

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

Table 1: Feature History

Feature Name	Release Information	Description
Software-Defined Interconnects Megaport	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance as the interconnect gateway in the Megaport 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 Megaport fabric.
Cisco Catalyst SD-WAN Cloud Interconnect with Megaport: Interconnects to Google Cloud and Microsoft Azure	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance as the interconnect gateway in the Megaport fabric and connect a Cisco Catalyst SD-WAN branch location to the interconnect gateway. From the interconnect gateway, 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 Megaport fabric.

Feature Name	Release Information	Description
Encrypted Multicloud Interconnects with Megaport	Cisco vManage Release 20.9.1	You can extend the Cisco Catalyst SD-WAN fabric from the Interconnect Gateway in Megaport 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.

Feature Name	Release Information	Description
Modify Additional Properties of Interconnect Connections to AWS and Microsoft Azure	Cisco vManage Release 20.10.1	

Feature Name	Release Information	Description
		Interconnect Connections to AWS: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwidth of a hosted VIF connection after it is created. Properties of hosted connections cannot be edited after connection creation. With this feature, edit additional properties of both hosted VIF and hosted connections after connection creation. For a full list of editable properties, see Table 4: Editable Properties of Interconnect Connections to AWS, on page 63. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VPC tag that is associated with a connection. With this feature, to attach VPCs to or detach VPCs from a Private Hosted VIF, Private Hosted Connection, or a Transit Hosted Connection, edit the VPC tags associated with the connection to add or remove VPCs. Interconnect Connections to Microsoft Azure: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwith of a connection after it is created. Other properties of a connection are not editable. With this feature, edit additional properties of both Microsoft peering and private peering connections. For a full list of editable properties, see Table 6: Editable Properties of Interconnect Connections to Microsoft Azure, on page

Feature Name	Release Information	Description
		65. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VNet tag that is associated with a connection. With this feature, to attach VNets to or detach VNets from a Private Peering Connection, edit the VNet tags associated with the connection to add or remove VNets.
Audit Management	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	The audit management feature helps in understanding if the interconnect cloud and provider connection states are in sync with the Cisco SD-WAN Manager connection state. The State refers to the various connection statuses that Cisco Catalyst SD-WAN establishes with cloud services and providers. The audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what is realized in the cloud.

• Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 5
• Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 6
• Information About Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 12
• Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 14
• Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Megaport, on page 16
• Create Interconnects to AWS, on page 22
• Create Interconnects to Google Cloud, on page 38
• Create Interconnects to Microsoft Azure, on page 47
• Create Interconnect Between Interconnect Gateways, on page 60
• Verify and Modify Configuration, on page 62
• Audit Management, on page 68
• Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 69

Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

- Create Megaport account.

As part of the ordering process on Cisco Commerce workspace, you receive an email from Megaport about creating your account. Refer to the email for more information.

- For a connection that requires a public peering between an Interconnect Gateway and a Cloud provider, specify a public BGP ASN and a public BGP peering IP address. Ensure that your organization is permitted to use the public BGP ASN and the public BGP peering IP address before you create the connection.
- Ensure you have UUIDs for the required number of Cisco Catalyst 8000v instances that you wish to deploy as Interconnect Gateways.
- Ensure that Cisco SD-WAN Manager can connect to the Internet.

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

Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

General Restrictions

- At each location, at a time, you can perform only a single interconnect operation such as deploying an Interconnect Gateway, or creating or deleting a connection at a 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.
- Cloud Service Provider allocations apply to all Interconnect cloud connections created from Cisco SD-WAN Manager.
- 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.

  While Cisco SD-WAN Manager enforces this restriction from Cisco vManage Release 20.9.2 and Cisco vManage Release 20.10.1, 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.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco Catalyst SD-WAN Cloud Interconnect with Megaport is supported only on versions Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later.
- 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.

Interconnects to AWS

- While creating a connection to an AWS cloud resource, adhere to 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.

- 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.
- Megaport AWS private hosted VIF connection fails if direct gateway BGP ASN is more than 4200000000.
- From Cisco vManage Release 20.9.2, for a transit-hosted connection, in an AWS region, you can associate only one transit gateway with a Direct Connect gateway.

