExpressRouteCircuits

When the task is successful, the connections are listed on the **Interconnect Connectivity** page.

You can also view the connection details on the Microsoft Azure portal.

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.
- When you upgrade to Cisco vManage Release 20.9.2 and Cisco vManage Release 20.10.1, you have to modify the device link by adding or removing some devices to push new configuration to the devices. Otherwise, the BFD session for site-to-site connection goes down when site-to-site and device link are present on the same Interconnect Gateway.

Add Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. Click **Device Links**.
5. Click **Add Device Links**.
6. Choose **Account name** from the drop down menu. This is the Equinix account that has been associated to Cisco SD-WAN Manager through Account Association.
7. Enter **Device link name**.
8. Choose **Bandwidth** from the drop down menu.

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

9. (Optional)

   Enter **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.

10. Select **Gateway Name** from the drop down menu. Select at least two gateway names.
11. Click **Save**.

Delete Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. Click **Device Links**.

   Existing device links are summarized in a table.
5. In the table, find the desired link and click **...**.

6. To delete a device link, click **Delete** and confirm that you wish to delete the device link.

Update Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. Click **Device Links**.

   Existing device links are summarized in a table.
5. In the table, find the desired link and click **...**.
6. To edit the device link, click **Edit**.
7. 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.

8. Click **Save**.

Create Interconnect Between Interconnect Gateways

From Cisco SD-WAN Manager, you can create an interconnect between interconnect gateways at two or more Equinix locations. By doing so, you can link the SD-WAN branch locations connected to these interconnect gateways via the Equinix fabric.

Prerequisites

For each SD-WAN branch location to be connected through the Equinix fabric, complete the following configuration prerequisites:

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Identify the nearest Equinix location.
5. Create an Interconnect Gateway at the Equinix location closest to the branch location.

Note If you have a VRF defined in two branch locations and wish to exchange traffic attached to the VRF through the connection between the interconnect gateways, you must configure the VRF and an appropriate centralized policy on the interconnect gateways to route the branch traffic through the connection between the interconnect gateways.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the source interconnect gateway.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Edge**.
Connection Name	Enter a unique name for the connection.
Interconnect Gateway	Choose destination interconnect gateway.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.

Note Interconnect gateways belonging to a device link group cannot be used to form a point to point connection.

9. Review the connection summary.
   - To create the connection, click **Save**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Verify and Modify Configuration for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

View Interconnect Gateway and Connection Summary

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** > **Interconnect**. On this page, you can view a summary of the interconnect gateways and connections that you have created. If you have not created any interconnect gateways, page provides an overview of the workflow for creating and managing interconnect gateways and connections.

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

   The following information is displayed:

Interconnect Gateways	• Total number of interconnect gateways • Number of interconnect gateways that reachable (Up) • Number of interconnect gateways that are unreachable (Down)
Connections	• Total number of connections • Number of connections in the Up state • Number of connections in the Down state
Summary Table	Summarized list of all interconnect gateways and connections from the gateways.
Device Link	• Total number of Device Link • Number of Device Link in the Up state • Number of Device Link in the Down state

View, Edit or Delete Connections

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.
- While creating a connection to AWS, if you created a direct connect gateway or transit gateway from Cisco SD-WAN Manager, deleting the connection does not delete the gateway. You need to manage these AWS resources as required.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you have the option to delete the Direct Connect Gateway or Transit Gateway while deleting the connection.
- When deleting a connection to AWS, because of uncommon timing issues in the order in which the resources are torn down by AWS and Equinix, it is possible that Cisco SD-WAN Manager returns an error stating a failure in connection deletion with a 400 error returned by the service provider. Cisco SD-WAN Manager fully clears the connection from its database, and clears all related device configurations. It is recommended that you login to the Equinix portal and verify that the interface configuration and association has been deleted from the Equinix database as well, so that the same interface can be reused at a later time for a different connection.

  Failure to verify the status of the interface in Equinix portal might lead to errors in creating any new connection for the same device.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.

   Existing connections are summarized in a table.
4. In the table, find the desired connection and click **...**.
   - To view more information about a connection, click **View**.
   - To delete a connection, click **Delete** and confirm that you wish to delete the connection.

Edit Connection Configuration

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1 and Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.

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

   The following tables describe the editable parameters based on the connection destination and the connection type, if any. Configure the parameters as required.

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

Note You can modify the properties of active connections only.

