Configuration

Action Parameters - Data Policy

Table 1: Feature History

Feature Name	Release Information	Description
Path Preference Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature extends to Cisco IOS XE Catalyst SD-WAN devices, support for selecting one or more local transport locators (TLOCs) for a policy action.
Traffic Redirection to SIG Using Data Policy	Cisco IOS XE Release 17.4.1 Cisco vManage Release 20.4.1	You can create a data policy where you can selectively define an application list along with other existing match criteria in the data-policy to redirect the application traffic to a Secure Internet Gateway (SIG).

Feature Name	Release Information	Description
Next Hop Action Enhancement in Data Policies	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature enhances match action conditions in a centralized data policy for parity with the features configured on Cisco IOS XE Catalyst SD-WAN devices. When you are setting up next-hop-loose action, this feature helps to redirect application traffic to an available route when next-hop address is not available.
Traffic Redirection to SIG Using Data Policy: Fallback to Routing	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	With this feature, you can configure internet-bound traffic to be routed through the Cisco Catalyst SD-WAN overlay, as a fallback mechanism, when all SIG tunnels are down.
Log Action for both Localized and Centralized Data Policies	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables you to set a log action parameter for data policy, application route policy, and localized policy while configuring data policies on Cisco IOS XE Catalyst SD-WAN devices. The log parameter allows packets to get logged and generate syslog messages. Logs are exported to an external syslog server every five minutes when a flow is active. You can control policy logs as per the configured rate using the command **policy log-rate-limit**.

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped. Then, you can associate parameters with accepted packets.

In the CLI, you configure the action parameters with the **policy data-policy vpn-list sequence action** command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

Action Condition	Description
Click **Accept**	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.
Cflowd	Enables cflowd traffic monitoring.
Counter	Counts the accepted or dropped packets. Specifies the name of a counter. Use the **show policy access-lists counters** command on the Cisco IOS XE Catalyst SD-WAN device.
Click **Drop**	Discards the packet. This is the default action.

Action Condition	Description
Log	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1 Click **Log** to enable logging. When (DP, AAR or ACL) data policy packets are configured with log action, logs generated and logged to syslog. Due to the global **log-rate-limit**, not all logs are logged. A syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active. For information on **policy log-rate-limit** CLI, see **policy log-rate-limit** command in the Cisco Catalyst SD-WAN Qualified Command Reference Guide.
Redirect DNS	Redirects DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions. For an inbound policy, **redirect-dns host** allows the DNS response to be correctly forwarded back to the requesting service VPN. For an outbound policy, specify the IP address of the DNS server. **Note** When you upgrade to releases later than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you must configure redirect DNS through **nat use-vpn 0** to redirect DNS to Direct Internet Interface (DIA). **Note** You can set only local TLOC preferences with redirect-dns as actions on the same sequence, but not remote TLOC. **Note** You cannot configure Redirect DNS and SIG at the same time.
TCP Optimization	Fine-tune TCP to decrease round-trip latency and improve throughout for matching TCP traffic.
Secure Internet Gateway	Redirect application traffic to a SIG **Note** Before you apply a data policy for redirecting application traffic to a SIG, you must have configured the SIG tunnels. For more information on configuring Automatic SIG tunnels, see Automatic Tunnels . For more information on configuring Manual SIG tunnels, see Manual Tunnels. Check the **Fallback to Routing** check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down. This option is introduced in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1.

Note On Cisco IOS XE Catalyst SD-WAN devices, all the ongoing optimized flows are dropped when the TCP Optimization is removed.

Then, for a packet that is accepted, the following parameters can be configured:

Action Condition	Description
Cflowd	Enables cflowd traffic monitoring.
NAT Pool or **NAT VPN**	Enables NAT functionality, so that traffic can be redirected directly to the internet or other external destination.
DSCP	DSCP value. The range is 0 through 63.
Forwarding Class	Name of the forwarding class.
Local TLOC	Enables sending packets to one of the TLOCs that matches the color and encapsulation. The available colors are: 3g, biz-internet, blue, bronze, custom1,custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red and silver. The encapsulation options are: **ipsec** and **gre**. By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the **restrict** option. By default, encapsulation is **ipsec**.
Next Hop	Sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, the **Use Default Route when Next Hop is not available** field is available next to the **Next Hop** action parameter. This option is available only when the sequence type is **Traffic Engineering** or **Custom**, and the protocol is either **IPv4** or **IPv6**, but not both.
Policer	Applies a policer. Specifies the name of policer configured with the **policy policer** command.

Action Condition	Description
Service	Specifies a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**,**netsvc3**, **netsvc4** TLOC list is configured with a **policy lists tloc-list** list. Configure the services themselves on the Cisco IOS XE Catalyst SD-WAN devices that are collocated with the service devices, using the **vpn service** command.
TLOC	Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic.
Click **Accept**, then action **VPN**.	Set the VPN that the packet is part of. The range is 0 through 65530.

Note Data policies are applicable on locally generated packets, including routing protocol packets, when the match conditions are generic.

Example configuration:

```
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

In such situations, it may be necessary to add a sequence in the data policy to escape the routing protocol packets. For example to skip OSPF, use the following configuration:

```
sequence 20
   match
    source-ip 10.0.0.0/8
    protocol  89
   action accept
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

The following table describes the IPv4 and IPv6 actions.

Table 2:

IPv4 Actions	IPv6 Actions
drop, dscp, next-hop (from-service only)/vpn, count, forwarding class, policer (only in interface ACL), App-route SLA (only)	N/A
App-route preferred color, app-route sla strict, cflowd, nat, redirect-dns	N/A
N/A	drop, dscp, next-hop/vpn, count, forwarding class, policer (only in interface ACL) App-route SLA (only), App-route preferred color, app-route sla strict
policer (DataPolicy), tcp-optimization, fec-always,	policer (DataPolicy)
tloc, tloc-list (set tloc, set tloc-list)	tloc, tloc-list (set tloc, set tloc-list)
App-Route backup-preferred color, local-tloc, local-tloc-list	App-Route backup-preferred color, local-tloc, local-tloc-list

Access the Software Upgrade Workflow

Table 3: Feature History

Feature Name	Release Information	Description
Software Upgrade Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1 Cisco SD-WAN Release 20.8.1	You can now upgrade software images on edge devices using the **Workflows** menu in Cisco SD-WAN Manager.
Schedule the Software Upgrade Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1 Cisco SD-WAN Release 20.9.1	Upgrade the software of Cisco edge devices using a **scheduler** which helps in scheduling the upgrade process at your convenience.
Software Upgrade Workflow Support for Additional Platforms	Cisco vManage Release 20.9.1	Added support for Cisco Enterprise NFV Infrastructure Software (NFVIS) and Cisco Catalyst Cellular Gateways.
Software Upgrade Scheduling Support for Additional Platforms	Cisco vManage Release 20.10.1	Added support for software upgrade scheduling for Cisco Catalyst Cellular Gateways.

Before You Begin

To check if there is an in-progress software upgrade workflow:

From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon. Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

Access the Software Upgrade Workflow

1. In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

Note In the Cisco vManage Release 20.8.1, the **Workflow Library** is titled **Launch Workflows**.

2. Start a new software upgrade workflow: **Library** > **Software Upgrade**.

   OR

   Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.

3. Follow the on-screen instructions to start a new software upgrade workflow.

Note Click **Exit** to exit from an in-progress software upgrade workflow. You can resume the in-progress workflow at your convenience.

Note In a multi-node cluster setup, if the control connection switches to a different node during a device upgrade from Cisco SD-WAN Manager, the upgrade may be impacted due to NetConf session timeout. The device then establishes control connection to a different node. You need to re-trigger the upgrade activity.

Verify the Status of the Software Upgrade Workflow

To check the software upgrade workflow status:

1. From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon.

   Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

2. Click the + icon to view the details of a task.

   Cisco SD-WAN Manager opens a pane displaying the status of the task and details of the device on which the task was performed.

Add a Cisco Catalyst SD-WAN Manager Server to a Cluster

Table 4: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Manager Persona-based Cluster Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	You can add Cisco SD-WAN Manager servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

The following sections provide information about adding a Cisco SD-WAN Manager server to a cluster in various Cisco SD-WAN Manager releases.

Add a Cisco SD-WAN Manager Server to a Cluster for Releases Before Cisco vManage Release 20.6.1

To add a new Cisco SD-WAN Manager server to a cluster for releases before Cisco vManage Release 20.6.1, perform the following steps on the primary Cisco SD-WAN Manager server.

Before you begin, ensure that the default IP address of the Cisco SD-WAN Manager server has been changed to an out-of-band IP address as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 20.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **Add vManage**.

   The **Edit vManage** window opens.
3. In the **vManage IP Address** field, select an IP address to assign to the Cisco SD-WAN Manager server.
4. Enter the username and password for logging in to the Cisco SD-WAN Manager server.
5. Enter the IP address of the Cisco SD-WAN Manager server that you are adding to the cluster.
6. Specify the username and password for the new Cisco SD-WAN Manager server.
7. Select the services to be run on the Cisco SD-WAN Manager server. You can select from the services listed below. Note that the **Application Server** field is not editable. The Cisco SD-WAN Manager Application Server is the local Cisco SD-WAN Manager HTTP web server.
   - Statistics Database: Stores statistics from all the Cisco Catalyst SD-WAN devices in the network.
   - Configuration Database: Stores all the device and feature templates and configurations for all the Cisco Catalyst SD-WAN devices in the network.
   - Messaging Server: Distributes messages and shares state among all the Cisco SD-WAN Manager cluster members.
8. Click **Add**.

   The Cisco SD-WAN Manager server that you just added reboots before joining the cluster.

Note

- In a cluster, we recommend that you run at least three instances of each service.
- When you add the first two compute or compute+data nodes to the cluster, the host node's application-server is unavailable. The following message is displayed on the host node's GUI, before the application-server shuts down in the host node: `\Node added to the cluster. The operation may take up to 30 minutes and may cause application-server to restart in between. Once the application server is back online, the post cluster operation progress can be viewed under tasks pop-up\.`
- Starting Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, ensure that you disable the **HTTP/HTTPs Proxy** option in the Cisco SD-WAN Manager settings, before adding a node to the cluster.

Add a Cisco SD-WAN Manager Server to a Cluster for Cisco vManage Release 20.6.1 and Later Releases

From Cisco vManage Release 20.6.1, a cluster supports any of the following deployments of nodes:

- Three Compute+Data nodes
- Three Compute+Data nodes and three Data nodes

Note DATA nodes should be added only after 3 node cluster with CONFIG+DATA is added.

- Three Compute nodes and three Data nodes (supported only in an upgrade from an existing deployment)

If you require a different combination of nodes, contact your Cisco representative.

To add a Cisco SD-WAN Manager server to a cluster from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on a Compute+Data node or a Compute node. Performing this procedure on a Data node is not supported because a Data node does not run all the services that are required for the addition.

Do not add a server that was a member of the cluster and then removed from the cluster. If you need to add that server to the cluster, bring up a new VM on that server to be used as the node to add.

Before you begin, ensure that the default IP address of the Cisco SD-WAN Manager server has been changed to an out-of-band IP address, as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 20.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management page** window appears. The table on this window shows the Cisco SD-WAN Manager servers that are in the cluster.

2. Click **Add vManage**.

   The **Add vManage** dialog box opens.

Note If the **Edit vManage** dialog box opens, configure an out-of-band IP address for the server, as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 20, and then repeat this procedure for adding a server.

3. In the **Add vManage** dialog box, perform the following actions:

   a. Click the **Node Persona** option (**Compute+Data**, **Compute**, or **Data**) that corresponds to the persona that has been configured for the server.

      You can determine the persona of a server by logging in to the server and looking at the persona display on the **Administration** > **Cluster Management** window. If you choose an incorrect persona, a message displays the persona that you should choose.

   b. From the **vManage IP Address** drop-down list, choose the IP address of the server to be added to the cluster.

   c. In the **Username** field, enter the user name for logging in to the server.

   d. In the **Password** field, enter the password for logging in to the server.

   e. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

      Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on one Cisco SD-WAN Manager server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.

      If you enabled Cisco SD-AVC for this server when you changed its IP address, the **Enable SD-AVC** check box is checked by default.

   f. Click **Add**.

   g. To confirm, click **OK**.

      The dialog box indicates that the services will restart, and that the existing metadata and other information that is not required when the server joins the cluster will be deleted from the server.

      When you click **OK**, the system starts the server add operation. The **Cluster Management** window displays the tasks that the system performs as it adds the server.

      As part of this operation, the system checks the compatibility of the server that you are adding. This check ensures that the server has sufficient disk space, and that the persona that you specified matches the persona of the node.

      After the server is added, the system performs a cluster sync operation, which rebalances the services in the cluster. Then the Cisco SD-WAN Manager servers in the cluster restart.

Add Tags to Devices Using Cisco SD-WAN Manager

Table 5: Feature History

Feature Name	Release Information	Description
User-Defined Device Tagging	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can add tags to devices using Cisco SD-WAN Manager. You can use the tags for grouping, describing, finding, or managing devices.
Enhancements to User-Defined Device Tagging	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	Device tagging has the following new functionality: • When you add devices to a configuration group using rules, you can choose **Match All** or **Match Any**. • You can use **Starts With** and **Ends With** operator conditions when you add devices to a configuration group using rules. In addition, the button formerly called **Add New Tag** is now **Create New Tag**.

You can add tags to devices in one of the following ways:

Use the Devices Window

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List** and choose a device.
3. Click **Add Tags**
4. Choose a tag from the list of existing tags or click **Create New Tag** to create a new tag.

   In Cisco vManage Release 20.11.1 and earlier, this was called **Add New Tag**.
5. Click **Apply**.

   The specified tag is added to the device.

Use the Quick Connect Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Launch Workflows**.
2. Click **Quick Connect**.

   The **Quick Connect** workflow starts.
3. Click **Add Tags**
4. Follow the instructions provided in the workflow.
5. Tag the devices.

The specified tag is added to the device.

Note You can edit the tags that are currently associated with a device by either adding new tags or removing unwanted tags.

Add Cisco Catalyst SD-WAN Validator to the Overlay Network

After you create a minimal configuration for Cisco SD-WAN Validator, you must add it to overlay network by making Cisco SD-WAN Manager aware of Cisco SD-WAN Validator. When you add Cisco SD-WAN Validator, a signed certificate is generated and is used to validate and authenticate the orchestrator.

Add Cisco Catalyst SD-WAN Validator and Generate Certificate

To add Cisco SD-WAN Validator to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, from **Add Controller** drop-down, select **vBond**.
3. In the **Add vBond** window:
   a. Enter the vBond management IP address.
   b. Enter the username and password to access Cisco SD-WAN Validator.
   c. Choose the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   d. Click **Add**.

Cisco SD-WAN Manager generates the CSR, retrieves the generated certificate, and automatically installs it on Cisco SD-WAN Validator. The new controller device is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on Cisco SD-WAN Validator:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose the new device listed, and check in the Certificate Status column to ensure that the certificate has been installed.

Add Cisco Catalyst SD-WAN Controller to the Overlay Network

After you create a minimal configuration for Cisco SD-WAN Controller, you must add it to an overlay network by making Cisco SD-WAN Manager aware of the controller. When you add Cisco SD-WAN Controller, a signed certificate is generated and is used to validate and authenticate the controller.

Cisco SD-WAN Manager can support up to 20 Cisco SD-WAN Controllers in the network.

Add a Cisco Catalyst SD-WAN Controller and Generate Certificate

To add a Cisco SD-WAN Controller to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and from the **Add Controller** drop-down menu, choose **vSmart**.
3. In the **Add vSmart** window:
   a. Enter the system IP address of Cisco SD-WAN Controller.
   b. Enter the username and password to access Cisco SD-WAN Controller.
   c. Choose the protocol to use for control-plane connections. The default is DTLS.
   d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.
   e. Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   f. Click **Add**.

Cisco SD-WAN Manager automatically generates the CSR, retrieves the generated certificate, and installs it on Cisco SD-WAN Controller. The new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on a Cisco SD-WAN Controller:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose the new controller listed and check in the Certificate Status column to ensure that the certificate has been installed.

Note If Cisco SD-WAN Controller and Cisco SD-WAN Validator have the same system IP addresses, they do not appear in Cisco SD-WAN Manager as devices or controllers. The certificate status of Cisco SD-WAN Controller and Cisco SD-WAN Validator is also not displayed. However, the control connections still successfully comes up.

What's Next

See *Deploy the vEdge Routers*.

Apply Policy to a Zone Pair

Table 6: Feature History

Feature Name	Release Information	Description
Self Zone Policy for Zone-Based Firewalls	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows you to define firewall policies for incoming and outgoing traffic between a self zone of an edge router and another zone. When a self zone is configured with another zone, the traffic in this zone pair is filtered as per the applied firewall policy.

Note For IPSEC overlay tunnels in Cisco Catalyst SD-WAN, if a self zone is chosen as a zone pair, firewall sessions are created for SD-WAN overlay BFD packets if inspect action is configured for UDP.