  While Cisco SD-WAN Manager enforces this restriction from Cisco vManage Release 20.9.2, 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.
- 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.
- With Cisco vManage Release 20.5.1, you cannot edit a connection after its creation.

  From Cisco vManage Release 20.6.1, you can modify the bandwidth of hosted VIF connections created earlier. However, you cannot modify the bandwidth of hosted connections after they have been created.
- 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.
- Cisco vManage Release 20.9.x and earlier: A host VPC tag selected for Interconnect Connectivity cannot be edited while the tag is in use.

  From Cisco vManage Release 20.10.1: A host VPC tag selected for Interconnect Connectivity can be edited while the tag is in use to add or remove host VPCs.
- Cisco vManage Release 20.9.x and earlier: If a host VPC is associated with a tag and the tag is used in configuring an Interconnect Connection, the host VPC cannot be dissociated from the tag and associated with another tag.

  From Cisco vManage Release 20.10.1: If a host VPC is associated with a tag and the tag is used in configuring an Interconnect Connection, you can dissociate the host VPC from the tag if one or both of the following conditions are met:
  - Additional host VPCs are associated with the tag
  - Additional VPC tags are used in configuring the Interconnect Connection

  After a host VPC is dissociated from a tag, it can be associated with another tag.

  If a VPC tag is used in configuring an Interconnect Connection, you can associate more host VPCs with the tag provided that these host VPCs belong to the same regions as the host VPCs already associated with the tag.
- While creating a Direct Connect Private Hosted VIF, a Direct Connect Private Hosted Connection, or a Direct Connect Transit Hosted Connection to an AWS Direct Connect Gateway from an Interconnect Gateway, you can specify a custom IP address for BGP peering or let Cisco SD-WAN Manager pick an IP address from an internally reserved pool.

In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the subnet 198.18.0.0/16. Before upgrading Cisco SD-WAN Manager from release 20.5.x to 20.6.1 or later, check if any connection to AWS is configured to use a custom BGP peering IP address from the subnet 198.18.0.0/16, which is internally reserved from Cisco vManage Release 20.6.1. If so, delete the connection and re-create the connection with a custom IP address that does not overlap with 198.18.0.0/16.

- When editing interconnect transit connection, if a new transit gateway is selected without a VPC tag in the same region, connection edit is discarded.

Interconnects to Microsoft Azure

- While creating host VNet tags, choose to use the tag with either the Microsoft Azure 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.
- Cisco vManage Release 20.9.x and earlier: A host VNet tag selected for Interconnect Connectivity cannot be edited after creation.

  From Cisco vManage Release 20.10.1: A host VNet tag selected for Interconnect Connectivity can be edited while the tag is in use to add or remove host VNets.
- Cisco vManage Release 20.9.x and earlier: If a host VNet is associated with a tag and the tag is used in configuring an Interconnect Connection, the host VNet cannot be dissociated from the tag in use and associated with another tag.

  From Cisco vManage Release 20.10.1: If a host VNet is associated with a tag and and the tag is used in configuring an Interconnect Connection, the host VNet can be dissociated from the tag if one or both of the following conditions are met:
  - Additional host VNets are associated with the tag
  - Additional VNet tags are used with the Interconnect Connection

  After a host VNet is dissociated from a tag, it can be associated with another tag.

  If a VNet tag is used in configuring an Interconnect Connection, you can associate more host VNets with the tag provided that these host VNets belong to the same regions as the host VNets already associated with the tag.
- 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 uses the same ASN for all its BGP sessions.

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 Megaport

Table 2: Connection Configuration Limits

Description	Count
Interconnect Gateway	
Maximum number of connections (VXC) per Interconnect Gateway	15 **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

Description	Count
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
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 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 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. Manage these AWS resources as required.
- 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.

In Cisco vManage Release 20.5.1, a default route to the virtual private gateway or transit gateway is created in the Main route table 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.

From Cisco vManage Release 20.6.1, a default route is created in the Main route table to only the transit gateway, and route propagation is enabled. Edit the routes and propagation as required.

- 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.

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. In the Megaport fabric, an interconnect is created from the Interconnect Gateway to 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. In the Megaport fabric, an interconnect is created from each of a pair of Interconnect Gateways to 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.