Table 4: Editable Properties of Interconnect Connections to AWS

Field	Description	Applicable Connection Types
Segment	Choose a different segment ID for this connection.	All connections to AWS
Transit Gateway	**a.** Click the **Refresh** button to fetch the transit gateways associated with the selected AWS account. **b.** Choose the transit gateway to which the direct connect connection must be created. **Note** • The transit gateway that you wish to remove is not the only transit gateway associated with the connection. • You can remove VPC tags corresponding to the region served by the transit gateway in the same edit operation. **Note** You cannot replace an existing transit gateway for a region with another transit gateway from the same region.	Transit-hosted connections
VPC Tags	Choose VPC tags to identify VPCs for which traffic must be routed through this connection.	• Private-hosted connections with VPC attachments • Transit-hosted connections
Allowed Prefixes	Click **Edit Prefixes**. Enter the IPv4 Classless Inter-Domain Routing (CIDR) prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard. **Note** You can add additional prefixes. You cannot remove existing prefixes.	Transit-hosted connections

Table 5: Editable Properties of Interconnect Connections to Google Cloud

Field	Description
Connection Speed	Choose the desired bandwidth from the **Connectivity Speed** drop-down list. In the case of redundant connections, modify the connection speed of either the primary or the secondary connection. The peer connection is updated to use the same connection speed. The bandwidth options for a connection may depend on the associated peering location.

Note Modify the property of either the primary or the secondary connection. The peer connection is updated to use the same configuration.

Table 6: Editable Properties of Interconnect Connections to Microsoft Azure

Field	Description	Applicable Connection Types
Bandwidth	Modify the connection bandwidth. Unit: Mbps. **Note** You can only increase the bandwidth of connections to Microsoft Azure. For connections to Microsoft Azure, you must increase the bandwidth of the ExpressRoute on the Azure portal before increase the connection bandwidth on Cisco SD-WAN Manager.	Private and public (Microsoft) peering connections
Segment	Choose a different from segment ID for this connection.	Private and public (Microsoft) peering connections
BGP Advertise Prefix	Enter the summary addresses and prefixes you wish to advertise to the interconnect gateway. **Note** By default Microsoft Azure uses an older version of API on its portal for displaying resources or network objects that do not display the BGP advertise prefix correctly. To verify the BGP advertise prefix from the Microsoft Azure portal, select 2020-05-01 or above API version.	Public (Microsoft) peering connections
VNet Settings		
VNet	Choose VNet tags to identify the VNets for which traffic must be routed through this connection.	Private peering connections

Field	Description	Applicable Connection Types
vHub Settings	**a.** Click **Edit Settings**. **b.** Review the virtual hub name and the address-prefix for applicable regions. If a virtual hub does not exist in a region, enter the virtual hub name and address-prefix to be used for the region. **Note** Ensure that the virtual hub address-prefix that you enter does not overlap with the address-prefixes of any VNets. **c.** To apply changes, click **Save**. To discard changes, click **Cancel**.	Private peering connections

Table 7: Editable Properties of Interconnect Connections Between Edge Devices

Field	Description
Bandwidth	Modify the connection bandwidth. Unit: Mbps.

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

View, Edit, or Delete an Interconnect Gateway

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

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

     Deleting the interconnect gateway disconnects the branch location from the Equinix fabric.

View, Edit, or Delete an Interconnect Account

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

2. Click **Interconnect**.
3. Click **Account Management**.

   The available interconnect accounts are listed in a table.
4. For the desired interconnect account, click **...** and do as follows:
   - To view more details about the interconnect account, click **View**.
   - To modify interconnect account details, click **Edit Account Information**.

     You can modify the **Account Name** and the **Description**.
   - To modify interconnect account credentials, click **Edit Account Credentials**.

     You can modify the **Customer Key** and **Customer Secret** for the account.

Note Modifying the credentials on Cisco SD-WAN Manager, does not modify the credentials with the interconnect provider. Use this configuration option only to replicate any changes to the account credentials that you have performed on the relevant portal of the Interconnect Provider.

   - To delete the interconnect account, click **Remove** and confirm that you wish to remove the account.

Audit Management

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1

The audit management support added to the fabric of the SDCI provider Equinix helps you check if the cloud state is in sync with the Cisco SD-WAN Manager state or not. The audit process involves scanning the provider resources, interconnect gateways, and connections to the cloud. When there are errors, they are displayed and if there are no errors, the status is displayed as **In Sync**.

Accessing the Audit Report

1. In the **Cloud onRamp for Multicloud** page, navigate to the **Interconnect** tab.
2. In the **Intent Management** pane, click **Audit**.
3. In the **Intent Management- Audit** screen, under **Interconnect Gateways**, choose an **Interconnect Provider** from the drop-down list.
4. Choose **Interconnect Connections**.
5. To view the desired audit report, choose a **Destination Type** and choose a **Cloud Provider** from the drop-down list when the destination type is **cloud**.
6. Select the **Device Links** option.