However, for GRE overlay tunnels, if you chose a self zone as a zone pair with the inspect action of protocol 47, firewall sessions are created only for TCP, UDP, ICMP packets; but not BFD packets.

Warning Control connections may be impacted when you configure drop action from self-zone to VPN0 and vice versa. This applies for DTLS/TLS, BFD packets, and IPsec overlay tunnel.

To apply policy to a zone pair:

1. Create security policy using Cisco SD-WAN Manager. For information see, Start the Security Policy Configuration Wizard.
2. Click **Apply Zone-Pairs**.
3. In the **Source Zone** field, choose the zone that is the source of the data packets.
4. In the **Destination Zone** field, choose the zone that is the destination of the data packets.

Note You can choose self zone for either a source zone or a destination zone, not both.

5. Click the plus (+) icon to create a zone pair.
6. Click **Save**.
7. At the bottom of the page, click **Save Firewall Policy** to save the policy.
8. To edit or delete a firewall policy, click the **...**, and choose the desired option.
9. Click **Next** to configure the next security block in the wizard. If you do want to configure other security features in this policy, click **Next** until the Policy Summary page is displayed.

Note When you upgrade to Cisco SD-WAN Release 20.3.3 and later releases from any previous release, traffic to and from a service VPN IPSEC interface is considered to be in the service VPN ZBFW zone and not a VPN0 zone. This could result in the traffic getting blackholed, if you allow traffic flow only between service VPN and VPN0 and not the intra service VPN.

You have to make changes to your ZBFW rules to accommodate this new behavior, so that the traffic flow in your system is not impacted. To do this, you have to modify your intra area zone pair to allow the required traffic. For instance, if you have a policy which has the same source and destination zones, you have to ensure the zone-policy allows the required traffic.

Attach and Detach a Device Template

To configure a device on the network, you attach a device template to the device. You can attach only one device template to a device, so the template—whether you created it by consolidating individual feature templates or by entering a CLI text-style configuration—must contain the complete configuration for the device. You cannot mix and match feature templates and CLI-style configurations.

On Cisco IOS XE Catalyst SD-WAN devices in the overlay network, you can perform the same operations, in parallel, from one or more Cisco SD-WAN Manager servers. You can perform the following template operations in parallel:

- Attach a device template to devices
- Detach a device template from a device
- Change the variable values for a device template that has devices attached to it

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. Then when you click **Update** > **Configure Devices**, all other template operations—including attach devices, detach devices, and edit device values—are locked on all Cisco SD-WAN Manager servers until the update operation completes. This means that a user on another Cisco SD-WAN Manager server cannot perform any template operations until the update completes.
- You can perform the attach and detach device template operations on different devices, from one or more Cisco SD-WAN Manager servers, at the same time. However, if any one of these operations is in progress on one Cisco SD-WAN Manager server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

Note You need to recreate the feature templates as the templates created prior to Cisco vManage Release 20.5 fails when attached to the device.

If the device being configured is present and operational on the network, the configuration is sent to the device immediately and takes effect immediately. If the device has not yet joined the network, the pushing of the configuration to the device is scheduled. When the device joins the network, Cisco SD-WAN Manager pushes the configuration immediately after it learns that the device is present in the network.

Attach a Device Template to Devices

You can attach the same templates to multiple devices, and you can do so simultaneously, in a single operation.

To attach a device template to one or more devices:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Attach Devices**. The **Attach Devices** dialog box opens with the **Select Devices** tab selected
4. In the **Available Devices** column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
5. Click the arrow pointing right to move the device to the **Selected Devices** column on the right.
6. Click **Attach**.
7. If the template contains variables, enter the missing variable values for each device you selected in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking **...** and **Edit Device Template**. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
   - Click **Import File** to upload a CSV file that lists all the variables and defines each variable's value for each device.
8. Click **Update**
9. Click **Next**.

   If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.
10. In the left pane, select the device, to preview the configuration that is ready to be pushed to the device. The right pane displays the device's configuration and the **Config Preview** tab is selected. Click the **Config Diff** tab to view the differences between this configuration and the configuration currently running on the device, if applicable. Click the **Back** button to edit the variable values entered in the previous screen.
11. If you are attaching a Cisco IOS XE Catalyst SD-WAN device, click **Configure Device Rollback Timer** to configure the time interval at which the device rolls back to its previous configuration if the router loses its control connection to the overlay network. **The Configure Device Rollback Time** dialog box is displayed.
    a. From the **Devices** drop-down list, select a device.
    b. To enable the rollback timer, in the **Set Rollback slider**, drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.

c. To disable the rollback timer, click the **Enable Rollback** slider. When you disable the timer, the Password field dialog box opens. Enter the password that you used to log in to Cisco SD-WAN Manager.

d. In the **Device Rollback Time slider**, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.

e. To exclude a device from the rollback timer setting, click **Add Exception** and select the devices to exclude.

f. The table at the bottom of the **Configure Device Rollback Time** dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the **Trash** icon from the device name.

g. Click **Save**.

12. Click **Configure Devices** to push the configuration to the devices. The **Status** column displays whether the configuration was successfully pushed. Click the right angle bracket to display details of the push operation.

Export a Variables Spreadsheet in CSV Format for a Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Export CSV**.

Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server

When you start Cisco SD-WAN Manager for the first time, the default IP address of the Cisco SD-WAN Manager server is shown as localhost. Before you can add a new Cisco SD-WAN Manager server to a cluster, you must change the localhost address of the primary Cisco SD-WAN Manager server to an out-of-band IP address. (From Cisco vManage Release 20.6.1, the primary Cisco SD-WAN Manager server has the Compute+Data persona.) Servers in the cluster use this out-of-band IP address to communicate with each other.

If you need to change the out-of-band IP address in the future, contact your Cisco support representative.

Cluster interconnection between Cisco SD-WAN Manager servers requires that each of the servers be assigned a static IP address. We recommend that you do not use DHCP to assign IP addresses to Cisco SD-WAN Manager servers that are to be a part of a cluster. Configure the IP address on a nontunnel interface in VPN 0.

Before you configure the cluster IP address of a Cisco SD-WAN Manager server, ensure that out-of-band IP addresses have been configured on VPN0 for its server interfaces. This configuration typically is done when

the server is provisioned. The port type for an out-of-band IP address must be **service** for the IP address to be available for assigning to a Cisco SD-WAN Manager server.

Note From Cisco vManage Release 20.11.1, some alarms display the hostname as **localhost** during the cluster setup for the first time as the system-ip/hostname is not configured in Cisco SD-WAN Manager. When the system-ip/hostname is configured, the alarms display the correct hostname.

Configure the IP Address for Releases Before Cisco vManage Release 20.6.1

Configure the IP address of a Cisco SD-WAN Manager server before you add the server to the cluster. To do so for releases before Cisco vManage Release 20.6.1, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **Add vManage**.

   The **Edit vManage** dialog box opens.
3. From the **vManage IP Address** drop-down list, choose an IP address to assign to the Cisco SD-WAN Manager server.
4. Enter the user name and password for logging in to the Cisco SD-WAN Manager server.
5. Click **Update**.

The Cisco SD-WAN Manager server reboots and displays the **Cluster Management** window.

Configure the IP Address for Cisco vManage Release 20.6.1 and Later Releases

Configure the IP address of a Cisco SD-WAN Manager server before you add the server to the cluster. To do so from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on the primary Cisco SD-WAN Manager server (which has the Compute+Data persona).

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management** window is displayed. The table on this window lists the Cisco SD-WAN Manager servers that are in the cluster.
2. Click **...** adjacent to the Cisco SD-WAN Manager server to configure and click **Edit**.

   The **Edit vManage** dialog box is displayed.
3. In the **Edit vManage** dialog box, perform the following actions.

Note You cannot change the persona of a server. So the Node Persona options are disabled.

   a. From the **vManage IP Address** drop-down list, choose an out-of-band static IP address to assign to the server.
   b. In the **Username** field, enter the user name for logging in to the server.
   c. In the **Password** field, enter the password for logging in to the server.

d. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on only one Cisco SD-WAN Manager server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.

Note If Cisco SD-WAN Manager is set up as a cluster and the cluster crashes as a result of a reboot or upgrade, the connection to the edge device is reset and the custom app ceases to function.

To resolve this and to resume operation, redefine the custom application name with a new, unique name. For more information to define custom applications, see the Define Custom Applications Using Cisco Catalyst SD-WAN Manager chapter of the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

e. Click **Update**.

The server reboots and displays the **Cluster Management** window.

Change Configuration Modes

A device can be in either of these configuration modes:

- Cisco SD-WAN Manager mode–A template is attached to the device and you cannot change the configuration on the device by using the CLI.
- CLI mode – No template is attached to the device and the device can be configured locally by using the CLI.

When you attach a template to a device from Cisco SD-WAN Manager, it puts the device in Cisco SD-WAN Manager mode. You can change the device back to CLI mode if needed to make local changes to its configuration.

To toggle a router from Cisco SD-WAN Manager mode to CLI mode:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List**, and select a device.
3. Click the **Change Mode** drop-down list and select **CLI mode**.

Note Starting from Cisco IOS XE SD-WAN Release 17.11.1a, click the **...** icon adjacent to the device that you want to change from Cisco SD-WAN Manager mode to the CLI mode and click **Config Lock (Provision Device)**.

You can use the **Config Lock (Provision Device)** only if a template is attached to a device.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

To toggle a controller device from Cisco SD-WAN Manager mode to CLI mode:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select a device.
3. Click the **Change Mode** drop-down list.
4. Select **CLI mode** and then select the device type. The **Change Mode - CLI** window opens.
5. From the **vManage mode** pane, select the device and click the right arrow to move the device to the **CLI mode** pane.
6. Click **Update to CLI Mode**.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

Note Starting from Cisco IOS XE SD-WAN Release 17.11.1a, click the **...** icon adjacent to the device that you want to change from Cisco SD-WAN Manager mode to the CLI mode and click **Config Lock (Provision Device)**.

You can use the **Config Lock (Provision Device)** only if a template is attached to a device.

Clone Service Groups

Table 7: Feature History

Feature Name	Release Information	Description
Clone Service Groups in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can easily create copies of service groups, download, and upload service group configuration properties using Cisco SD-WAN Manager.

When you clone or create copies of service chains, remember the following:

- Cisco SD-WAN Manager copies all configuration information of a service group to a cloned service group regardless of whether the cloned service group is attached to a cluster.
- Verify the CSV file and ensure that configuration information has a matching service group name during CSV file upload. Otherwise, an unmatched service group name can result in an error message during CSV file upload.
- To get an updated list of service group configuration values, always download service group configuration properties from the service group design view.

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

Step 2 Click **Service Group**.

The service group configuration page appears and all the service groups are displayed.

Step 3 For the desired service group, click **...** and choose **Clone Service Group**.

A clone of the original service group appears in the service group design view. Note the following points:

- By default, the cloned service group name and VM names are suffixed with a unique string.
- To view any VM configuration, click a VM in service chains.
- Cisco SD-WAN Manager marks the service chains that require configuration as **Unconfigured**, next to the edit button of the service chain.

Step 4 Modify the service group name, if required. Provide a description for the service group.

Step 5 To configure a service chain, use one of the following methods:

- Click the edit button for a service chain, enter the values, and then click **Save**.
- Download the configuration values from a CSV file, modify the values, upload the file, and then click **Save**. See Steps 6, 7, 8 on how to download, modify, and upload a CSV file.

The cloned service group appears on the service group configuration page. You can now download the updated service group configuration values.

Step 6 To download the cloned service group configuration values, do one of the following:

Note The download and upload of a CSV file is supported for creating, editing, and cloning of the service groups that aren't attached to a cluster.

- On the service group configuration page, click a cloned service group, click **More Actions** to the right of the service group, and choose **Download Properties (CSV)**.
- In the service group design view, click **Download CSV** in the upper right corner of the screen.

Cisco SD-WAN Manager downloads all configuration values of the service group to an Excel file in CSV format. The CSV file can consist of multiple service groups and each row represents configuration values for one service group. To add more rows to the CSV file, copy service group configuration values from existing CSV files and paste them in this file.

For example, ServiceGroup1_Clone1 that has two service chains with one VM in each of the service chains is represented in a single row.

Note In the Excel file, the headers and their representation in the service chain design view is as follows:

- sc1/name represents the name of the first service chain.
- sc1/vm1/name represents the name of the first VNF in the first service chain.
- sc2/name represents the name of the second service chain.
- sc2/vm2/name represents the name of the second VNF in the second service chain.

Step 7 To modify service group configuration values, do one of the following:

- To modify the service group configuration in the design view, click a cloned service group from the service group configuration page.

  Click any VM in service chains to modify the configuration values, and then click **Save**.

- To modify the service group configuration using the downloaded Excel file, enter the configuration values in the Excel file manually. Save the Excel file in CSV format.

Step 8 To upload a CSV file that includes all the configuration values of a service group, click a service group in the service group configuration page, and then click **Upload CSV** from the right corner of the screen.

Click **Browse** to choose a CSV file, and then click **Upload**.

You can view the updated values displayed for the service group configuration.

Note You can use the same CSV file to add configuration values for multiple service groups. But, you can update configuration values for a specific service group only, when uploading a CSV file using Cisco SD-WAN Manager.

Step 9 To know the representation of service group configuration properties in the CSV file and Cisco SD-WAN Manager design view, click a service group from the service group configuration page.

Click **Show Mapping Names**.

A text appears next to all the VMs in the service chains. Cisco SD-WAN Manager displays this text after mapping it with the configuration properties in the CSV file.

Cisco Catalyst SD-WAN Multitenancy

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

Table 8: Feature History

Feature Name	Release Information	Description
Enhanced Cisco Catalyst SD-WAN Manager Dashboard for Multitenancy	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature is enhanced to support consistent user experience in tenant and service providers dashboard. The Cisco Catalyst SD-WAN Manager dashboard provides visibility into the available resources on shared devices.

Enable Multitenancy on Cisco SD-WAN Manager

Prerequisites

Do not migrate an existing single-tenant Cisco SD-WAN Manager into multitenant mode, even if you invalidate or delete all devices from the existing Cisco SD-WAN Manager. Instead, download and install a new software image of Cisco vManage Release 20.6.1 or a later release.

Note After you enable multitenancy on Cisco SD-WAN Manager, you cannot migrate it back to single tenant mode.

1. Launch Cisco SD-WAN Manager using the URL `https://vmanage-ip-address:port`. Log in as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
3. In the **Tenancy Mode** bar, click the **Edit**.
4. In the **Tenancy** field, click **Multitenant**.
5. In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).
6. Enter a **Cluster Id** (for example, cluster-1 or 123456).
7. Click **Save**.
8. Click **Proceed** to confirm that you want to change the tenancy mode.

   Cisco SD-WAN Manager reboots in multitenant mode and when a provider user logs in to Cisco SD-WAN Manager, the provider dashboard appears.

Note The **Domain** and **Cluster Id** values created in steps 5 and 6 serve as the Provider FQDN. Ensure these values conform to current DNS naming conventions. You can not modify these values after the configuration is saved. To change these values, a new Cisco SD-WAN Manager cluster need to be deployed. For more details on Provider and Tenant DNS requirements, see step 3.d in Add a New Tenant.

Add Cisco SD-WAN Controller to Cisco SD-WAN Multitenant Deployment

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
3. Click **Controllers**.
4. Click **Add Controller** and click **vSmart**.
5. In the **Add vSmart** dialog box, do the following:
   a. In the **vSmart Management IP Address** field, enter the system IP address of the Cisco SD-WAN Controller.
   b. Enter the **Username** and **Password** required to access the Cisco SD-WAN Controller.

c. Select the protocol to use for control-plane connections. The default is **DTLS**.

   If you select **TLS**, enter the port number to use for TLS connections. The default is 23456.

d. Check the **Generate CSR** check box for Cisco SD-WAN Manager to create a Certificate Signing Request.

e. Click **Add**.

6. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

   For the newly added Cisco SD-WAN Controller, the **Operation Status** reads **CSR Generated**.

   a. For the newly added Cisco SD-WAN Controller, click **More Options** icon and click **View CSR**.

   b. Submit the CSR to the Certificate Authority (CA) and obtain a signed certificate.

7. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

8. Click **Install Certificate**.

9. In the **Install Certificate** dialog box, paste the **Certificate Text** or click **Select a file** upload the certificate file. Click **Install**.

   Cisco SD-WAN Manager installs the certificate on the Cisco SD-WAN Controller. Cisco SD-WAN Manager also sends the serial number of the certificate to other controllers.

   On the **Configuration** > **Certificates** page, the **Operation Status** for the newly added Cisco SD-WAN Controller reads as **vBond Updated**.

   On the **Configuration** > **Devices** page, the new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details. The **Mode** is set to **CLI**.

10. Change the mode of the newly added Cisco SD-WAN Controller to **vManage** by attaching a template to the device.

    a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

    b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

    c. Find the template to be attached to the Cisco SD-WAN Controller.

    d. Click **...**, and click **Attach Devices**.

    e. In the **Attach Devices** dialog box, move the new controller to the **Selected Device** list and click **Attach**.

    f. Verify the **Config Preview** and click **Configure Devices**.