- In the Azure portal, if cloud gateway extension connections intended for one ExpressRoute gateway also appear in a second ExpressRoute gateway, create two ExpressRoute gateways with a different prefix.

- 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.
- Each region of a virtual WAN must have only one virtual hub.
- 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 Megaport 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 Megaport

You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance in the fabric of the SDCI provider Megaport. Further, you can link a branch location to the Cisco Catalyst 8000v instance using the Cisco Catalyst SD-WAN fabric. We recommend that you deploy the Cisco Catalyst 8000v instance at a Megaport location closest to your branch location.

The Cisco Catalyst 8000v instance acts as an edge device in the Cisco Catalyst SD-WAN fabric and as the Interconnect Gateway in the Megaport fabric. From the Interconnect Gateway, you can create a direct Layer 2 connection (an interconnect) in the Megaport fabric to a cloud onramp or another Interconnect Gateway. The interconnects link branch locations, or link branch locations to cloud service providers through the Megaport fabric.



Note In the Megaport terminology, the interconnect gateway is also referred to as the Megaport Virtual Edge (MVE). The direct Layer 2 connection from an interconnect gateway to a Cloud OnRamp or another interconnect gateway is called a Virtual Cross Connect (VXC).

In this setup, Cisco Catalyst SD-WAN fabric acts as the overlay network, and the Megaport fabric acts as the underlay network. The Megaport fabric provides data-center-agnostic, efficient, high-speed, low-latency, high-bandwidth connectivity across data centers in 700 global locations.

You can create the following types of connections from an Interconnect Gateway:

Table 3: Connection Types

Destination	Connection Types	From Release
Amazon Web Services	• Direct Connect - Public Hosted Virtual Interface (VIF) • Direct Connect - Private Hosted VIF • Direct Connect - Public Hosted Connection • Direct Connect - Private Hosted Connection • Direct Connect - Transit Hosted Connection	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1
Google Cloud	Partner Interconnect Attachment to a Google Cloud Router	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1
Microsoft Azure	• Partner ExpressRoute Circuit - Microsoft Peering • Partner ExpressRoute Circuit - Private Peering	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1
Interconnect Gateway	Link between Cisco Catalyst SD-WAN Branch Locations connected to the Interconnect Gateways	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1

Cisco SD-WAN Manager enables you to

- Configure and deploy the Cisco Catalyst 8000v instance at a Megaport location
- Create software-defined cloud interconnects to public or private clouds
- Create interconnects to link Cisco Catalyst SD-WAN branch locations across the Megaport fabric

Support is offered along with this solution. Contact Cisco Support for any questions or issues regarding this solution.

Benefits of Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

1. Branch locations connect seamlessly to the Megaport fabric over the Cisco Catalyst SD-WAN fabric.
2. Interconnects to public or private cloud with assured SLAs.
3. End-to-end traffic security, segmentation, and policy through the Cisco Catalyst SD-WAN fabric.
4. Cisco is the single point of contact for billing, provisioning, and support.
5. Cisco SD-WAN Manager provides a single pane to manage your connectivity to any cloud.

6. End-to-end visibility across the Cisco Catalyst SD-WAN fabric and the Megaport SDN.
7. Data-center-agnostic links between Cisco Catalyst SD-WAN branch locations and between Cisco Catalyst SD-WAN branch locations and a public or private 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 Megaport

Prerequisite Configuration

1. Create Megaport account.

   As part of the ordering process on Cisco Commerce Workspace (CCW), you receive an email from Megaport about creating your account. Refer to the email for more information.
2. Associate Megaport account with Cisco SD-WAN Manager.
3. Configure Global Settings for Interconnect Gateways.
4. Create necessary network segments. For more information refer to Segmentation Configuration Guide.
5. Ensure you have UUIDs for the required number of Cisco Catalyst 8000v instances that you wish to deploy as Interconnect Gateways.
6. Attach Megaport Template to a Cisco Catalyst 8000v instance.

7. Create Interconnect Gateway at Megaport location closest to your Cisco Catalyst SD-WAN branch location.

   For connectivity to AWS, create an Interconnect Gateway at the Megaport location.