Parameter Name	Description
Interconnect Provider	Choose the interconnect provider type from the drop-down. The options are: • **Megaport** • **Equinix**
Interconnect Connections	Enable or disable the interconnect connections.
Destination Type	Choose the destination type from the drop-down list. The options are: • **Cloud** • **Edge**
Cloud Provider	Choose the cloud provider from the drop-down list. The options are: • **Amazon Web Servcies** • **Microsoft Azure** • **Google Cloud**
Device Links	Choose the device links for the interconnect provider.

Note After the audit is completed, the following reports are generated:

- **Edge Gateway**: Provides information about configured edge gateways.
- **Edge Connections**: Provides information about configured edge connections.
- **Unknown Edge Gateways**: Provides information about unknown edge gateways.
- **Unknown Edge Connections**: Provides information about unknown edge connections.

The following are the statuses that are displayed in the audit report along with the details:

- **In Sync**
- **Out of Sync**
- **AUDIT_INFO**

Benefits of Audit

Audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what has been realized in the cloud. The gaps are in terms of cloud resources, connectivity, and states. When such gaps are detected, Cisco SD-WAN Manager flags such gaps and helps you take corrective action.

Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

Scenario	Resolution
Unable to add Interconnect Account	• Verify that the account credentials associated with Cisco SD-WAN Manager are correct. • If you updated the credentials with interconnect provider, update the account credentials on Cisco SD-WAN Manager.
While attempting to create an interconnect gateway, the device list is empty	Verify that you have attached the Equinix template to the devices. (Recommended template: *Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02*)
While attempting to create an interconnect gateway, cannot find the desired location	Click the Refresh button to update the list of available locations.
Creation of interconnect gateway failed	**1.** Check the configuration task progress on Cisco SD-WAN Manager for any error messages. **2.** If you are using the Interconnect Global Settings, check whether the selected software image is available at the Interconnect Provider location. **3.** If the VM instance is not deployed or the IP pool is exhausted, check with the Interconnect provider.
Certificate is not installed successfully for interconnect gateway	From the Cisco SD-WAN Manager menu, click **Maintenance** > **Device Reboot**. From the **Device Reboot** page, reboot the interconnect gateway.
While creating a direct connect connection, the direct connect gateway or the transit gateway list is empty	**1.** On the AWS portal, verify that the desired direct connect gateway or transit gateway is available. **2.** Click the Refresh button to fetch the list of gateways from AWS. **3.** If a gateway is not available in AWS, create the gateway through Cisco SD-WAN Manager.
While creating a direct connect connection, host VPC tags are not listed	Verify that the host VPC tags are available and enabled for Interconnect connectivity.

Scenario	Resolution
Creation of Direct Connect connection failed	**1.** Check the configuration task progress on Cisco SD-WAN Manager for any error messages. **2.** If you are using the interconnect global settings, check whether the internal IP address pool has been exhausted. If yes, delete some connections and retry. **3.** If you are using custom settings, ensure that you haven't entered overlapping CIDR subnets for peering. **4.** Check whether you have reached any connection limits. See *Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix*. **5.** Verify permissions of the interconnect provider account and the AWS account.
Traffic flow issues	**1.** Ensure that the required security rules for inbound and outbound traffic are configured for the host VPC. **2.** Verify whether the virtual interface has been created and attached to the direct connect gateway. **3.** In AWS, verify whether the BGP peering status is in the UP state for the virtual interface. **4.** Verify whether the correct route table is being used as the main routing table for the host VPC and whether the necessary routes are being propagated towards the virtual private gateway or the transit gateway. **5.** Verify whether the virtual private gateway or transit gateway is attached to the direct connect gateway.
Latency issues	**1.** Verify whether the interconnect gateway location is in close proximity to the direct connect location chosen while creating the connection. **2.** Ensure that you have configured the appropriate bandwidth for the connection.
Cloud gateways are not displayed in the drop-down list	Ensure that the necessary cloud gateways are created using the multicloud workflow and the minimum requirements listed in this document are met.

Scenario	Resolution
Traffic to VPC or VNET workload is sent over the internet even after creating an interconnect connection to the cloud gateway	When an Cisco Catalyst SD-WAN branch is connected to a cloud gateway through the internet and through an interconnect connection from an interconnect gateway to access the same VPC or VNET workload, by default, traffic from the branch is sent through the internet. To make the private path through the interconnect gateway the preferred path, apply appropriate control and data policies to the WAN edge device at the branch, the interconnect gateway, and the cloud gateway.