Cisco SD-WAN Manager pushes the configuration from the template to the new controller.

In the **Configuration** > **Devices** page, the **Mode** for the Cisco SD-WAN Controller shows **vManage**. The new Cisco SD-WAN Controller is ready to be used in your mutitenant deployment.

Add a New Tenant

Table 9: Feature History

Feature Name	Release Information	Description
Tenant Device Forecasting	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	While adding a new tenant to the multitenant Cisco Catalyst SD-WAN deployment, a service provider can forecast the number of WAN edge devices that the tenant may deploy in their overlay network. Cisco SD-WAN Manager enforces this forecast limit. If the tenant tries to add devices beyond this limit, Cisco SD-WAN Manager responds with an appropriate error message and the device addition fails.

Prerequisites

- At least two Cisco SD-WAN Controllers must be operational and in the `vManage` mode before you can add new tenants.

  A Cisco SD-WAN Controller enters the `vManage` mode when you push a template onto the controller from Cisco SD-WAN Manager. A Cisco SD-WAN Controller in the `CLI` mode cannot serve multiple tenants.

- Each pair of Cisco SD-WAN Controllers can serve a maximum of 24 tenants and a maximum of 1000 tenant devices. Ensure that there at least two Cisco SD-WAN Controllers that can serve a new tenant. If no pair of Cisco SD-WAN Controllers in the deployment can serve a new tenant, add two Cisco SD-WAN Controllers and change their mode to `vManage`.

- If you add a second tenant immediately after adding a tenant, Cisco SD-WAN Manager adds them sequentially, and not in parallel.

- Each tenant must have a unique Virtual Account (VA) on **Plug and Play Connect** on Cisco Software Central. The tenant VA should belong to the same Smart Account (SA) as the provider VA.

- For an on-premises deployment, create a Cisco SD-WAN Validator controller profile for the tenant on **Plug and Play Connect**. The fields in the following table are mandatory.

  Table 10: Controller Profile Fields

Field	Description/Value
Profile Name	Enter a name for the controller profile.
Multi-Tenancy	From the drop-down list, select **Yes**.
SP Organization Name	Enter the provider organization name.

Field	Description/Value
Organization Name	Enter the tenant organization name in the format `<SP Org Name>-<Tenant Org Name>`. **Note** The organization name can be up to 64 characters.
Primary Controller	Enter the host details for the primary Cisco SD-WAN Validator.

For a cloud deployment, the Cisco SD-WAN Validator controller profile is created automatically as part of the tenant creation process.

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
3. Click **Add Tenant**. In the **Add Tenant** dialog box:
   a. Enter a name for the tenant.

      For a cloud deployment, the tenant name should be same as the tenant VA name on **Plug and Play Connect**.

   b. Enter a description of the tenant.

      The description can be up to 256 characters and can contain only alphanumeric characters.

   c. Enter the name of the organization.

      The organization name is case-sensitive. Each tenant or customer must have a unique organization name.

      Enter the organization name in the following format:

      `<SP Org Name>-<Tenant Org Name>`

      For example, if the provider organization name is 'multitenancy' and the tenant organization name is 'Customer1', while adding the tenant, enter the organization name as **`multitenancy-Customer1`**.

Note The organization name can be up to 64 characters.

   d. In the **URL Subdomain Name** field, enter the fully qualified sub-domain name of the tenant.

      - The sub-domain name must include the domain name of the service provider. For example, for the `managed-sp.com` service provider, a valid domain name can be `customer1.managed-sp.com`.

Note The service provider name is shared amongst all tenants. Hence, ensure that the URL naming convention follows the same domain name convention that was provided while enabling multitenancy from **Administration** > **Settings** > **Tenancy Mode**.

- For an on-premises deployment, add the fully qualified sub-domain name of the tenant to the DNS. Map the fully qualified sub-domain name to the IP addresses of the three Cisco SD-WAN Manager instances in the Cisco SD-WAN Manager cluster.
  - **Provider Level**: Create DNS A record and map it to the IP addresses of the Cisco SD-WAN Manager instances running in the Cisco SD-WAN Manager cluster. The A record is derived from the domain and Cluster ID that was created in steps 5 and 6 in Enable Multitenancy on Cisco SD-WAN Manager. For example, if domain is **sdwan.cisco.com** and Cluster ID is **vmanage123**, then A record will need to be configured as **vmanage123.sdwan.cisco.com**.

Note If you fail to update DNS entries, it will result in authentication errors when logging in to Cisco SD-WAN Manager. Validate DNS is configured correctly by executing **nslookup vmanage123.sdwan.cisco.com**.

  - **Tenant Level**: Create DNS CNAME records for each tenant created and map them to the FQDN created at the Provider Level. For example, if domain is **sdwan.cisco.com** and tenant name is **customer1** the CNAME record will need to be configured as **customer1.sdwan.cisco.com**.

Note Cluster ID is not required for CNAME record. Validate DNS is configured correctly by executing **nslookup customer1.sdwan.cisco.com**.

For a cloud deployment, the fully qualified sub-domain name of the tenant is automatically added to the DNS as part of the tenant creation process. After you add a tenant, it could take up to an hour before the fully qualified sub-domain name of the tenant can be resolved by the DNS.

e. In the **Number of Devices** field, enter the number of WAN edge devices that the tenant can deploy.

If the tenant tries to add WAN edge devices beyond this number, Cisco SD-WAN Manager reports an error and the device addition fails.

f. Click **Save**.

The **Create Tenant** screen appears, and the **Status** of the tenant creation reads **In progress**. To view status messages related to the creation of a tenant, click the > button to the left of the status.

Cisco SD-WAN Manager does the following:

- creates the tenant
- assigns two Cisco SD-WAN Controllers to serve the tenant and pushes a CLI template to these controllers to configure tenant information
- sends the tenant and Cisco SD-WAN Controller information to Cisco SD-WAN Validator.

What to do next:

After the **Status** column changes to **Success**, you can view the tenant information on the **Administration** > **Tenant Management** page.

Modify Tenant Information

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
3. In the left pane, click the name of the tenant.

   The tenant information is displayed in a pane on the right.
4. To modify tenant data, do as follows:
   a. In the right pane, click the pencil icon.
   b. In the **Edit Tenant** dialog box, you can modify the following:
      - **Description**: The description can be up to 256 characters and can contain only alphanumeric characters.
      - **Forecasted Device**: The number of WAN edge devices that the tenant can deploy.

        A tenant can add a maximum of 1000 devices.

Note This option is available from Cisco IOS XE Release 17.6.2, Cisco vManage Release 20.6.2.

If you increase the number of devices that a tenant can deploy, you must add the required number of device licenses to the tenant virtual account on **Plug and Play Connect** on Cisco Software Central.

Before you increase the number of devices that a tenant can deploy, ensure that the Cisco SD-WAN Controller pair assigned to the tenant can support this increased number. A pair of Cisco SD-WAN Controllers can support a maximum of 24 tenants and 1000 devices across all these tenants.

      - **URL Subdomain Name**: Modify the fully qualified sub-domain name of the tenant.

   c. Click **Save**

Delete a Tenant

Before you delete a tenant, delete all tenant WAN edge devices. See Delete a WAN Edge Device from a Tenant Network.

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
3. In the left pane, click the name of the tenant.

   The tenant information is displayed in a pane on the right.
4. To delete the tenant, do as follows:
   a. In the right pane, click the trash icon.

b. In the **Delete Tenant** dialog box, enter the provider **admin** password and click **Save**.

View OMP Statistics per Tenant on a Cisco SD-WAN Controller

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
3. In the table of devices, click on the hostname of a Cisco SD-WAN Controller.
4. In the left pane, click **Real Time**.
5. In the **Device Options** field, enter `OMP` and select the OMP statistics you wish to view.
6. In the **Select Filters** dialog box, click **Show Filters**.
7. Enter the **Tenant Name** and click **Search**.

Cisco SD-WAN Manager displays the selected OMP statistics for the particular tenant.

View Tenants Associated with a Cisco SD-WAN Controller

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. Click a **vSmart** connection number to display a table with detailed information about each connection.

   Cisco SD-WAN Manager displays a table that provides a summary of the Cisco SD-WAN Controllers and their connections.
3. For a Cisco SD-WAN Controller, click **...** and click **Tenant List**.

   Cisco SD-WAN Manager displays a summary of tenants associated with the Cisco SD-WAN Controller.

Manage Tenant WAN Edge Devices

Add a WAN Edge Device to a Tenant Network

Note If you are adding a WAN edge device that you had previously invalidated and deleted from an overlay network, you must reset the device software after adding the device. To reset the software on a Cisco IOS XE Catalyst SD-WAN device, use the command **request platform software sdwan software reset**.

1. Log in to Cisco SD-WAN Manager.

   If you're a provider user, log in as the **admin**. In the provider dashboard, choose a tenant from the drop-down list to enter the provider-as-tenant view.

   If you're a tenant user, log in as the **tenantadmin**.

2. Upload the device serial number file to Cisco SD-WAN Manager.
3. Validate the device and send details to controllers.
4. Create a configuration template for the device and attach the device to the template.

   While configuring the device, configure the service provider organization name and the tenant organization name as in the following example:

   ```
   sp-organization-name multitenancy
   organization-name multitenancy-Customer1
   ```

Note Enter the `organization-name` in the format `<SP Org Name>-<Tenant Org Name>`.

5. Bootstrap the device using bootstrap configuration generated through Cisco SD-WAN Manager or manually create the initial configuration on the device.
6. If you are using Enterprise Certificates to authenticate the device, download the CSR from Cisco SD-WAN Manager and get the CSR signed by the Enterprise CA. Install the certificate on Cisco SD-WAN Manager.

Delete a WAN Edge Device from a Tenant Network

1. Log in to Cisco SD-WAN Manager.

   If you're a provider user, log in as the **admin**. In the provider dashboard, choose a tenant from the drop-down list to enter the provider-as-tenant view.

   If you're a tenant user, log in as the **tenantadmin**.
2. Detach the device from any configuration templates.
3. Delete a WAN Edge Router.

Flexible Tenant Placement on Multitenant Cisco Catalyst SD-WAN Controllers

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

Table 11: Feature History

Feature Name	Release Information	Description
Flexible Tenant Placement on Multitenant Cisco Catalyst SD-WAN Controllers	Cisco vManage Release 20.9.1	With this feature, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco SD-WAN Controllers that serve the tenant. After onboarding a tenant, you can migrate the tenant to a different pair of multitenant Cisco SD-WAN Controller, if necessary.

Assign Cisco SD-WAN Controllers to Tenants During Onboarding

Prerequisites

- At least two Cisco SD-WAN Controllers must be operational and in Cisco SD-WAN Manager before you can add new tenants.

  A Cisco SD-WAN Controller enters the **vManage** mode when you push a template to the controller from Cisco SD-WAN Manager. A Cisco SD-WAN Controller in the **CLI** mode cannot serve multiple tenants.

- Each pair of Cisco SD-WAN Controllers can serve a maximum of 24 tenants and a maximum of 1000 tenant devices. Ensure that there are at least two Cisco SD-WAN Controllers that can serve a new tenant. If no pair of Cisco SD-WAN Controllers in the deployment can serve a new tenant, add two Cisco SD-WAN Controllers and change their mode to **vManage**.

- Add up to 16 tenants in a single operation. If you add more than one tenant, during the **Add Tenant** task, Cisco SD-WAN Manager adds the tenants one after another and not in parallel.

  While an **Add Tenant** task is in progress, do not perform a second tenant addition operation. If you do so, the second Add Tenant task fails.

- Each tenant must have a unique Virtual Account (VA) on Plug and Play Connect on Cisco Software Central. The tenant VA should belong to the same Smart Account (SA) as the provider VA.

- For an on-premises deployment, create a Cisco SD-WAN Validator controller profile for the tenant on Plug and Play Connect. The fields in the following table are mandatory.

Field	Description
Profile Name	Enter a name for the controller profile.
Multi-Tenancy	From the drop-down list, select **Yes**.
SP Organization Name	Enter the provider organization name.
Organization Name	Enter the tenant organization name in the format <SP Org Name>-<Tenant Org Name>. The organization name can be up to 64 characters.
Primary Controller	Enter the host details for the primary Cisco SD-WAN Validator.

For a cloud deployment, the Cisco SD-WAN Validator controller profile is created automatically as part of the tenant creation process.

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
3. Click **Add Tenant**.
4. In the **Add Tenant** slide-in pane, click **New Tenant**.
5. Configure the following tenant details:

Field	Description
Name	Enter a name for the tenant. For a cloud deployment, the tenant name should be same as the tenant VA name on Plug and Play Connect.
Description	Enter a description for the tenant. The description can have up to 256 characters and can contain only alphanumeric characters.
Organization Name	Enter the name of the tenant organization. The organization name can have up to 64 characters. The organization name is case-sensitive. Each tenant or customer must have a unique organization name. Enter the organization name in the following format: `<SP Org Name>-<Tenant Org Name>` For example, if the provider organization name is ‘managed-sp’ and the tenant organization name is 'customer1', while adding the tenant, enter the organization name as ‘managed-sp-customer1’.

Field	Description
URL Subdomain	

Field	Description
	Enter the fully qualified subdomain name of the tenant. • The subdomain name must include the domain name of the service provider. For example, for the managed-sp.com service provider, a valid domain name for customer1 is customer1.managed-sp.com. **Note** The service provider name is shared amongst all tenants. Ensure that the URL naming convention follows the same domain name convention that was followed while enabling multitenancy using **Administration** > **Settings** > **Tenancy Mode**. • For an on-premises deployment, add the fully qualified subdomain name of the tenant to the DNS. Map the fully qualified subdomain name to the IP addresses of the three Cisco SD-WAN Manager instances in the Cisco SD-WAN Manager cluster. • Provider DNS: Create a DNS A record and map it to the IP addresses of the Cisco SD-WAN Manager instances running in the Cisco SD-WAN Manager cluster. The A record is derived from the provider's domain name and the cluster ID that was created while enabling multitenancy on Cisco SD-WAN Manager. For example, if the provider's domain name is `sdwan.cisco.com` and the cluster ID is `vmanage123`, configure the A record as `vmanage123.sdwan.cisco.com`. **Note** If you fail to add the DNS A record, you will experience authentication errors when logging in to Cisco SD-WAN Manager. Validate that the DNS is configured correctly by using the **nslookup** command. Example: `nslookup vmanage123.sdwan.cisco.com` . • Tenant DNS: Create DNS CNAME records for each tenant that you created and map them to the provider FQDN. For example, if the provider's domain name is `sdwan.cisco.com` and tenant name is `customer1`, configure the CNAME record as `customer1.sdwan.cisco.com`. Cluster ID is not required in the CNAME record. Validate that the DNS is configured correctly by using the **nslookup** command. Example: `nslookup customer1.sdwan.cisco.com`. • For a cloud deployment, the fully qualified subdomain name of the tenant is automatically added to the DNS as part of the

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>tenant creation process. After you add a tenant, it could take up to an hour before the fully qualified subdomain name of the tenant can be resolved by the DNS.</td></tr>
<tr><td>Forecasted Devices</td><td>Enter the number of WAN edge devices that the tenant can add to the overlay.

If the tenant tries to add WAN edge devices beyond this number, Cisco SD-WAN Manager reports an error and the device addition fails.</td></tr>
<tr><td>Select two vSmarts</td><td>• Automatic tenant placement: Ensure that the Select two vSmarts field has the value Autoplacement. This is the default configuration.

• Flexible tenant placement:

a. Click the Select two vSmarts drop-down list.

Cisco SD-WAN Manager lists the hostnames of the available Cisco SD-WAN Controllers. For each Cisco SD-WAN Controller, Cisco SD-WAN Manager shows whether the controller is reachable and reports the following utilization details:

<table>
<tr><td>Tenant hosting capacity</td><td>Each Cisco SD-WAN Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisc SD-WAN Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.</td></tr>
<tr><td>Used device capacity</td><td>Each Cisco SD-WAN Controller can support a maximum of 1000 tenant WAN edge devices. Use device capacity represents the number of tenant WAN edge devices connected to the Cisco SD-WAN Controller in the form of a percentage of the maximum capacity (1000 WAN edge devices). Thi value indicates whether the Cisco SD-WAN Controller can support the number of devices forecast for the tenant that you are onboarding.</td></tr>
<tr><td>Memory utilized</td><td>This value represents memory consumption as a percentage.</td></tr>
<tr><td>CPU utilized</td><td>This value represents CPU usage as a percentage.</td></tr>
</table>
b. Select two Cisco SD-WAN Controllers to assign to the tenant based on the utilization details.

To select a Cisco SD-WAN Controller, check the check box adjacent to its hostname.</td></tr>
</table>

6. To save the tenant configuration, click **Save**.
7. To add another tenant, repeat Step 4 to Step 6.
8. To onboard tenants to the deployment, click **Add**.

Cisco SD-WAN Manager initiates the Create Tenant Bulk task to onboard the tenants.