   For redundant connectivity to Google Cloud, create a pair of Interconnect Gateways in the Megaport fabric. For nonredundant connectivity, deploy an Interconnect Gateway at a Megaport location.

   For connectivity to Microsoft Azure, create a pair of Interconnect Gateways in the Megaport fabric. Redundant connectivity is the default and only supported configuration.

   For connectivity between Cisco Catalyst SD-WAN branch locations, for each branch location, create an Interconnect Gateway at the closest Megaport 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 Virtual Interface (VIF)	Use this connection for a link to a public AWS resource, with the link having a bandwidth between 50 Mbps and 1 Gbps.
Direct Connect - Private Hosted VIF	Use this connection for a dedicated link to an AWS VPC, with the link having a bandwidth between 50 Mbps and 1 Gbps. **Note**: Bandwidth of a connection must not exceed the purchased entitlement.
Direct Connect - Public Hosted Connection	Use this connection for a link to a public AWS resource, with the link having a fixed bandwidth of more than 1 Gbps.
Direct Connect - Private Hosted Connection	Use this connection for a dedicated link to an AWS VPC, with a link bandwidth of more than 1 Gbps.
Direct Connect - Transit Hosted Connection	Use this connection for dedicated links to up 5,000 AWS VPCs via a transit gateway, with a link bandwidth of more than 1 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.
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. Create the required Azure ExpressRoute circuits.
3. Discover Host Private Networks to connect to Azure Virtual Networks (VNets).
4. 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 Megaport

Associate Megaport Account with Cisco SD-WAN Manager

Prerequisite

Create Megaport account. As part of the ordering process on Cisco Commerce Workspace (CCW), you receive an email from Megaport about creating your account. Refer to the email for more information.

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 **Megaport**.
Account Name	Enter a name of your choice. This name is used to identify the Megaport account in workflows that define the cloud or site-to-site interconnects. **Note** Starting from Cisco vManage Release 20.6.1, spaces are not allowed in Account Name. If you are upgrading Cisco SD-WAN Manager from Cisco vManage Release 20.5.1 to Cisco vManage Release 20.6.1, remove the spaces in your Account Name or replace the spaces with '_'.
Description (Optional)	Enter a description.
User Name	Enter the username of your Megaport account.
Password	Enter the password of your Megaport account.

5. Click **Add**.

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

Configure Global Settings for Interconnect Gateways

Prerequisites

1. Create a Megaport account. As part of the ordering process on Cisco Commerce Workspace (CCW), you receive an email from Megaport about creating your account. Refer to the email for more information.
2. Associate Megaport 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**.
   a. To add global settings, click **Add**.
   b. 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 **Megaport**.
Software Image	Choose a Catalyst 8000v image.
Instance Size	Instance Size determines the compute footprint and throughput of each Cisco Catalyst 8000v instance.
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 Megaport Template to Cisco Catalyst 8000v Instance



Note This procedure is not required if you enabled configuration groups. In this case, skip to Create Interconnect Gateway at a Megaport Location section in the Cisco Catalyst SD-WAN Cloud Interconnect with Megaport chapter in *Cloud OnRamp Configuration Guide*.

Before you can deploy a Cisco Catalyst 8000v instance as an Interconnect Gateway at a Megaport location, you must attach the Megaport default template to the device. We recommend that you attach the template named *Default_MEGAPORT_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_MEGAPORT_ICGW_C8000V_Template_V01*.
4. For the template, click **...** and click **Attach Devices**.
5. Choose the Cisco Catalyst 8000v instance from **Available Devices** and move it to **Selected Devices**. Click **Attach**.
6. Configure the following and click **Next**.
   - Color
   - Hostname
   - System IP
   - Site ID
7. Click **Configure Devices**.

Create an Interconnect Gateway at a Megaport Location

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

Before You Begin

1. Associate a Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Attach a Megaport template to a Cisco Catalyst 8000v instance, if you do not wish to enable configuration groups.
4. If you enable configuration groups, ensure that you configure device parameters for devices that are associated with the configuration group.
5. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the Interconnect Gateway. Without the required license, Interconnect Gateway creation fails.