As part of this task, Cisco SD-WAN Manager performs the following activities:

- creates the tenant
- assigns two Cisco SD-WAN Controllers to serve the tenant and pushes a CLI template to these controllers to configure tenant information
- sends the tenant and Cisco SD-WAN Controller information to Cisco SD-WAN Validator

When the task is successfully completed, you can view the tenant information, including the Cisco SD-WAN Controller and Cisco SD-WAN Validators assigned to the tenant, on the **Administration** > **Tenant Management** page.

Update Cisco SD-WAN Controllers Placement For a Tenant

You can migrate a tenant to a different pair of Cisco SD-WAN Controllers from the controllers that are currently assigned to the tenant. For instance, if you need to increase the tenant WAN edge device forecast and the controllers assigned to the tenant cannot connect to these revised number of tenant WAN edge devices, you can migrate the tenant to a pair of controllers that can accommodate the revised forecast.

If you wish to migrate a tenant to different pair of Cisco SD-WAN Controllers, you must change the Cisco SD-WAN Controllers that are assigned to the tenant one at a time. Doing so ensures that one of the Cisco SD-WAN Controllers is available to the tenant WAN edge devices during the migration and prevents disruptions in traffic.

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
3. For the tenant you wish to migrate to a different controller, click **…** adjacent to the tenant organization name.
4. Click **Update vSmart Placement**.
5. In the **Update vSmart Placement** slide-in pane, configure the following:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Source vSmart (currently applied)</td><td>a. Click the Source vSmart (currently applied) drop-down list.

Cisco SD-WAN Manager lists the hostnames of the Cisco SD-WAN Controllers assigned to the tenant. For each Cisco SD-WAN Controller, Cisco SD-WAN Manager shows whether the controller is reachable and reports the following utilization details:

<table>
<tr><td>Tenant hosting capacity</td><td>Each Cisco SD-WAN Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisco SD-WAN Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.</td></tr>
<tr><td>Used device capacity</td><td>Each Cisco SD-WAN Controller can support a maximum of 1000 tenant WAN edge devices. Used device capacity represents the number of tenant WAN edge devices connected to the Cisco SD-WAN Controller in the form of a percentage of the maximum capacity (1000 devices). This value indicates whether the Cisco SD-WAN Controller can support the number of devices forecast for the tenant that you are onboarding.</td></tr>
<tr><td>Memory utilized</td><td>This value represents memory consumption as a percentage.</td></tr>
<tr><td>CPU utilized</td><td>This value represents CPU usage as a percentage.</td></tr>
</table>
b. Check the check box adjacent to the hostname of one of the Cisco SD-WAN Controllers assigned to the tenant.</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Destination vSmart</td><td>
a. Click the Destination vSmart drop-down list.

Cisco SD-WAN Manager lists the hostnames of the available Cisco SD-WAN Controllers that are not assigned to the tenant. For each Cisco SD-WAN Controller, Cisco SD-WAN Manager shows whether the controller is reachable and reports the following utilization details:
<table>
<tr><td>Tenant hosting capacity</td><td>Each Cisco SD-WAN Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisco SD-WAN Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.</td></tr>
<tr><td>Used device capacity</td><td>Each Cisco SD-WAN Controller can support a maximum of 1000 tenant WAN edge devices. Used device capacity represents the number of tenant WAN edge devices connected to the Cisco SD-WAN Controller in the form of a percentage of the maximum capacity (1000 devices). This value indicates whether the Cisco SD-WAN Controller can support the number of devices forecast for the tenant that you are onboarding.</td></tr>
<tr><td>Memory utilized</td><td>This value represents memory consumption as a percentage.</td></tr>
<tr><td>CPU utilized</td><td>This value represents CPU usage as a percentage.</td></tr>
</table>
b. Check the check box adjacent to the hostname of the Cisco SD-WAN Controller you want to assign to the tenant.

If you select a Cisco SD-WAN Controller that does not have the required capacity to serve the tenant devices, the update operation fails.
</td></tr>
</table>

6. Click **Update**.
7. To change the other Cisco SD-WAN Controller that is assigned to the tenant, repeat Step 3 to Step 6.

Cisco SD-WAN Manager initiates the **Tenant vSmart Update** task to assign the selected Cisco SD-WAN Controller to the tenant, migrating the tenant details from the Cisco SD-WAN Controller that was previously assigned. When the task is successfully completed, you can view the tenant information, including the Cisco SD-WAN Controllers assigned to the tenant, on the **Administration** > **Tenant Management** page.

Configure Adaptive QoS

Table 12: Feature History

Feature Name	Release Information	Description
Adaptive QoS	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can now configure adaptive QoS from the **Adaptive QoS** tab using the Cisco VPN template for one of the supported interfaces.

To configure adaptive QoS use the Cisco VPN template for one of the following interfaces: Ethernet, Cellular, or DSL.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Choose a device from the list on the left. Feature templates that are applicable to the device are shown in the right pane.
4. Choose one of the available Cisco VPN Interface templates. In this example, we've chosen the **Cisco VPN Interface Ethernet** template.
5. Enter a name and description for the feature template.
6. Click **ACL/QoS**.
7. Notice that Adaptive QoS is disabled by default. To enable it, from the Adaptive QoS drop-down list, choose **Global**, and choose **On**.
8. (Optional) Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values.
   - **Adapt Period:** Choose **Global** from the drop-down list, click **On**, and enter the period in minutes.
   - **Shaping Rate Upstream:** Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps.
   - **Shaping Rate Downstream:** Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps.
9. Click **Save**.
10. Attach the feature template to a device template.

Configure Application Performance Monitor

Table 13: Feature History

Feature Name	Release Information	Description
Application Performance Monitor	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides an express method for configuring an intent-based performance monitor with the help of predefined monitoring profiles. Configure this feature using the CLI Add-on feature template in Cisco SD-WAN Manager.

You can enable application performance monitor globally (on all WAN tunnel interfaces) or on specific WAN tunnel interfaces. You can also enable performance monitoring for ART, or media monitors, or both.

To configure application performance monitoring using Cisco SD-WAN Manager, create a CLI add-on feature template and attach it to the device template.

Enable Performance Monitor Globally

The following example shows how to configure a performance monitor context using the sdwan-performance profile. This configuration enables monitoring of traffic metrics for ART and media, and applies the configuration to all SD-WAN tunnel interfaces. Here, 10.0.1.128 is the IP address of the third-party collector, GigabitEthernet9 is the source interface, and 2055 is the listening port of the third-party collector.

```
performance monitor context CISCO-APP-MONITOR profile sdwan-performance
 exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
 traffic-monitor application-response-time
 traffic-monitor media
!
performance monitor apply CISCO-APP-MONITOR sdwan-tunnel
```

Enable Performance Monitor on a Specific Interface

The following example shows how to configure a performance monitor context using the sdwan-performance profile. This configuration enables monitoring of traffic metrics for ART and media, and applies it to a specific tunel interface, in this case, Tunnel1. Here, 10.0.1.128 is the IP address of the third-party collector, GigabitEthernet9 is the source interface, and 2055 is the listening port of the third-party collector.

```
performance monitor context CISCO-APP-MONITOR profile sdwan-performance
 exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
 traffic-monitor application-response-time
 traffic-monitor media
!
interface Tunnel1
 performance monitor context CISCO-APP-MONITOR
```

Specify Additional Monitoring Filters and Sampling Rate

The following example shows how to enable specific type of traffic to be monitored. In this case, the match protocol of rtp-audio is defined in the class map named match-audio. This class in then referenced in **traffic-monitor media class-and** *match-audio* so that rtp-audio traffic is specifically monitored. Alternatively,

you can use the keyword **class-and** . In such a case, the customized class map replaces the default class map, which is automatically created when you enable the sdwan-performance profile.

In this example, performance monitor is applied globally, which means that it is applied on all Cisco Catalyst SD-WAN tunnel interfaces. The sampling rate of 10 indicates that one in 10 flows is monitored. Sampling rate 100 indicates that one in 100 flows is monitored.

```
class-map match-any match-audio
 match protocol rtp-audio
!
performance monitor context CISCO-APP-MONITOR profile sdwan-performancekeyword
 exporter destination 10.75.212.84 source GigabitEthernet0/0/0 port 2055
 traffic-monitor application-response-time
 traffic-monitor media class-and (or class-replace) match-audio
!
performance monitor apply CISCO-APP-MONITOR sdwan-tunnel
performance monitor sampling-rate 10
```

Use Cisco Catalyst SD-WAN Manager to Configure and Upgrade a Device

Table 14: Feature History

Feature Name	Release Information	Description
Remote Server Support for ZTP Software Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	You can now upgrade the software of Cisco IOS XE Catalyst SD-WAN devices at scale using Zero Touch Provisioning (ZTP).

Devices in the overlay network that are managed by Cisco SD-WAN Manager must be configured using Cisco SD-WAN Manager in order to be upgraded.

Use the following steps to configure and upgrade a device, using Cisco SD-WAN Manager:

1. Create feature templates:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and choose **Add Templates**.
2. Create device templates.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose **Create Templates**.
3. Attach device templates to individual devices.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose a template.

c. Click **…**, and choose **Attach Devices**.

d. You can see the added device in the list of **Available Devices** list. Send the particular device to the **Selected Devices** window using the **Right arrow** button.

e. Click **Attach**.

4. In the **Device Template** window, click **...** to update the device template by entering the following parameters:

Field	Description
Status	Displays the current status of the device template.
Chassis Number	Displays the chassis number of the device.
System IP	Displays the system IP address, if applicable.
Host Name	Displays the host name, if applicable.
DNS Address (vpn_dns_primary)	Enter the DNS address.
Host Name	Enter the host name.
System IP	Enter the system IP address.
Site ID	Enter the site ID.

5. Click **Update**. and then click **Next**.
6. After the device template is added, select the device template and click **Configure Devices**.
7. The **Config Preview** is displayed.
8. Click **Configure Devices**.
9. You are routed to the **Task List** window, where you can see the status of the configuration.
10. The configuration is attached to the device once the device is online.
11. Cisco SD-WAN Manager creates a task for this software upgrade through the ZTP server, and you can monitor the status of the upgrade using the **Task List** window.

Configure Application Probe Class through Cisco Catalyst SD-WAN Manager

Table 15: Feature History

Feature Name	Release Information	Description
Per-Class Application-Aware Routing	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This release supports Per-class application-aware routing to Cisco Catalyst SD-WAN. You can configure Application Probe Class using Cisco vManage.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. In **Centralized Policy**, click **Add Policy**. The **Create Groups of Interest** page appears.
3. Choose the list type **App Probe Class** from the left navigation panel to create your groups of interest.
4. Click **New App Probe Class**.
5. Enter the probe class name in the **Probe Class Name** field.
6. Choose the required forwarding class from the **Forwarding Class** drop-down list.

   If there are no forwarding classes, then create a class from the **Class Map** list page under the **Localized Policy Lists** in the **Custom Options** menu.

   To create a forwarding class:

   a. In the **Custom Options** drop-down, choose **Lists** from the Localized Policy options.
   b. In the Define Lists window, choose the list type **Class Map** from the left navigation panel.
   c. Click **New Class List** to create a new list.
   d. Enter **Class** and choose the **Queue** from the drop-down list.
   e. Click **Save**.

7. In the **Entries** pane, choose the appropriate color from the **Color** drop-down list and enter the **DSCP** value.

   Click **+** sign, to add more entries as required.
8. Click **Save**.

Configure AppQoE Controllers and Service Nodes

Table 16: Feature History

Feature Name	Release Information	Description
Support for Multiple, External AppQoE Service Nodes	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can now configure supported devices as external AppQoE service nodes through Cisco vManage.
Support for Automated MTU Setting for Tunnel Adjacency	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This feature enables a programmatic setting of the maximum transmission unit (MTU) size to 1500 for the network connecting the service controllers and service nodes. This automation prevents broken communication due to packet fragmentation that can bring down the throughput requirements.

Configure AppQoE Service Nodes

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Under **Device Templates**, click **Create Template** and choose **From Feature Template**.

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

3. In the **Device Model** field, choose **C8000v**.

Note Only Cisco Catalyst 8000V instances can be configured as AppQoE service nodes. If you choose any other device, the Service Node option isn't available in the Device Role field.

4. In the **Device Role** field, choose **Service Node** from the drop-down list.
5. Enter **Template Name** and **Description**.
6. Click **Additional Templates**. In the AppQoE field, notice that the Factory Default AppQoE External Service Node template is attached by default.

   No further configuration is required for devices configured as AppQoE service nodes. Additional configuration for connecting the service nodes to a service node controller is done through the AppQoE controller configuration screens in Cisco SD-WAN Manager.
7. Attach the device template to the device.

Configure AppQoE Service Controller

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

2. Under **Device Templates**, click **Create Template** and choose **From Feature Template**.

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

3. In the **Device Model** field, choose any one of the devices that support the service controller role. See the Supported Platforms section in this chapter for a complete list of devices that support the service controller role.
4. In the **Device Role** field, choose **SDWAN Edge** from the drop-down list.

Note The **SDWAN Edge** option is only visible for devices that support the service controller role.

5. Enter **Template Name** and **Description**.
6. Click **Additional Templates**. In the AppQoE field, you can either choose an existing AppQoE feature template or create a new one. This procedure includes steps to create a new AppQoE template for the device being configured with the service controller role.
7. Click the drop-down list for the AppQoE field and then click **Create Template.**
8. In the **Template Name** and **Description** fields, enter a name and description for your template respectively.
9. In the **Controller** area, enter the requested details.
   a. **Controller IP address:** Enter the service-side interface IP address of the controller. This is the IP address that the controller uses to communicate with the service nodes connected to it in a service cluster.
   b. **Service VPN:** Specify the service VPN ID in which the LAN-side connections of the service nodes reside. The VPN ID can be anyone from the following ranges: from 1 through 511, or from 513 through 65527.
   c. **Service Node IP 1:** Enter the IP address of the service nodes to enable the service controllers to communicate with the service nodes.

Note Click + next to the Service Node IP field to add more service nodes. You can add up to 64 service nodes for a single service controller.

Note From Cisco vManage Release 20.6.1, the AppQoE feature template allows you to configure multiple service node groups and add the external service nodes to such groups. You can configure a maximum of 32 service node groups per cluster. The name range of a service node group is SNG-APPQOE0 to SNG-APPQOE31.

However, if the version of the device that you are configuring as a service controller is lower than Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and you use Cisco vManage Release 20.6.1 to configure the AppQoE template for such device, ensure that you configure only one service node group, even though the template allows you to configure multiple service node groups.

10. Attach the device template to the device.

Configure Authorization and Accounting

Table 17: Feature History

Feature Name	Release Information	Description
Authorization and Accounting	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure authorization, which authorizes commands that a user enter on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device.

Navigating to the Template Screen and Naming the Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Select **Basic Information**.
6. To create a custom template for AAA, select Factory_Default_AAA_CISCO_Template and click **Create Template**. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA parameters.
7. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the **Scope** drop-down list to the left of the parameter field and select one of the following:

Table 18:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configuring Authorization

You can configure authorization, which causes a TACACS+ server to authorize commands that users enter on a device before the commands can be executed. Authorization is based on the policies that are configured in the TACACS+ server an on the parameters that you configure on the Authorization tab.

Prerequisites

- The TACACS+ server and the local server must be configured as first in the authentication order on the **Authentication** tab.

To configure authorization, choose the **Authorization** tab, click **+ New Authorization Rule**, and configure the following parameters:

Parameter Name	Description
Console	Enable this option to perform authorization for console access commands.
Config Command	Enable this option to perform authorization for configuration commands.
Method	Choose **Command**, which causes commands that a user enters to be authorized.
Privilege Level 1 or 15	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.

Parameter Name	Description
Groups	Choose a previously configured TACACS group. The parameters that this authorization rule defines are used by the TACACS servers that are associated with this group.
Authenticated	Enable this option to apply only to authenticated users the parameters that this authorization rule defines. If you do not enable this option, the rule is applied to all users.

Click Add to **add** the new authorization rule.

To add another authorization rule, click **+ New Accounting Rule** again.

To remove an authorization rule, click the trash icon on the right side of the line.

CLI equivalent:

```
system
   aaa
     aaa authorization console
     aaa authorization config-commands
     aaa authorization exec default list-name method
     aaa authorization commands level default list-name method
```

Configuring Accounting

You can configure accounting, which causes a TACACS+ server to generate a record of commands that a user executes on a device.

Prerequisite

- The TACACS+ server and the local server must be configured as first and second, respectively, in the authentication order on the **Authentication** tab. See Configuring Authentication Order.

To configure accounting, choose the **Accounting** tab, click **+ New Accounting Rule**, and configure the following parameters:

Table 19:

Parameter Name	Description
Method	Choose **Command**, which causes commands that a user executes to be logged.
Privilege Level 1 or 15	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Enable Start-Stop	Click **On** if you want the system to send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Groups	Choose a previously configured TACACS group. The parameters that this accounting rule defines are used by the TACACS servers that are associated with this group.

Click **Add** to add the new accounting rule.

To add another accounting rule, click **+ New Accounting Rule** again.