Create an Interconnect Gateway at a Megaport Location

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 **Megaport**.
Gateway Name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.
Account Name	Choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager. (Minimum release: Cisco vManage Release 20.9.1) To view the Interconnect Gateway licenses associated with the account, click **Check available licenses**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose the Megaport location where the Cisco 8000v instance must be deployed.
Provider License Type	(Minimum release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Choose one of the following: • **Prepaid**: Choose a prepaid license type to create the interconnect gateway. Before Cisco Catalyst SD-WAN Manager Release 20.14.1, by default, only the prepaid license type was available. • **PayG**: Choose a pay-as-you-go (PAYG) license type to create the interconnect gateway.
IP Transit	(Minimum release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Choose the IP transit bandwidth value.
NHM Region	(Minimum release: Cisco Catalyst SD-WAN Manager Release 20.14.1) From the drop-down list, choose a network health monitoring (NHM) region for which you want to create the interconnect gateway.
Site Name	(Minimum release: Cisco vManage Release 20.10.1) From the drop-down list, choose a site for which you want to create the interconnect gateway.

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 are created in Cisco Catalyst SD-WAN. The configuration groups in this drop-down list include the options that are needed for this provider.
Chassis Number	Choose the chassis number of a Cisco Catalyst 8000v instance that has the Megaport default template attached. **Note** From Cisco vManage Release 20.10.1, the chassis numbers are auto-populated when you choose a site from the **Site Name** drop-down list.
Instance Settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect Global Settings. • **Custom**: Choose a specific instance size and software image for this gateway.
MRF Role	(Minimum release: Cisco vManage Release 20.10.1) Choose a router role: **Border** or **Edge**. This option is available only when Multi-Region Fabric is enabled.
Transport Gateway	(Minimum release: Cisco vManage Release 20.10.1) Choose **Enabled** or **Disabled**. This option is available only when Multi-Region Fabric is enabled.

5. Click **Add**.

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

Create Interconnects 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.

Add a Tag

Group VPCs and tag them 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 **Amazon Web Services**.

   The available host VPCs are discovered and listed in a table.
5. Select the VPCs that you wish to tag using the check boxes in the left-most column.

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

Field	Description
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.
(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 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 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**.

Edit a Tag

Add VPCs to or remove VPCs from an existing tag.

From Cisco vManage Release 20.10.1, edit a VPC tag associated with an Interconnect Connection subject to the following conditions:

- If only one VPC is associated with a VPC tag, you cannot remove the VPC from the tag. To remove the VPC from the tag, delete the Interconnect Connection and then edit the tag.
- For a Transit Hosted Connection, the VPCs you wish to associate with a tag must be from the same regions as the VPCs already associated with the tag.

  To attach VPCs from a new region to the Transit Hosted Connection, do the following:

  1. Create a new tag for the region and associate required VPCs.
  2. Edit the Transit Hosted Connection and attach the VPC tag to the connection.

- For a private VIF or private hosted connection, you can associate VPCs from a new region while editing the tag.

Note In Cisco vManage Release 20.9.1 and earlier releases, you cannot edit a VPC 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 **Amazon Web Services**.

   The available host VPCs 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 VPCs associated with the tag. • Choose additional regions from the drop-down list. • Click **X** to omit a region and associated VPCs from the tag.
Selected VPCs	This field shows the list of VPCs associated with the tag. • Choose additional VPCs from the drop-down list. • Click **X** to omit a VPC 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**	(Read only) Indicates whether the VPC 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 VPCs.

Note You cannot delete a VPC 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 **Amazon Web Services**.

   The available host VPCs 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 Direct Connect Public Hosted VIF to AWS from Interconnect Gateway

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments.
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Attach Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateway at a Megaport Location.
7. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails.

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 **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

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

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

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	Specify 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 addresses and prefixes you wish to advertise to AWS.
Segment	Choose the segment ID for this connection.

11. 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 VIF to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.

2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments.
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag AWS VPCs.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateway at a Megaport Location.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails.

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 **MEGAPORT**.



Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

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

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

VIF Type	Choose **Private**.

Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location. **Note** We recommend not to use any AWS GovCloud locations for non AWS GovCloud accounts.
Bandwidth	Specify 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. In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the 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. • Beginning with Cisco vManage Release 20.8.1: • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. • The custom subnet must be specified as /30. • The custom subnet should not conflict with 172.31.251.0/21. • The custom subnet must not conflict with the subnets used for other connections. **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	Cisco vManage Release 20.8.1 and earlier: Choose **VPC**. **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.