To remove an accounting rule, click the trash icon on the right side of the line.

CLI equivalent:

```
system
  aaa
    aaa accounting exec default start-stop group group-name
    aaa accounting commands level default start-stop group group-name
    aaa accounting network default start-stop group group-name
    aaa accounting system default start-stop group group-name
```

Configure Automatic Bandwidth Detection

Table 20: Feature History

Feature Name	Release Information	Description
Day 0 WAN Interface Automatic Bandwidth Detection	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can enable a device to automatically determine the bandwidth for WAN interfaces in VPN0 during day 0 onboarding by performing a speed test using an iPerf3 server.

You can configure the Cisco VPN Interface Ethernet template to cause a device to automatically detect the bandwidth for WAN interfaces in VPN0 during its day 0 onboarding. If you configure a template in this way, a Cisco IOS XE Catalyst SD-WAN device attempts to determine the bandwidth for WAN interfaces in VPN0 after completing the PnP process.

Automated bandwidth detection can provide more accurate day 0 bandwidth configuration than manual configuration because there is limited user traffic that can affect results.

A device determines the bandwidth by performing a speed test using an iPerf3 server. iPerf3 is a third-party tool that provides active measurements of bandwidth on IP networks. For more information, see the Iperf.fr website.

If a device has a connection to the internet, the device uses a public iPerf3 server for automatic bandwidth detection, unless you specify a private iPerf3 server. If a device has a connection to a private circuit and no internet connection, you must specify a private iPerf3 server for automatic bandwidth detection.

We recommend that you specify a private iPerf3 server. If a private iPerf3 server is not specified, the device pings a system defined set of public iPerf3 servers and selects for the speed test the public server with the minimum hops value or, if all servers have the same minimum hops value, the server with the minimum latency value. If the speed test fails, the device selects another public server from the list. The device continues to select other public iPerf3 servers until the speed test is successful or until it has tried all servers. Therefore, a speed test on a public iPerf3 server can use a server that is far away, resulting in a larger latency than the minimum.

The set of system defined public iPerf3 servers includes the following:

- iperf.scottlinux.com
- iperf.he.net
- bouygues.iperf.fr

- ping.online.net
- iperf.biznetnetworks.com

The following settings on the Cisco SD-WAN Manager VPN Interface Ethernet template control bandwidth detection. These settings are supported for WAN interfaces in VPN0 only.

- **Auto Detect Bandwidth**—When enabled, the device detects the bandwidth.
- **Iperf Server**—To use a private iPerf3 server for automatic bandwidth detection, enter the IPv4 address of the private server. To use a public iPerf3 server for automatic bandwidth detection, leave this field blank.

  The private iPerf3 server should run on port 5201, which is the default iPerf3 port.

In addition, automatic bandwidth detection requires that the allow-service all command be configured for the tunnel interface. See "VPN, Interface, and Tunnel Configuration for WAN and LAN interfaces."

The device writes the results of a speed test to the auto_speedtest.json file in its bootflash directory. It also displays the results in the **Auto Upstream Bandwidth (bps)** and **Auto Downstream Bandwidth (Mbps)** areas on the **Monitor** > **Devices** > **Interface** page of Cisco SD-WAN Manager.

If a device does not receive a response from an iPerf3 server, an error is recorded in the auto_speedtest.json file and displays on the **Monitor** > **Devices** > **Interface** page of Cisco SD-WAN Manager.

Note In Cisco vManage Release 20.6.x and earlier releases, the speed test results are displayed on the **Monitor** > **Network** > **Interface** page.

CLI Equivalent

auto-bandwidth-detect

iperf-server *ipv4-address*

There also is a no auto-bandwidth-detect form of this command.

Example

```
Device# show sdwan running-config sdwan
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation gre
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
  auto-bandwidth-detect
```

```
 iperf-server 192.0.2.255
exit
appqoe
 no tcpopt enable
 no dreopt enable
```

Configure AWS GovCloud (US)

Table 21: Feature History

Feature Name	Release Information	Description
Support for AWS GovCloud (US) with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, you can store your highly sensitive workloads in the Amazon Web Services (AWS) GovCloud (US). The same features that are available with the AWS integration are also available with Amazon GovCloud (US).

The workflow for configuring AWS GovCloud (US) is the same as the workflow for configuring Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud with AWS.

1. Create an AWS GovCloud (US) cloud account.

   For more information on creating an AWS GovCloud (US) account, see Create AWS Cloud Account.

2. Configure global settings for the cloud transit gateway.

   For more information on configuring global settings for the cloud transit gateway, see Configure Cloud Global Settings.

3. Discover host Virtual Private Clouds (VPCs) in all the accounts across the AWS GovCloud (US) regions.

   For more information on discovering host VPNs in AWS, see Discover Host Private Networks.

4. Create a cloud gateway.

   For more information on creating a cloud gateway, see Create Cloud Gateway.

5. Attach sites to a cloud gateway.

   For more information on attaching sites to a cloud gateway, see Configure Site Attachment.

6. Enable connectivity between Cisco Catalyst SD-WAN VPNs and VPCs.

   For more information on enabling connectivity between Cisco Catalyst SD-WAN VPNs and VPCs, see Intent Management - Connectivity.

7. Enable peer connections between the transit gateways in different AWS GovCloud (US) regions.

   For more information on enabling peer connections between transit gateways in different AWS GovCloud (US) regions, see Transit Gateway Peering.

8. Conduct an audit to identify gaps or disconnects between the Cisco SD-WAN Manager intent and what has been realized in the cloud.

   For more information on conducting an audit management review, see Audit Management.

Configure AWS Integration

Table 22: Feature History

Feature Name	Release Information	Description
Integration of AWS Branch with Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can configure Cloud OnRamp on Multicloud environment using the **Cloud OnRamp for Multicloud** option under **Configuration**.
Support for Pay As You Go License for Cisco Catalyst 8000V Edge Software Instances	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can use Cisco Catalyst 8000V Edge Software instances with pay as you go (PAYG) licenses when creating a new cloud gateway in Amazon Web Services (AWS), in addition to the previously supported bring your own license (BYOL) model.
Integration of Cisco Catalyst SD-WAN Branches with AWS using Cisco IOS XE Catalyst SD-WAN Devices and the AWS Transit Gateway Connect feature	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can use the AWS Transit Gateway Connect feature to connect a cloud gateway to an AWS Transit Gateway when creating a new cloud gateway in AWS.
AWS Branch Connect Solution	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure site attachment to connect branch devices to the cloud from the Cloud Gateways screen. For each of the cloud gateways, you can view, delete, or attach more sites.
AWS Cloud WAN Integration	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enables the use of AWS Cloud WAN to easily connect and route traffic from remote sites, regions and cloud applications over the AWS global network.

AWS Configuration Prerequisites

You need the following to configure AWS integration using Cisco SD-WAN Manager.

- AWS cloud account details
- Subscription to AWS marketplace

- Cisco SD-WAN Manager must have two cloud router licenses that are free to use for creating a new account

Create AWS Cloud Account

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. The Cloud OnRamp for Multicloud dashboard displays.
2. Click **Associate Cloud Account** in the Setup pane. Note the external Id from the **Associate Cloud Account** page.
3. In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.
4. Enter the account name in the **Account Name** field.
5. (Optional) Enter the description in the **Description** field.
6. In **Use for Cloud Gateway**, choose **Yes** if you want to create cloud gateway in your account, or choose **No**.
7. Choose the authentication model you want to use in the field **Login in to AWS With**.
   - **Key**
   - **IAM Role**

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

   Or

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

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

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

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

```
{

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

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]
```

```
}
```

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

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

Note The following set of permissions are allowed:

- AmazonEC2FullAccess
- IAMReadOnlyAccess
- AWSNetworkManagerFullAccess
- AWSResourceAccessManagerFullAccess

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

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

1. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require external ID** and pasting the external Id that you noted in Step 2.
2. See the Modifying a role trust policy (console) topic of AWS Documentation to change who can assume a role.

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

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

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

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

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

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

```
        "Condition": {
          "StringEquals": {
            "sts:ExternalId": "[vManage provided External ID]"
          }
        }
      }
    ]
}
```

8. Click **Add**.

To view or update cloud account details, click **...** on the Cloud Account Management page.

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

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

Configure Cloud Global Settings

To configure cloud transit gateway global settings, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Cloud Global Settings** in the **Setup** pane. The **Cloud Global Settings** window appears.
2. In the **Cloud Provider** field, choose **Amazon Web Services**.
3. Click **Cloud Gateway Solution** drop-down list to choose the AWS Transit Gateway and CSR in Transit VPC, or, beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, one of the following options.

   Beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, a combination of options is not supported. For example, if there are cloud gateways that were created using VPN connections, you must delete these cloud gateways before you can create AWS Transit Gateway Connect connections.

   - **Transit Gateway–VPN based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach.
   - **Transit Gateway–Connect based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS TGW Connect (GRE tunnels) approach.
   - **Transit Gateway–Branch-connect**—Allows connectivity of different Cisco Catalyst SD-WAN edge devices to VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. This option uses the AWS VPN connection (IPSec) approach.

- (Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1)

  Cloud WAN–VPN based (using TVPC)—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach.

- (Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1)

  Cloud WAN–Connect based (using TVPC)—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS Connect attachments (supporting GRE tunnels) approach.

4. Beginning with Cisco vManage Release 20.8.1, the following fields are available:

   - Click the **Reference Account Name** drop-down list to choose the reference account name. Cisco SD-WAN Manager discovers the software images and instance sizes using this reference account name.

Note You can still choose a different account, if required, at the time of a cloud gateway creation.

   - Click the **Reference Region** drop-down list to choose the reference region. Cisco SD-WAN Manager discovers the software images and instance sizes in this reference region under the referenced account name.

5. In the **Software Image** field, do the following:

   a. Click **BYOL** to use a bring your own license software image or **PAYG** to use a pay as you go software image.

   b. From the drop-down list, select a software image.

6. Click the **Instance Size** drop-down list to choose the required size.
7. Enter the **IP Subnet Pool**.
8. Enter the **Cloud Gateway BGP ASN Offset**.
9. Choose the **Intra Tag Communication**. The options are **Enabled** or **Disabled**.
10. Choose the **Default Route**. The options are **Enabled** or **Disabled**.
11. Click **Update**.

Parameter	Description
Software Image	Specifies the preinstalled or the subscibed software images for your account.

Parameter	Description
Instance Size	

Parameter	Description
	Specifies the instance size. The options are: • t2.medium • t3.medium • c4.2xlarge • c4.4xlarge • c4.8xlarge • c4.xlarge • c5.2xlarge • c5.4xlarge • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge • c5n.4xlarge • c5n.9xlarge • c5n.large • c5n.xlarge **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, following instance types are supported: • t3.medium • c5.2xlarge • c5.4xlarge **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, c5.4xlarge is not supported. • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge • c5n.4xlarge

Parameter	Description
	• c5n.9xlarge • c5n.large • c5n.xlarge Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, following instance is supported: • c5n.18xlarge **Note** Upgrade Cisco Catalyst SD-WAN Cloud devices running on Cisco SD-WAN Manager Release 19.2.1 on c3.2xlarge to Cisco SD-WAN Manager Release 20.4.1 or later in the following order. **1.** Resize c3.2xlarge to c5.4xlarge **2.** Upgrade the software to Cisco SD-WAN Manager Release 20.4.1 or later.
Cloud Gateway Solution	Specifies the combination of the Cloud Gateway Solution. For example, AWS Transit Gateway and CSR in Transit VPC.
IP Subnet Pool	Specifies the list of IP subnets separated by comma in CIDR format. More than one subnets can be specified. A single /24 subnet pool is able to support one cloud gateway only. You cannot modify the pool when a few cloud gateways are already making use of pool. Overlapping of subnets is not allowed.
Cloud Gateway BGP ASN Offset	Specifies the offset for allocation of transit gateway BGP ASNs. It is used to block routes learnt from one transit gateway (eBGP) to another. A band of 30 ASNs are reserved for transit gateway ASNs. Starting offset plus 30 will be the organization side BGP ASN. For example, if the offset is 64830, Org BGP ASN will be 64860. Acceptable start offset range is 64520 to 65500. It must be a multiple of 10.

Parameter	Description
Tunnel Count	This field appears if you choose **Transit Gateway–Connect based (using TVPC)** from the **Cloud Gateway Solution** drop-down list. Enter the number of tunnels for a VPN connection. You can configure up to 4 tunnels for each VPN connection. Each tunnel supports up to 5 Gbps of traffic. **Note** Changing the value of this parameter does not affect existing cloud gateways. To update the tunnel count for an existing cloud gateway, edit the cloud gateway from the **Configuration** > **Cloud OnRamp For Multicloud** > **Cloud Gateway** page.
Intra Tag Communication	Specifies if the communication between host VPCs under the same tag is enabled or disabled. If any tagged VPCs are already present and cloud gateways exist in those regions, then this flag cannot be changed.
Program Default Route in VPCs towards TGW	Specifies if the main route table of the host VPCs is programmed with default route is enabled or disabled.
Full Mesh of Transit VPCs	Specifies the full mesh connectivity between TVPCs of cloud gateways in different regions to carry site to site traffic (through CSRs).

Table 23: Expected Behavior for Global Settings

Item	Changeable after cloud gateway is created (Yes/No)	Default (Enabled/Disabled)
Software Image	Yes	NA
Instance Size	Yes	NA
IP Subnet Pool	See the description below	NA
Cloud Gateway BGP ASN Offset	No	NA
Intra Tag Communication	Cannot be changed if both cloud gateways and tagged host VPCs exist in any region	Enabled at the API level
Program Default Route in VPCs towards TGW	No	Enabled at the API level
Full Mesh of Transit VPCs	Yes	Disabled

Global IP Subnet Pool – can only be updated if there is no cloud gateway using global subnet pool. A cloud gateway uses global subnet pool whether it has custom setting or not. The subnet pool value is similar to the one in global setting (you can compare after splitting the list of CIDRs by comma; for example, *10.0.0.0/8, 10.255.255.254/8* and *10.255.255.254/8, 10.0.0.0/8* are similar).

If there is no cloud gateway using global subnet pool, the updated subnet pool in the global setting should not overlap with any of the existing custom subnet pools.

Custom IP Subnet Pool – when a custom setting is created, its subnet pool should not overlap with any of the existing custom subnet pools. It cannot partially overlap with the configured global subnet pool.

Discover Host Private Networks

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

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

   The host VPC table includes the following columns:

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

   Click a column to sort the VPCs, as required.

2. Click the **Region** drop-down list to select the VPCs based on particular region.
3. Click **Tag Actions** to perform the following actions:

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

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

Create Cloud Gateway

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

Note Before beginning this procedure, ensure that you have two devices with templates attached, which have the same type of license (BYOL or PAYG).

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Create Cloud Gateway** under **Manage**. The **Manage Cloud Gateway - Create** window appears.
2. In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.
3. In the **Cloud Gateway Name** field, enter the cloud gateway name.
4. (Optional) In the **Description**, enter the description.
5. Choose the account name from the **Account Name** drop-down list.
6. Choose the region from the **Region** drop-down list.
7. (Optional) Choose the SSH Key from the drop-down list.
8. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.
9. In the **Software Image** field, do the following:
   a. Choose a licensing option: **BYOL** for bring your own license or **PAYG** for pay as you go.
   b. In the drop-down menu, choose a software image.

Note The software image options are determined by the selection of **BYOL** or **PAYG**.

Note For information about onboarding a Cisco Catalyst 8000V without using Cisco Cloud OnRamp for Multicloud, see the Cisco SD-WAN Getting Started Guide.

10. Choose the UUID details in the **UUID (specify 2)** drop-down list.

Note
- Only logical devices (UUIDs) with a template attached appear in the list.
- From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

11. In the **Settings** field, select the required option. The options are:
    - Default
    - Customized - you can override the global settings. The selection is applicable only for the newly created cloud gateway.

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

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

13. Click **Add** to create a new cloud gateway.

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

Configure Site Attachment

Perform the following steps to attach sites to a cloud gateway:

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

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

2. For the desired cloud gateway, click **...** and choose **Cloud Gateway**.
3. Click **Attachment**.
4. Click **Attach Sites**.
5. In the **Circuit Color** drop-down list, choose a circuit color. A circuit color defines the search criteria for the sites you want to connect to your cloud gateway.
6. Click **Next**. The **Attach Sites - Select Sites** window appears. The table shows the sites with the selected circuit color.
7. Choose one or more sites from **Available Sites** and move them to **Selected Sites**.
8. Click **Next**.
9. On the **Attach Sites - Site Configuration** window, enter the **Tunnel Count**. The tunnel count ranges from 1 to 8 and each tunnel gives a bandwidth of 2.5 Gbps.
10. For the **Accelerated VPN** option, choose **Enabled** or **Disabled**. AWS Global Accelerator helps in optimized connectivity to the cloud.
11. Click **Next**. The **Attach Sites - Configuration Override** window appears. You can override the configuration that you performed in previous step, if required. You can alter the values for tunnel count and accelerated VPN status.
12. Click **Next**. The **Next Steps** window appears, where you can save the attachments you've added and exit the flow.
13. Click **Save and Exit**. If the configuration is successful, you see a message that indicates that the branch endpoints were successfully attached.