11. 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 Public Hosted Connection to AWS from Interconnect Gateway

Prerequisites

1. Associate Megaport 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 Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateway at a Megaport Location.
7. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport.

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 **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

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

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

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	Specify 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.

11. 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 Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments.
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag AWS VPCs.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateway at a Megaport Location.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails.

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 **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.

8. Click **Add Connection**.
9. Configure the following and click **Next**:

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

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

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. **Note** We recommend not to use any AWS GovCloud locations for non AWS GovCloud accounts.
Bandwidth	Specify 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. In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the 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. • Beginning with Cisco vManage Release 20.8.1: • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. • The custom subnet must be specified as /30. • The custom subnet should not conflict with 172.31.251.0/21. • The custom subnet must not conflict with the subnets used for other connections. **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	Cisco vManage Release 20.8.1 and earlier: Choose **VPC**. **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.

11. 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 Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments.
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and Tag AWS VPCs.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateway at a Megaport Location.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails.

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 **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

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

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

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. **Note** We recommend not to use any AWS GovCloud locations for non AWS GovCloud accounts.
Bandwidth	Specify 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. In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the 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. • Beginning with Cisco vManage Release 20.8.1: • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. • The custom subnet must be specified as /30. • The custom subnet should not conflict with 172.31.251.0/21. • The custom subnet must not conflict with the subnets used for other connections. **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. Click **Add Prefixes**. Enter the IPv4 CIDR prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard.

11. 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.



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

3. Associate Megaport Account with Cisco SD-WAN Manager.
4. Configure Global Settings for Interconnect Gateways.
5. Attach Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateway at a Megaport Location closest to your Cisco Catalyst SD-WAN branch location.

   For redundant connectivity to Google Cloud, create a pair of Interconnect Gateways in the Megaport fabric. For nonredundant connectivity, deploy an Interconnect Gateway at a Megaport location.
7. Create necessary network segments (see Segmentation Configuration Guide).
8. Associate Google Cloud Account with Cisco SD-WAN Manager.
9. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

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 **MEGAPORT**.
5. **Choose Interconnect Account**: choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. 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 releases: Cisco vManage Release 20.9.1 Choose a Google Cloud region.
VPC Network	Minimum supported releases: 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.

10. Configure the following settings for the primary virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the primary interconnect attachment.
Connection Name	Enter a unique name for the primary 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 virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the secondary interconnect attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary interconnect attachment.
Connection Name	Enter a unique name for the secondary 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 interconnect 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 virtual cross connect 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 Interconnect Connection to a Cloud Gateway In Google Cloud

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

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Associate Megaport Account with Cisco SD-WAN Manager.
3. Configure Global Settings for Interconnect Gateways.
4. Attach Megaport Template to Cisco Catalyst 8000v Instance.
5. Create Interconnect Gateway at a Megaport Location closest to your Cisco Catalyst SD-WAN branch location.

   Only redundant connectivity is supported on Google Cloud. You must create a pair of Interconnect Gateways in the Megaport fabric.
6. Create necessary network segments.
7. Associate Google Cloud Account with Cisco SD-WAN Manager.
8. Create a Google Cloud Gateway using the Multicloud workflow.
9. Ensure that you have the required license to create the connection. Without the required license, connection creation fails.

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 **MEGAPORT**.
5. **Choose Interconnect Account**: choose a Megaport 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. To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. 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.

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

PRIMARY	
Google Cloud Router	Primary Google Cloud router is autopopulated based on the selected Cloud Gateway.
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 for the interconnect attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network. • IC 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	Secondary Google Cloud router is autopopulated based on the selected Cloud Gateway.

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 interconnect 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 for the interconnect attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network. • IC Attachment Name: Enter a unique attachment name. • Secondary Zone: If you want to deploy this attachment on the secondary zone, check the checkbox.

11. Configure the following settings for the primary virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the primary interconnect attachment.
Connection Name	Enter a unique name for the primary connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

12. Configure the following settings for the secondary virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the secondary interconnect attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary interconnect attachment.
Connection Name	Enter a unique name for the secondary 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 interconnect attachment.