Note To view the tunnel status, go to the **Cloud OnRamp for Multicloud** Dashboard or the **Site Details** window.

Detach Sites

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Gateway Management** under **Manage**. The **Cloud Gateways** window appears. The table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.
2. For the desired cloud gateway, click **...** and choose **Cloud Gateway**. Next, click **Attachment**. The **Attachments - Cloud Gateway Name** window appears. The window displays the list of sites attached to the cloud gateway.
3. Click **Detach Sites**. The **Are you sure you want to detach sites from cloud gateway?** window appears.
4. Click **OK**. The sites attached to a cloud gateway are detached. The unmapping of the site happens and the VPN configuration is removed from the device.

Remove Cloud Gateway

On the **Cloud Gateways** window, for the desired cloud gateway, click **...**, and choose **Delete**. You must detach all the sites from a cloud gateway before trying to delete the cloud gateway.

You can view the cloud resources in the Cloud Resources Inventory for each cloud gateway in Cisco SD-WAN Manager.

Configure Azure for US Government

Table 24: Feature History

Feature Name	Release Information	Description
Support for the Azure for US Government Cloud with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, you can store your highly sensitive workloads in the Azure for US Government cloud. The same features that are available with the Azure integration with Virtual WAN are also available with the Azure for US Government cloud.

The workflow for configuring Azure for US Government integration is the same as the workflow as for the Azure Virtual WAN integration.

1. Associate your Azure for US Government account with Cisco SD-WAN Manager.

   For more information on associating your Azure for US Government account, see Integrate Your Azure Cloud Account.
2. Add and manage your cloud global settings.

For more information on configuring cloud global settings for Azure for US Government, see Integrate Your Azure Cloud Account.

3. Create and manage your cloud gateways.

   For more information on creating and managing your cloud gateways, see Create and Manage Cloud Gateways.

4. Discover your host virtual network (VNets) and create tags.

   For more information on discovering host VNets and creating tags, see Discover Host VNets and Create Tags.

5. Map your VNet tags and branch network VPNs.

   For more information on mapping your VNets and branch network VPNs, see Map VNet Tags and Branch Network VPNs.

Configure Azure Virtual WAN Hubs

Table 25: Feature History

Feature Name	Release Information	Description
Automated Integration of Azure Virtual WAN and Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can now configure Azure virtual WAN hubs using the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager.
Azure Scaling, Audit, and Security of Network Virtual Appliances	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure the SKU scale value, security of your Network Virtual Appliances (NVAs), and initiate the audit services using the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager. You can initiate an on-demand audit.
Periodic Audit, Enhancement to Azure Scaling and Audit, and ExpressRoute Connection.	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can now enable periodic audit and auto correct options from Cisco SD-WAN Manager.
Support for Multiple Virtual Hubs in Each Region	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	You can create multiple virtual hubs in a single Azure region.

Feature Name	Release Information	Description
Added an Azure Instance Type	Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	For Azure's West Central US and Australia East regions, added the Standard_D16_v5 Azure instance type, which includes 16 CPU cores and 64 GB of memory. You can deploy this type of instance for SKU scale values of 20, 40, 60, and 80.

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

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

Configuration Prerequisites

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

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

Integrate Your Azure Cloud Account

Associate your Account with Cisco SD-WAN Manager

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

Field	Description
Cloud Account Name	Enter a name for your Azure subscription.
Description (optional)	Enter a description for the account. This field is optional.
Use for Cloud Gateway	Choose **Yes** to create a cloud gateway in your account. The option **No** is chosen by default.

Field	Description
Tenant ID	Enter the ID of your Azure Active Directory (AD). To find the tenant ID, go to your Azure Active Directory and click **Properties**.
Subscription ID	Enter the ID of the Azure subscription you want to use as part of this workflow.
Client ID	Enter your existing Azure application ID. See Azure documentation for more information on how to register an application in Azure AD, get the client ID and secret key, and more.
Secret Key	Enter the password associated with the client ID.

5. Click **Add**.

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

Add and Manage Global Cloud Settings

1. On the **Cloud OnRamp for Multicloud** window, click **Cloud Global Settings** in the Setup area.
2. In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.
3. To edit global settings, click **Edit**.
4. To add global settings, click **Add**.
5. In the **Software Image** field, choose the software image of the WAN edge device to be used in the Azure Virtual Hub. This should be a preinstalled Cisco Catalyst 8000V image.

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

6. In the **SKU Scale** field, from the drop-down list, choose a scale based on your capacity requirements.
7. In the **IP Subnet Pool** field, specify the IP subnet pool to be used for the Azure virtual WAN hub. A subnet pool needs prefixes between /16 and /24.

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

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

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

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

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

Important

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

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

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

Create and Manage Cloud Gateways

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

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

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

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

5. (Optional) In the **Description** field, enter a description for the cloud gateway.
6. In the **Account Name** field, choose your Azure account name from the drop-down list.
7. In the **Region** field, choose an Azure region from the drop-down list.
8. In the **Resource Group** field, either choose a resource group from the drop-down list, or choose **Create New**.

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

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

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

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

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

11. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.
12. In the **Settings** field, choose one of the following:

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

(Minimum supported release: Cisco vManage Release 20.10.1)

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

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

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

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

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

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

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

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

15. Click **Add**.

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

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

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

- Before creating multiple cloud gateways in different regions, create the resource group, virtual WAN, and storage account for the first cloud gateway.
- Before creating multiple cloud gateways in the same region, create the virtual hub for the first cloud gateway in the region.

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

Discover Host VNets and Create Tags

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

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

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

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

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

Map VNets Tags and Branch Network VPNs

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

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

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

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

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

Configure SKU Scale Value

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

Follow these steps to configure SKU Scale value:

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

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

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

5. Click **Update**.

Initiate On-Demand Audit

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

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

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

3. For the **Cloud Provider** drop-down list, choose **Microsoft Azure**.

   The window displays the status for various Microsoft Azure objects. If the status is **In Sync** for any of the objects, it means the object is free from errors. If the status of an object is **Out of Sync**, it means that there are discrepancies between the object details available on Cisco SD-WAN Manager and the details available on the Azure database.

4. If the status is **Out of Sync** for any of the objects, click **Fix Sync issues**. This option resolves recoverable errors, if any, and opens a window that displays the status activity log.

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

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

Enable Periodic Audit

The following steps describe the procedure to enable periodic audit:

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

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

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

Configure Security Rules of NVAs

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

Follow these steps to configure security rules for NVA:

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

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

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

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

Table 26: Parameters Table

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

b. Click **Add**.

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

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

4. Click **Update**.

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

Configure Backup Server Settings

Table 27: Feature History

Feature Name	Release Information	Description
RMA Support for Cisco CSP Devices	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure the **Backup** information to enter storage server settings and backup intervals.

Points to Consider

- If you don't use an NFS server, Cisco SD-WAN Manager can’t successfully create backup copies of a CSP device for future RMA requirements.
- The NFS server mount location and configurations are same for all the CSP devices in a cluster.
- Don't consider an existing device in a cluster as the replacement CSP device.

Note If a replacement CSP device isn’t available, wait until the device appears in Cisco SD-WAN Manager.

- Don't attach further service chains to a cluster after you identify that a CSP device in the cluster is faulty.

- The backup operation on a CSP device creates backup files containing NFVIS configuration and VMs (if VMs are provisioned on the CSP device). You can use the following information for reference.
  - An automated backup file is generated and is in the format:

    serial_number + "_" + time_stamp + ".bkup"

    For example,

    `WZP22180EW2_2020_06_24T18_07_00.bkup`
  - An internal state model is maintained that specifies the status of the overall backup operation and internal states of each backup component:
    - NFVIS: A configuration backup of the CSP device as an xml file, config.xml.
    - VM_Images: All VNF tar.gz packages in `data/intdatastore/uploads` which are listed individually.
    - VM_Images_Flavors: The VM images such as, img_flvr.img.bkup.
    - Individual tar backups of the VNFs: The files such as, vmbkp.
  - The backup.manifest file contains information of files in the backup package and their checksum for verification during restore operation.

To create backup copies of all CSP devices in a cluster, perform the following steps:

1. On the **Cluster Topology** window, click **Add** next to **Backup**.

   To edit backup server settings, on the **Cluster Topology** window, click **Edit** next to **Backup**

   In the **Backup** configuration window, enter information about the following fields:
   - Mount Name—Enter the name of the NFS mount after mounting an NFS location.
   - Storage Space—Enter the disk space in GB.
   - Server IP: Enter the IP address of the NFS server.
   - Server Path: Enter the folder path of the NFS server such as, `/data/colobackup`
   - Backup: Click **Backup** to enable it.
   - Time: Set a time for scheduling the backup operation.
   - Interval: Choose from the options to schedule a periodic backup process.
     - Daily: The first backup is created a day after the backup configuration is saved on the device, and everyday thereafter.
     - Weekly: The first backup is created seven days after the backup configuration is saved on the device, and every week thereafter.
     - Once: The backup copy is created on a chosen day and it's valid for the entire lifetime of a cluster. You can choose a future calendar date.
2. Click **Save**.

3. To view the status of the previous five backup operations, use the **show hostaction backup status** command. To know about the backup status configuration command, see Backup and Restore NFVIS and VM Configurations. To use this command:
   a. In Cisco SD-WAN Manager, click the **Tools** > **SSH Terminal** screen to start an SSH session with Cisco SD-WAN Manager.
   b. Choose the CSP device.
   c. Enter the username and password for the CSP device and click **Enter** to log in to the CSP device and run the **show hostaction backup status** command.

Restore CSP Device

You can perform the restore operation only by using the CLI on the CSP device that you're restoring.

1. Use the **mount nfs-mount storage** command to mount NFS:

   For more information, see Network File System Support.

Note To access the backup file, the configuration for mounting an NFS file system should match the faulty device. You can view this information from other healthy CSP devices as the NFS mount location and configurations are same for all the CSP devices. To view and capture the information, you can do one of the following:

- In the **Cluster Topology** window, click **Add** next to **Backup**.
- Use the **show running-config** command to view the active configuration that is running on a CSP device.

mount nfs-mount storage { *mount-name* | **server_ip** *server_ip* | **server_path** *server_path* | **storage_space_total_gb** *storage_space_total_gb* | **storage_type** *storage_type* }

For example, `mount nfs-mount storage nfsfs/ server_ip 172.19.199.199 server_path /data/colobackup/ storage_space_total_gb 100.0 storagetype nfs`

2. Restore the backup information on a replacement CSP device using the **hostaction restore** command:

   For example,

```
hostaction restore except-connectivity file-path
nfs:nfsfs/WZP22180EW2_2020_06_24T18_07_00.bkup
```

Note Specify the except-connectivity parameter to retain the connectivity with the NFS server mounted in Step 2.

3. Use the **show hostaction backup status** command to view the status of the previous five backup images and their operational status.

   Also, you can view the backup images from the notifications available on the Cisco SD-WAN Manager **Monitor** > **Logs** > **Events** page.

Note In Cisco vManage Release 20.6.1 and earlier releases, you can view the backup images from the notifications available on the Cisco SD-WAN Manager **Monitor** > **Events** page.

4. Use the **show hostaction restore-status** command on the CSP device to view the status of the overall restore process and each component such as system, image and flavors, VM and so on.
5. To fix any failure after viewing the status, perform a factory default reset of the device.

Note The factory default reset sets the device to default configuration. Therefore, before performing the restore operation from Steps 1-4 on the replacement device, verify that all the restore operation prerequisites are met.

To know more about how to configure the restore operation on CSP devices, see Backup and Restore NFVIS and VM Configurations.

Configure BFD for Routing Protocols

Table 28: Feature History

Feature Name	Release Information	Description
BFD for Routing Protocols in Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can now use the CLI add-on feature templates in Cisco SD-WAN Manager to configure BFD for supported routing protocols.

Cisco SD-WAN Manager does not provide an independent template to configure BFD for routing protocols. However, supported protocols can be registered or deregistered to received BFD packets by adding configurations using the CLI add-on template in Cisco SD-WAN Manager. Use the CLI add-on template to configure the following:

- Add a single-hop BFD template with parameters such as timer, multiplier, session mode, and so on.
- Enable the BFD template under interfaces. Only one BFD template can be added per interface.
- Enable or disable BFD for the supported routing protocols. The configuration to enable or disable BFD is different for each of the supported routing protocols: BGP, EIGRP, OSPF, and OSPFv3.

Configure BFD for Service-Side BGP

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device from the device list.
5. Choose the **CLI Add-on Template** under **Other Templates**.
6. Enter the CLI configuration to add a single-hop BFD template and to enable BFD for service-BGP as shown in the following example.

```
bfd-template single-hop t1
 interval min-tx 500 min-rx 500 multiplier 3
 !
interface GigabitEthernet1
   bfd template t1

router bgp 10005
address-family ipv4 vrf 1
    neighbor 10.20.24.17 fall-over bfd
    !
  address-family ipv6 vrf 1
    neighbor 2001::7 fall-over bfd
```

Understanding the CLI Configuration

In this example, a single hop BFD template is created specifying the minimum and maximum interval and the multiplier. Specifying these parameters is mandatory. In addition, you have the option to also specify other BFD parameters such as echo mode (enabled by default), and BFD dampening (off by default). Once created, the BFD template is enabled under an interface (GigabitEthernet1, in this example).

Note To modify a BFD template enabled on an interface, you need to remove the existing template first, modify it, and then enable it on the interface again.

Note If you attach the BFD configuration to a device template that already has a BGP feature template attached, ensure that you update the BGP configuration in the CLI add-on template to include the **no neighbor** *ip-address* **ebgp-multihop** command. This change is required because the **neighbor** *ip-address* **ebgp-multihop** command is activated on the BGP feature template by default.

7. Click **Save**.
8. Attach the CLI Add-on Template with this configuration to the device template.

Note For the configuration to take effect, the device template must have a BGP feature template attached to it.

9. Attach the device template to the device.

Configure BFD for Transport-Side BGP

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device from the device list.
5. Choose the **CLI Add-on Template** under **Other Templates**.
6. Enter the CLI configuration to add a single-hop BFD template and to enable BFD for transport-BGP as shown in the following example:

```
bfd-template single-hop t1
interval min-tx 500 min-rx 500 multiplier 3
!
interface GigabitEthernet1
bfd template t1
!
router bgp 10005
neighbor 10.1.15.13 fall-over bfd
!
sdwan
interface GigabitEthernet1
tunnel-interface
allow-service bfd
allow-service bgp
```

Understanding the CLI Configuration

In this example, a single hop BFD template is created specifying the minimum and maximum interval and the multiplier. Specifying these parameters is mandatory. In addition, you have the option to also specify other BFD parameters such as echo mode (enabled by default), and BFD dampening (off by default). Once created, the BFD template is enabled under an interface (GigabitEthernet1, in this example). In this example, GigabitEthernet1 is also the source of the SD-WAN tunnel. Allowing service under the tunnel interface of GigabitEthernet1 ensures that BGP and BFD packets pass over the tunnel.

Note To modify a BFD template enabled on an interface, you need to remove the existing template first, modify it, and then enable it on the interface again.

Note If you attach the BFD configuration to a device template that already has a BGP feature template attached, ensure that you update the BGP configuration in the CLI add-on template to include the **no neighbor** *ip-address* **ebgp-multihop** command. This change is required because the **neighbor** *ip-address* **ebgp-multihop** command is activated on the BGP feature template by default.

7. Click **Save**.

8. Attach the CLI Add-on Template with this configuration to the device template.

Note For the configuration to take effect, the device template must have a BGP feature template attached to it.

Configure BFD for Service-Side EIGRP

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device from the device list.
5. Choose the **CLI Add-on Template** under **Other Templates**.
6. Enter the CLI configuration to add a single-hop BFD template enable BFD for EIGRP as shown in the example below.

```
bfd-template single-hop t1
 interval min-tx 500 min-rx 500 multiplier 3
 !
interface GigabitEthernet5
   bfd template t1

router eigrp myeigrp
address-family ipv4 vrf 1 autonomous-system 1
    af-interface GigabitEthernet5
     bfd
```

Understanding the CLI Configuration

In this example, a single hop BFD template is created specifying the minimum and maximum interval and the multiplier. Specifying these is mandatory. In addition, you have the option to also specify other BFD parameters such as echo mode (enabled by default), and BFD dampening (off by default).

Once created, the BFD template is enabled under an interface (GigabitEthernet5, in this example).

Note To modify a BFD template enabled on an interface, you first need to remove the existing template, modify it, and enable it on the interface again.

7. Click **Save**.
8. Attach the CLI Add-on Template with this configuration to the device template.

Note For the configuration to take effect, the device template must have an EIGRP feature template attached to it.

9. Attach the device template to the device.

Configure BFD for Service-Side OSPF and OSPFv3

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device from the device list.
5. Choose the **CLI Add-on Template** under **Other Templates**.
6. Enter the CLI configuration to add a single-hop BFD template enable BFD for OSPF and OSPFv3 as shown in the examples below.

OSPF

```
bfd-template single-hop t1
interval min-tx 500 min-rx 500 multiplier 3
!
interface GigabitEthernet5
bfd template t1
!
interface GigabitEthernet1
bfd template t1
!
router ospf 1 vrf 1
 bfd all-interfaces
!
```

OSPFv3

```
bfd-template single-hop t1
 interval min-tx 500 min-rx 500 multiplier 3

interface GigabitEthernet5
   bfd template t1
router ospfv3 1
 address-family ipv4 vrf 1
  bfd all-interfaces
```

Understanding the CLI Configuration

In these examples, a single hop BFD template is created specifying the minimum and maximum interval and the multiplier. Specifying these is mandatory. In addition, you have the option to also specify other BFD parameters such as echo mode (enabled by default), and BFD dampening (off by default).

Once created, the BFD template is enabled under an interface (GigabitEthernet5, in this example).

Note To modify a BFD template enabled on an interface, you first need to remove the existing template, modify it, and enable it on the interface again.

7. Click **Save**.
8. Attach the CLI Add-on Template with this configuration to the device template.

Note For the configuration to take effect, the device template must have an OSPF feature template attached to it.

9. Attach the device template to the device.

Configure or Cancel Cisco SD-WAN Manager Server Maintenance Window

You can set or cancel the start and end times and the duration of the maintenance window for the Cisco SD-WAN Manager server.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. From **Maintenance Window**, click **Edit**.

   To cancel the maintenance window, click **Cancel**.
3. Click the **Start date and time** drop-down list, and select the date and time when the **Maintenance Window** will start.
4. Click the **End date and time** drop-down list, and select the date and time when the **Maintenance Window** will end.
5. Click **Save**. The start and end times and the duration of the maintenance window are displayed in the **Maintenance Window** bar.

Two days before the start of the window, the Cisco SD-WAN Manager Dashboard displays a maintenance window alert notification.

Configure Carrier Supporting Carrier

Table 29: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Support for Carrier Supporting Carrier Connectivity	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Carrier supporting carrier (CSC) functionality enables you to interconnect different sites over a multiprotocol label switching (MPLS) backbone network. To use CSC, each site requires an edge router, called a customer edge (CE) device, that supports CSC functionality. You can configure a Cisco IOS XE Catalyst SD-WAN device to function as a CE device.

Perform the following steps to configure a CE device for CSC using a new feature template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and click **Create Template**. From the drop-down, choose **From Feature Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

3. In the **Device Model** field, choose the correct device model.
4. In the **Device Role** field, choose **SDWAN Edge**.
5. In the **Template Name** field, enter a name for the template.
6. In the **Transport & Management VPN** section, in the **Cisco VPN 0** field, choose a template to configure VPN 0 according to the network architecture.

   For information about configuring VPN 0, see Configure Interfaces in the WAN Transport VPN (VPN 0) in the Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x.
7. In the **Cisco VPN Interface Ethernet** field, choose a template to configure the interface.

   For information about configuring this field, see Configure VPN Ethernet Interface in the Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x.
8. In the **Transport & Management VPN** section, click **Cisco BGP** to add the Cisco BGP field.

   For information about configuring a BGP template, see Configure BGP Using SD-WAN Manager Templates in the Cisco Catalyst SD-WAN Routing Configuration Guide, Cisco IOS XE Release 17.x.
9. In the **MPLS Interface** section, in the **Interface Name 1** field, enter the interface used to connect the device to the backbone carrier.
10. In the **Neighbor** section, click **Advanced Options** to display CSC options.
11. Configure the following fields, which are specific to CSC support:

Field	Description
Send Label	Choose **On** to enable CSC support.
Explicit Null	If the device uses a loopback WAN interface, choose **On**.
As Override	If the two CE devices (CE1 and CE2) that connect through the backbone carrier use the same autonomous system (AS) number, choose **On**.
Allowas In	Similarly to **As Override**, if the two CE sites use the same AS number, choose **On**.

12. Click **Save** to save the BGP configuration.
13. Click **Create** to create the feature template.

    The **Configuration** > **Templates** page appears, showing available templates.
14. Attach the template to the device.
    a. On the **Configuration** > **Templates** page.
    b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

    c. For the new template, click **…** and choose **Attach Devices**.
    d. Move a device to the **Selected Devices** column and click **Attach**.

Configure a Cellular Gateway

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

Table 30: Feature History

Feature Name	Release Information	Feature Description
Cellular Gateway Configuration	Cisco vManage Release 20.4.1 Cisco IOS XE Catalyst SD-WAN Release 17.4.1a (on devices)	You can configure a supported cellular gateway as an IP pass-through device from the Templates tab.

You can configure a supported cellular gateway as an IP pass-through device. By positioning the configured device in an area in your facility that has a strong LTE signal, the signal can be extended over an Ethernet connection to a routing infrastructure in a location with a weaker LTE signal.

To configure a cellular gateway in Cisco SD-WAN Manager:

1. Create a device template for the **Cisco Cellular Gateway CG418-E** device.

   See "Create a Device Template from Feature Templates" in *Systems and Interfaces Configuration Guide*.

   After you enter a description for the feature template:

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

   c. From the **Create Template** drop-down list choose **From Feature Template**.

   d. From the **Device Model** drop-down list select the type of device for which you are creating the template.

   e. Choose **Cellular Gateway** > **Cellular Gateway Platform** > **Create Template**. Then configure the Cellular Gateway Platform feature template as shown in the following table.

Table 31: Cellular Gateway Platform Template Parameters

Parameter Name	Description
Basic Configuration Tab	
Time Zone	Choose the time zone to use for the device. The device uses this time zone for clock synchronization when NTP is configured.
Management Interface	Enter the IPv4 address of the management interface for accessing the device.
Admin-Password	Enter the admin user password for logging in to the device by using an SSH client or a console port.
NTP-Servers	Configure one or more NTP servers to which the device synchronizes its clock.

Parameter Name	Description
Cellular Configuration Tab	
IP-Src-Violation	Choose **v4 only**, **v6 only**, or **v4 and v6** to enable the IP source violation feature for the corresponding IP address types. Choose **None** if you do not want to enable this feature.
Auto-SIM	Choose **On** to enable the auto-SIM feature. When this feature is enabled, the device automatically detects the service provider to which SIMs in the device belong and automatically loads the appropriate firmware for that provider.
Primary SIM Slot	Choose the slot that contains the primary SIM card for the device. If the device loses service to this slot, it fails over to the secondary slot.
Failover-Timer (minutes)	Enter the number of minutes that the device waits before trying to communicate with the primary SIM slot after the device detects loss of service to this slot.
Max-Retry	Enter the number of consecutive unsuccessful attempts by the device to communicate with the primary SIM before failing over to the secondary slot

f. Choose **Cellular Gateway** > **Cellular Gateway Profile** and choose **Create Template** from the Cellular Gateway Profile drop-down list. Then configure the Cellular Gateway Profile feature template as shown in the following table.

Table 32: Cellular Gateway Profile Template Parameters

Parameter Name	Description
Basic Configuration Tab	

Parameter Name	Description
SIM	Choose a SIM slot and configure the following options to create a profile for the SIM in that slot. This profile indicates to the service provider which of its cellular networks the SIM should attach to. • Profile ID: Enter a unique ID for the profile • Access Point Name: Enter the name of the access point for this profile • Packet Data Network Type: Choose the type of network for data services for this profile (**IPv4**, **IPv6**, or **IPv4v6**) • Authentication: Choose the authentication method that this profile uses for data, and enter the user name and password for this method in the Profile Username and Profile Password fields that display You can configure one profile for each SIM slot in the device.
Add Profile	Click to add an access point name (APN) profile that the cellular device uses to attach to a cellular network. You can add up to 16 profiles.
Profile ID	Enter a unique identifier for the profile. Valid values: Integers 1 through 16.
Access Point Name	Enter a name to identify the cellular access point.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network (**IPv4**, **IPv6**, or **IPv46**).
Authentication	Choose the authentication method that is used to attach to the cellular access point (**none**, **pap**, **chap**, **pap_chap**).
Profile Username	If you choose an authentication method other than **none**, enter the user name to use for authentication when attaching to the cellular access point.
Password	If you choose an authentication method other than **none**, enter the password to use for authentication when attaching to the cellular access point.
Add	Click to add the profile your are configuring.
Advanced Configuration Tab	

Parameter Name	Description
Attach Profile	Choose the profile that the device uses to connect to the cellular network.
Cellular 1/1 Profile	Choose the profile that the device uses for data connectivity over the cellular network.

2. Attach the device template to the device.

   See "Attach and Detach a Device Template" in *Systems and Interfaces Configuration Guide*.

Configure Cellular Profile

Use the Cellular Profile feature template to configure the profiles used by cellular modems on devices.

To configure a cellular profile using Cisco SD-WAN Manager templates:

1. Create a Cellular Profile template to configure the profiles used by the cellular modem, as described in this section.
2. Create a VPN-Interface-Cellular feature template to configure cellular module parameters.
3. Create a VPN feature template to configure VPN parameters. .

Create a Cellular Profile Feature Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Under **Device Templates**, click **Create Template** and choose **From Feature Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. From the **Device Model** drop-down list, choose the device for which you are creating the template.
4. Click **Cellular**.
5. In the **Cellular** area, click **Cellular Profile**.
6. In the **Cellular Profile** field, choose **Create Template** from the drop-down list.

   The Cellular-Profile template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Cellular-Profile parameters.

Minimum Cellular Profile Configuration

The following table describes the parameters that are required to specify the cellular profile on the cellular modem of a device. Click **Save** after you enter the values for the template.

Parameter Name	Description
Template Name	Enter the template name. It can contain only alphanumeric characters.
Description (Template)	Enter a description for the template. It can contain only alphanumeric characters.
Interface name	Enter the name of the cellular interface, which must be cellular0.
Profile ID	Enter the identification number of the profile to be used on the device. You use this profile identification number when you configure for the cellular interface in the VPN-Interface-Cellular template. Range: 1 through 15.

CLI Equivalent

```
cellular cellular0
  profile number
```

Modify Cellular Profile Parameters

You can modify paramters of a profile if your service provider requires you to do so. For example, if you procure a data plan with static IP addresses, you might need to modify the APN field in the profile.

Parameter Name	Description
Access Point Name	Enter the name of the gateway between the service provider network and the public Internet. The name can contain up to 32 characters.
Authentication	Choose the authentication method used for the connection to the cellular network. It can be CHAP, None, PAP, or PAP/CHAP.
IP Address	Enter the static IP address assigned to the cellular interface. This field is used when the service provider requires that a static IP address be preconfigured before attaching to the network.
Profile Name	Enter a name to identify the cellular profile. The name can contain up to 14 characters.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv46.
Profile Username	Enter the username to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces.

Parameter Name	Description
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES encrypted key.
Primary DNS Address	Enter the IP addresses of the primary DNS servers in the service provider network, in decimal four-part dotted notation.
Secondary DNS Address	Enter the IP addresses of the secondary DNS servers in the service provider network, in decimal four-part dotted notation.

Configure Certificate Revocation

Table 33: Feature History

Feature Name	Release Information	Feature Description
Certificate Revocation	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can revoke enterprise certificates from devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.

Before You Begin

Make a note of the URL of the root CA CRL.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Administration Settings** window, click **Edit** next to **Certificate Revocation List**.

   The certificate revocation options appear.
3. Click **Enabled**.
4. In the **CRL Server URL** field, enter the URL of the CRL that you created on your secure server.
5. In the **Retrieval Interval** field, enter the interval, in hours, at which Cisco SD-WAN Manager retrieves the CRL from your secure server and revokes the certificates that the CRL designates.

   Enter a value from 1 to 24. The default retrieval interval is 1 hour.
6. Click **Save**.

   Cisco SD-WAN Manager immediately retrieves the CRL and revokes the certificates that the CRL designates. From then on, Cisco SD-WAN Manager retrieves the CRL according to the retrieval interval period that you specified.

Configure Certificate Settings

New controller devices in the overlay network—Cisco SD-WAN Manager instances, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers—are authenticated using signed certificates. From Cisco SD-WAN Manager, you can automatically generate the certificate signing requests (CSRs), retrieve the generated certificates, and install them on all controller devices when they are added to the network.

Note All controller devices must have a certificate installed on them to be able to join the overlay network.

To automate the certificate generation and installation process, configure the name of your organization and certificate authorization settings before adding the controller devices to the network.

For more information on configuring certificate settings, see Certificates.

Configure Cflowd Monitoring Policy

Table 34: Feature History

Feature Name	Release Information	Description
Flexible NetFlow Support for IPv6 and Cache Size Modification	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	Configure Cflowd traffic flow monitoring on Cisco IOS XE Catalyst SD-WAN devices.
Log Packets Dropped by Implicit ACL	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	To enable logging of dropped packets, check the **Implicit ACL Logging** check box and to configure how often the packet flows are logged, enter the value in the **Log Frequency** field.
Flexible NetFlow Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Configure Cflowd traffic flow monitoring to collect ToS, sampler ID, and remarked DSCP values in netflow records.
Flexible NetFlow for VPN0 Interface	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Configure this feature using the CLI template and also add-on CLI template.

Feature Name	Release Information	Description
Flexible NetFlow Export Spreading	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco Catalyst SD-WAN Control Components Release 20.9.x Cisco vManage Release 20.9.1	This feature enables export spreading to prevent export storms that occur when a burst of packets are sent to external collector. The export of the previous interval is spread during the current interval to prevent export storms. When NetFlow packets are sent over a low-bandwidth circuit, the export spreading functionality is enabled to avoid packet drops.
Flexible NetFlow Export of BFD Metrics	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	With this feature, you can export Bidirectional Forwarding Detection (BFD) metrics to an external collector for generating BFD metrics of loss, latency, and jitter. This feature provides enhanced monitoring and faster collection of network state data.
Real-Time Device Options for Monitoring Cflowd and SAIE Flows	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	With this feature, you can apply filters for monitoring specific Cflowd and SD-WAN Application Intelligence Engine (SAIE) applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. This feature was already available on Cisco vEdge devices and is being extended to Cisco IOS XE Catalyst SD-WAN devices in this release.

To configure a policy for Cflowd traffic flow monitoring, use the Cisco SD-WAN Manager policy configuration wizard. The wizard consists of four sequential pages that guide you through the process of creating and editing policy components:

1. **Create Applications or Groups of Interest**: Create lists that group related items together and that you call in the match or action components of a policy.
2. **Configure Topology**: Create the network structure to which the policy applies.
3. **Configure Traffic Rules**: Create the match and action conditions of a policy.
4. **Apply Policies to Sites and VPNs**: Associate a policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard pages, create policy components or blocks. In the last page, apply policy blocks to sites and VPNs in the overlay network. For the Cflowd policy to take effect, activate the policy.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options**.
3. Under **Centralized Policy**, click **Traffic Policy**.
4. Click **Cflowd**.
5. Click **Add Policy** and then click **Create New**.
6. Enter the **Name** and **Description** for the policy.

7. In the **Cflowd Template** section, enter **Active Flow Timeout**.
8. In the **Inactive Flow Timeout** field, enter the timeout range.
9. In the **Flow Refresh** field, enter the range.
10. In the **Sampling Interval** field, enter the sample duration.
11. In the **Protocol** drop-down list, choose an option from the drop-down list.

    Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the **Advanced Settings** field displays when you choose **IPv4** or **Both** from the options.
12. Under the **Advanced Settings**, do the following to collect additional IPv4 flow records:
    - Check the **TOS** check box.
    - Check the **Re-marked DSCP** check box.
13. Under the **Collector List**, click **New Collector**. You can configure up to four collectors.
    a. In the **VPN ID** field, enter the number of the VPN in which the collector is located.
    b. In the **IP Address** field, enter the IP address of the collector.
    c. In the **Port** field, enter the collector port number.
    d. In the **Transport Protocol** drop-down list, choose the transport type to use to reach the collector.
    e. In the **Source Interface** field, enter the name of the interface to use to send flows to the collector.
    f. In the **Export Spreading** field, click the **Enable** or **Disable** radio button.

       Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, the **Export Spreading** field is available to prevent export storms that occur due to the creation of a synchronized cache. The export of the previous interval is spread during the current interval to prevent export storms.
    g. In the **BFD Metrics Exporting** field, click the **Enable** or **Disable** radio button.

       Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **BFD Metrics Exporting** field is available for collecting BFD metrics of loss, jitter, and latency.
    h. In the **Exporting Interval** field, enter the interval in seconds for sending BFD metrics.

       Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **Exporting Interval** field is available for specifying the export interval for BFD metrics.

       Once you enable BFD metrics exporting, you can see the **Exporting Interval** field.

       The **Exporting Interval** field controls the intervals by which BFD metrics are sent.

       The default BFD export interval is 600 seconds.

Field	Description
Cflowd Policy Name	Enter a name for the Cflowd policy.
Description	Enter a description for the Cflowd policy.