13. 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 virtual cross connect 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.

14. 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.

Field	Description
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.
(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 Megaport 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 Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateways at Megaport Location.

   For connectivity to Microsoft Azure, create a pair of Interconnect Gateways in the Megaport fabric. Redundant connectivity is the default and only supported configuration.
7. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

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 **MEGAPORT**.

5. **Choose Interconnect Account**: Choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. 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. Equinix ExpressRoutes are not supported in Cisco vManage Release 20.6.1 and Cisco vManage Release 20.7.1. • 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 **Megaport**. • 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**.

10. 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.

11. 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.

12. 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.

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. This task creates the following resources:

- virtual cross connects in the Megaport 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 Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments.
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag Microsoft Azure VNets.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateways at Megaport Location.

   For connectivity to Microsoft Azure, create a pair of Interconnect Gateways in the Megaport fabric. Redundant connectivity is the default and only supported configuration.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails.

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 **MEGAPORT**.
5. **Choose Interconnect Account**: choose a Megaport 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. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. 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. Equinix ExpressRoutes are not supported in Cisco vManage Release 20.6.1 and Cisco vManage Release 20.7.1. • 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 **Megaport**. • 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**.

10. 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.

11. 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.

12. 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.
	• Beginning with Cisco vManage Release 20.8.1:
	  • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.
	  • The custom subnet must be specified as /30.
	  • The custom subnet should not conflict with 172.31.251.0/21.
	  • The custom subnet must not conflict with the subnets used for other connections.

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. The same virtual WAN is attached to any subsequent connection to which you choose to attach a virtual WAN. Starting from Cisco vManage Release 20.8.1, Cisco SD-WAN Manager supports one vWAN per Microsoft Azure resource group per Microsoft Azure account. Once that vWAN is chosen and used as part of a vWAN connection, subsequent vWAN connections to the same Microsoft Azure resource group use the same vWan. The Microsoft Azure resource group is determined for the connection when the Express Route 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 Express Route 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.

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.

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

- virtual cross connects in the Megaport 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 Megaport 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.

Create Interconnect Between Interconnect Gateways

In Cisco SD-WAN Manager, you can create an interconnect between Interconnect Gateways at two or more Megaport locations. By doing so, you can link the Cisco Catalyst SD-WAN branch locations connected to these Interconnect Gateways via the Megaport fabric.

Prerequisites

For each Cisco Catalyst SD-WAN branch location to be connected through the Megaport fabric,

1. Associate Megaport 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 Megaport location.
5. Create an Interconnect Gateway at the Megaport 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.

6. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

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 **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the source Interconnect Gateway.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Edge**.
Provider	Choose **Megaport**. **Note** This field is not available from Cisco vManage Release 20.6.1.
Connection Name	Enter a unique name for the connection.
Interconnect Gateway	Choose destination Interconnect Gateway.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.

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.

Verify and Modify Configuration

View Interconnect Gateway and Connection Summary

On the **Interconnect** page, you can view a summary of Interconnect Gateways and connections that you have created. If you have not created any Interconnect Gateways, the 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.

View, Edit, or Delete Connections

View Connection Properties

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

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

Edit Connection Configuration

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
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 connection destination and connection type, if any. Configure the parameters as required.

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

Note You can modify the properties of active connections only.

Table 4: Editable Properties of Interconnect Connections to AWS

Field	Description	Applicable Connection Types
Bandwidth	Modify the connection bandwidth. Unit: Mbps.	Private and Public Hosted VIF
Segment	Minimum supported release: Cisco vManage Release 20.10.1 Choose a different segment ID for this connection.	All connections to AWS

Field	Description	Applicable Connection Types

Transit Gateway	Minimum supported release: Cisco vManage Release 20.10.1
	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
	• You can remove a transit gateway subject to the following conditions:
	  • The transit gateway that you wish to remove is not the only transit gateway associated with the connection.
	  • You remove VPC tags corresponding to the region served by the transit gateway in the same edit operation.
	• You cannot replace an existing transit gateway for a region with another transit gateway from the same region.
		Transit Hosted Connections

VPC Tags	Minimum supported release: Cisco vManage Release 20.10.1 Choose VPC tags to identify VPCs for which traffic must be routed through this connection.	• Private Hosted VIF and Private Hosted Connections with VPC attachments • Transit Hosted Connections
Allowed Prefixes	Minimum supported release: Cisco vManage Release 20.10.1 Click **Edit Prefixes**. Enter the IPv4 CIDR prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard. **Note** You can only add more 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 connnections, 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	Minimum supported release: Cisco vManage Release 20.10.1 Choose a different segment ID for this connection.	Private and Public (Microsoft) Peering Connections
BGP Advertise Prefix	Minimum supported release: Cisco vManage Release 20.10.1 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		

Field	Description	Applicable Connection Types
vNet	Minimum supported release: Cisco vManage Release 20.10.1 Choose VNet tags to identify the VNets for which traffic must be routed through this connection.	Private Peering Connections
vHub Settings	Minimum supported release: Cisco vManage Release 20.10.1 **a.** 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**.	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 the changes, click **Update** or **Save**.

Delete Connection

Note

- When you delete a connection to AWS, Cisco SD-WAN Manager deletes only the VIF, the virtual private gateway, and the route table that were created while establishing the connection.
- While creating a connection to AWS, if you created a direct connect gateway or a transit gateway, from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can optionally delete the direct connect gateway and transit gateway.
- When you delete a connection to Microsoft Azure, Cisco SD-WAN Manager deletes any ExpressRoutes, VNet gateways, ExpressRoute gateways, and virtual hubs created for the connection only if these elements are not used in other connections.

  From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can optionally choose to delete Express-Route and Virtual Wan at the time of deleting a connection, or manage these Azure resources as required. When you delete a GCP connection, you can optionally select to delete the Google Cloud Router, or manage these resources as required.

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 delete a connection, click **...** for the desired connection and click **Delete**. Confirm that you wish to delete the connection.

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, click **…** for the desired Interconnect Gateway.
   - 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.

Note You can delete an Interconnect Gateway only if there are no connections associated with it.

Deleting the Interconnect Gateway disconnects the branch location from the Megaport 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. In the table, click **...** for the desired interconnect account.

   - 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 **User Name** and **Password** 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

The fabric of the SDCI provider, Megaport, incorporates audit management support that assists you in verifying the synchronization of the cloud connection state with the Cisco SD-WAN Manager state. The audit process scans the provider resources, interconnect gateways, and connections to the cloud. In the **Audit** screen, when there are errors, they are displayed and if there are no errors, the status is displayed as **In Sync**.

Note In the Cisco vManage Release 20.11.1, the audit management feature is supported only on the Megaport fabric.

Accessing the Audit Report

1. In **Cloud OnRamp for Multicloud**, navigate to the **Interconnect** tab.
2. In the **Intent Management** pane, click **Audit**.
3. In **Intent Management- Audit**, under **Interconnect Gateways**, choose an **Interconnect Provider** from the drop-down list.

4. Choose a **Destination Type** and choose a **Cloud Provider** from the drop-down list when the Destination Type is **cloud** to view the desired audit report.

Note Choose **Destination Type** as **cloud** or **edge** depending on the requirement.

Note The following are the different connections that are scanned and reported by the audit report:

- **Edge Gateway** indicates that there are edge gatways created using Cisco SD-WAN Manager workflows with the respective details.
- **Edge Connections** indicates that there are edge connections created using Cisco SD-WAN Manager workflows with the respective details.
- **Unknown Edge Gateways** indicates that Cisco SD-WAN Manager is unable to recognize certain edge gateways.
- **Unknown Edge Connections** indicates that Cisco SD-WAN Manager is unable to recognize certain edge connections.

The following are the statuses that are displayed in the audit report:

- **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 Megaport

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.

Scenario	Resolution
While attempting to create an Interconnect Gateway, the device list is empty	Verify that the devices has been assigned a template. (Recommended template: *Default_MEGAPORT_ICGW_C8000V_Template_V01*)
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.
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.
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 Megaport*. **5.** Verify permissions of the Interconnect Provider account and the AWS account.

Scenario	Resolution
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.
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.