Field	Description
Active Flow Timeout	Enter an active flow timeout value. The range is 30 to 3600 seconds.
Inactive Flow Timeout	Enter an inactive flow timeout value. The range is 1 to 3600 seconds.
Flow Refresh	Enter the interval for sending Cflowd records to an extremal collector. The range is 60 through 86400 seconds.
Sampling Interval	Enter the sample duration. The range is 1 through 65536 seconds.
Protocol	Choose the traffic protocol type from the drop-down list. The options are: **IPv4**, **IPv6**, or **Both**. The default protocol is **IPv4**.
TOS	Check the **TOS** check box. This indicates the type of field in the IPv4 header.
Re-marked DSCP	Check the **Re-marked DSCP** check box. This indicates the traffic output specified by the remarked data policy.
VPN ID	Enter the VPN ID. The range is 0 through 65536.
IP Address	Enter the IP address of the collector.
Port	Enter the port number of the collector. The range is from 1024 through 65535.
Transport Protocol	Choose the transport type from the drop-down list to reach the collector. The options are: **TCP** or **UDP**.
Source Interface	Choose the source interface from the drop-down list.
Export Spreading	Click the **Enable** or **Disable** radio button to configure export spreading. The default is **Disable**.
BFD Metrics Exporting	Click the **Enable** or **Disable** radio button to configure export of Bidirectional Forwarding Detection (BFD) metrics. The default is **Disable**.
Exporting Interval	Enter the export interval in seconds for sending the BFD metrics to an external collector. Enter an integer value. This field is displayed only if you enable BFD metrics export. The default BFD export interval is 600 seconds.

14. Click **Save Cflowd Policy**.

Configure HTTP CONNECT Using a CLI Add-On Template

Table 35: Feature History

Feature Name	Release Information	Description
HTTP CONNECT	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	HTTP CONNECT method is introduced in Cisco AppQoE. This method helps in optimizing HTTP CONNECT encrypted traffic using services such as SSL Proxy and DRE.

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

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

Table 36: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy a Cisco Cloud Services Router 1000v (Cisco CSR 1000v) instance as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway. From the Interconnect Gateway, you can create software-defined interconnects to an AWS Cloud OnRamp or another interconnect gateway in the Equinix fabric.

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix: Google Cloud and Microsoft Azure	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can create software-defined interconnects to Google Cloud VPCs, or Microsoft Azure VNets or Virtual WANs to link your branch location to the cloud resources through the Equinix fabric. You can also create, update and delete device links from Interconnect Gateway in the Equinix fabric.
Encrypted Multicloud Interconnects with Equinix	Cisco vManage Release 20.9.1	You can extend the Cisco Catalyst SD-WAN fabric from the Interconnect gateway in Equinix into the AWS, Google Cloud and Microsoft Azure Cloud Service Providers. You can provision a secure private Cisco Catalyst SD-WAN connection between an Interconnect Gateway and Cloud Service Providers through the Cloud OnRamp workflows in Cisco SD-WAN Manager.
Support for Cisco Catalyst 8000V Edge Software	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can deploy a Cisco Catalyst 8000v Edge Software as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway.
Addition of VPC and VNet Tags to SDCI Connections	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can modify VPC and VNet Tags and some other properties that are associated with an SDCI connection
Management of Audit in Equinix	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	The audit management helps in understanding if the interconnect cloud and provider states are in sync with the Cisco Catalyst SD-WAN Manager state. The audit process involves scanning the provider resources, interconnect gateways, and connections to the cloud. For more information, see Audit Management.

Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Equinix

Associate Equinix Account with Cisco SD-WAN Manager

Prerequisites

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

Procedure

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

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

5. Click **Add**.

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

Configure Global Settings for Equinix Interconnect Gateways

Prerequisites

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

4. Associate Equinix account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Global Settings**.
   - To add global settings, click **Add**.
   - To modify global settings, click **Edit**.
4. Configure the following:

Interconnect Provider	Choose **EQUINIX**.
Software Image	Choose a Cisco CSR 1000v image.
Instance Size	Instance size determines the compute footprint and throughput of each Cisco CSR 1000v instance. Choose one of the following: • **Small**: 2vCPU, 4 GB DRAM, up to 1 Gbps • **Medium**: 4vCPU, 4 GB DRAM, up to 2.5 Gbps • **Large**: 6vCPU, 4 GB DRAM, up to 2.5 Gbps
Interconnect Transit Color	Choose the color to be assigned for connection between Interconnect Gateways. This color is restricted to prevent direct peering between branch locations. Do not assign the same color to another connection in the Cisco Catalyst SD-WAN fabric. **Note** It is recommended to use private colors. Do not use default colors.
BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

Interconnect CGW SDWAN Color	Minimum supported release: Cisco vManage Release 20.9.1 Choose the color to be used for the interface through which the interconnect gateway connects to the cloud gateway. **Note** Color assigned to an interface must be unique for the interconnect gateway devices and common across cloud interconnect providers. For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the cloud gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, interconnect gateway, and cloud gateway.

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

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

Attach Equinix Template to Cisco CSR 1000v Instance

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

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

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

3. Choose the **Template Type** as **Default** and find the template named *Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02.*
4. Click **…** and click **Attach Devices**.
5. Choose the UUID of desired Cisco CSR 1000v instance from the list of **Available Devices** and move the instance to the list of **Selected Devices**.
6. Click **Attach**.
7. The template contains variables. To enter values for the variables in the template, click **…** and click **Edit Device Template**.
8. Enter the values for the following variables and click **Update**:
   - DNS Address (vpn_dns_primary)
   - DNS Address (vpn_dns_secondary)
   - Color (vpn_if_tunnel_color_value)
   - System IP (system-ip)

- Site ID (site-id)
- Hostname (host-name)

9. Click **Next**.
10. Click **Configure Devices**.

Create Interconnect Gateway at an Equinix Location

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

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Attach Equinix Template to Cisco CSR 1000v Instance.

Procedure

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

Interconnect Provider	Choose **EQUINIX**.
Gateway Name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.
Account Name	Choose an Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose the Equinix location where the Cisco CSR 1000v instance must be deployed.
Billing Account ID	Choose the appropriate billing account for the location.
Site Name	Choose the site. Starting Cisco vManage Release 20.10.1, Site Name field is available.
UUID	Choose the UUID of a Cisco CSR 1000v instance that has the Equinix default template attached. **Note** When a site name is selected, UUID field is auto-populated with the UUID associated with the site name.

Settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect Global Settings. • **Custom**: Choose a specific instance size and software image for this gateway.

5. Click **Add**.

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

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

Create Interconnect to AWS

Associate AWS Account with Cisco SD-WAN Manager

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

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

5. Click **Add**.

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

Discover Host Private Networks and Tag AWS VPCs

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

Prerequisite

Associate AWS Account with Cisco SD-WAN Manager.

Procedure

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

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

   The host VPC table includes the following columns:

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

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

   You can perform the following actions:

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

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

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

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

8. Click **Add**.

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

Create Direct Connect Public Hosted Connection to AWS from Interconnect Gateway

Prerequisites

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

Procedure

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

Destination Type	Choose **Cloud**.

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

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

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

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

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

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

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag AWS VPCs.
6. Attach Equinix template to Cisco CSR1000v Instance.
7. Create Interconnect Gateway at an Equinix Location.

Procedure

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

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

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

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

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

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

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

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

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

Prerequisites

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

   Attach Equinix Template to Cisco CSR 1000v Instance for versions prior to Cisco Catalyst SD-WAN Manager Release 20.12.1.
7. Create Interconnect Gateway at an Equinix Location.

Procedure

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

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

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

Equinix Hosted Connection VIF Type	Choose **Transit**.

Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.
Direct Connect Gateway	**a.** Click the Refresh button to fetch the direct connect gateways associated with the selected AWS account. **b.** Choose the Direct Connect Gateway to which the direct connect connection must be created. Alternatively, create a new Direct Connect Gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.
Settings	Choose one of the following: • **Global**: • BGP peering IP address is picked from an internally reserved /16 subnet (198.18.0.0/16). • BGP ASN is picked from the Global Settings. • **Custom**: **a.** Enter a custom /30 CIDR IP address for BGP peering. **b.** Enter custom BGP ASN for peering. **Note** You can specify a custom BGP ASN only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.
Segment	Choose the segment ID for this connection.

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

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

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

Create Interconnects to Google Cloud

Associate Google Cloud Account with Cisco SD-WAN Manager

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

Cloud Provider	Choose **Google Cloud**.
Cloud Account Name	Enter a name of your choice.

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

5. Click **Add**.

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

Create Interconnect to Google Cloud Routers from Interconnect Gateways

Prerequisites

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

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

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

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

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

3. Associate Equinix Account with Cisco SD-WAN Manager.
4. Configure Global Settings for Interconnect Gateways.
5. Attach Equinix Template to Cisco Catalyst 1000v Instance.
6. Create Interconnect Gateway at a Equinix Location closest to your Cisco Catalyst SD-WAN branch location.

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

    When the task is successful, the connections are listed on the **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

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

Create Interconnect Connection to a Cloud Gateway In Google Cloud

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Associate Equinix Account with Cisco SD-WAN Manager.
3. Configure Global Settings for interconnect gateways.
4. Attach Equinix Template to Cisco Catalyst 1000v Instance.
5. Create Interconnect Gateway at a Equinix Location closest to your Cisco Catalyst SD-WAN branch location.

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

Procedure

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

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

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

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

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

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

Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

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

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

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

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

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

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

When the task is successful, the connections are listed on the **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

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

Create Interconnects to Microsoft Azure

Associate Microsoft Azure Account with Cisco SD-WAN Manager

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

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

5. Click **Add**.

Discover Host Private Networks and Tag Microsoft Azure VNets

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

Prerequisite

Associate Microsoft Azure Account with Cisco SD-WAN Manager.

Add a Tag

Group VNets and tag them together.

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

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

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

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

8. Click **Add**.

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

Edit a Tag

Add VNets to or remove VNets from an existing tag.

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

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

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

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

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

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

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

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

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

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

7. Click **Update**.

Delete a Tag

Remove a tag that groups together VNets.

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

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

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

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

Prerequisites

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

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

Procedure

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

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

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following and click **Save**: • Resource Group: Choose a resource group associated with the Microsoft Azure account. • Region: Choose an Azure region. • Instance Name: Enter a name for the ExpressRoute instance. • Provider: Choose **Equinix**. • Peering Location: Click the Refresh button to update the list of available locations. Choose an ExpressRoute location. • Bandwidth: Choose the bandwidth of the ExpressRoute circuit. • SKU: Choose the **Premium** or the **Standard** SKU. • Billing Model: Choose **Metered** billing or **Unlimited**.

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

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.

Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

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

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

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

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

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

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

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

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

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

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

Prerequisites

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

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

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

Procedure

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

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

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following and click **Save**: • Resource Group: Choose a resource group associated with the Microsoft Azure account. • Region: Choose an Azure region. • Instance Name: Enter a name for the ExpressRoute instance. • Provider: Choose **Equinix**. • Peering Location: Click the Refresh button to update the list of available locations. Choose an ExpressRoute location. • Bandwidth: Choose the bandwidth of the ExpressRoute circuit. • SKU: Choose the **Premium** or the **Standard** SKU. • Billing Model: Choose **Metered** billing or **Unlimited**.

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

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.

Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

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

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

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

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

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

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

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

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

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

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

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

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

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

Device Links

Add Device Links

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

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

9. (Optional)

   Enter **Subnet**.

Note
- Provide IP subnets for interconnect gateway device link interface.
- The subnet should be in 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 range.
- The subnet should not conflict with 172.31.251.0/21.
- The subnet should not conflict with other connections.
- If you do not enter the subnet, 198.19.0.0/16 is used by default.

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

Delete Device Links

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

   Existing device links are summarized in a table.
5. In the table, find the desired link and click **...**.
6. To delete a device link, click **Delete** and confirm that you wish to delete the device link.

Update Device Links

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

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

7. In the **Edit Device Link** page, you can only update the **Bandwidth** and **Gateway Name** to add or remove gateways.

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

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

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

8. Click **Save**.

Create Interconnect Between Interconnect Gateways

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

Prerequisites

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

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

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

Procedure

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

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

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

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

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

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

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

View Interconnect Gateway and Connection Summary

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

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

   The following information is displayed:

Interconnect Gateways	• Total number of interconnect gateways • Number of interconnect gateways that reachable (Up) • Number of interconnect gateways that are unreachable (Down)
Connections	• Total number of connections • Number of connections in the Up state • Number of connections in the Down state

Summary Table	Summarized list of all interconnect gateways and connections from the gateways.

View, Edit or Delete Connections

Note

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

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

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

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

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

Edit Connection Configuration

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

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

   Existing connections are summarized in a table.

4. To modify connection configuration, click **...** for the desired connection and click **Edit**.

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

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

Note You can modify the properties of active connections only.

Table 37: Editable Properties of Interconnect Connections to AWS

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

Field	Description	Applicable Connection Types
Allowed Prefixes	Click **Edit Prefixes**. Enter the IPv4 Classless Inter-Domain Routing (CIDR) prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard. **Note** You can add additional prefixes. You cannot remove existing prefixes.	Transit-hosted connections

Table 38: 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 39: Editable Properties of Interconnect Connections to Microsoft Azure

Field	Description	Applicable Connection Types
Bandwidth	Modify the connection bandwidth. Unit: Mbps. **Note** You can only increase the bandwidth of connections to Microsoft Azure. For connections to Microsoft Azure, you must increase the bandwidth of the ExpressRoute on the Azure portal before increase the connection bandwidth on Cisco SD-WAN Manager.	Private and public (Microsoft) peering connections
Segment	Choose a different from segment ID for this connection.	Private and public (Microsoft) peering connections

Field	Description	Applicable Connection Types
BGP Advertise Prefix	Enter the summary addresses and prefixes you wish to advertise to the interconnect gateway. **Note** By default Microsoft Azure uses an older version of API on its portal for displaying resources or network objects that do not display the BGP advertise prefix correctly. To verify the BGP advertise prefix from the Microsoft Azure portal, select 2020-05-01 or above API version.	Public (Microsoft) peering connections
VNet Settings		
VNet	Choose VNet tags to identify the VNets for which traffic must be routed through this connection.	Private peering connections
vHub Settings	**a.** Click **Edit Settings**. **b.** Review the virtual hub name and the address-prefix for applicable regions. If a virtual hub does not exist in a region, enter the virtual hub name and address-prefix to be used for the region. **Note** Ensure that the virtual hub address-prefix that you enter does not overlap with the address-prefixes of any VNets. **c.** To apply changes, click **Save**. To discard changes, click **Cancel**.	Private peering connections

Table 40: Editable Properties of Interconnect Connections Between Edge Devices

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

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

View, Edit, or Delete an Interconnect Gateway

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

Existing interconnect gateway details are summarized in a table.

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

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

View, Edit, or Delete an Interconnect Account

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

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

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

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

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

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

Configure Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

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

Table 41: 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 42: Editable Properties of Interconnect Connections to AWS, on page 190. • 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 44: Editable Properties of Interconnect Connections to Microsoft Azure, on page

Feature Name	Release Information	Description
		192. • 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.

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 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:

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. Choose one of the following: • **Small**: 2vCPU, 4GB DRAM, 500Mbps • **Medium**: 4vCPU, 8GB DRAM, 1Gbps • **Large**: 8vCPU, 16GB DRAM, 5Gbps

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

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 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 deploy the Cisco Catalyst 8000v instance at a Megaport location closest to your branch location.

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Attach Megaport Template to Cisco Catalyst 8000v Instance.
4. 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. 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 **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.
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.
UUID	Choose the UUID of a Cisco Catalyst 8000v instance that has the Megaport default template attached. **Note** From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.
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.

Field	Description
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	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 (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 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 (see Segmentation Configuration Guide).
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. 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 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.
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 (see Segmentation Configuration Guide).
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. 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 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.
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 (see Segmentation Configuration Guide).
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. 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 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.
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 (see Segmentation Configuration Guide).
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. 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. 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 vManage.
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 (see Segmentation Configuration Guide).
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag Microsoft Azure VNets.
6. Attach 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. 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 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 42: 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 43: 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 44: 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

Field	Description	Applicable Connection Types
vNet Settings		
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 45: 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.

License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

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

Table 46: Feature History

Feature Name	Release Information	Description
License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport	Cisco vManage Release 20.9.1	To create Interconnect Gateways and Interconnect Connections in the Megaport fabric, you must purchase required licenses on Cisco Commerce workspace. With this feature, Cisco SD-WAN Manager operates together with Megaport to enable you to monitor your licenses while Cisco and Megaport jointly enforce the license requirements when you create Interconnect Gateways or Interconnect Connections.

View Licenses Associated with a Megaport Account

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. From **SETUP** under **WORKFLOWS**, click **Account Licenses**.
4. **Provider**: From the drop-down list, choose **Megaport**.
5. **Account Name**: From the drop-down list, choose a Megaport account name.
6. To view Interconnect Gateway licenses, click **INTERCONNECT GATEWAY LICENSES**.

   Cisco SD-WAN Manager displays the Interconnect Gateway license SKUs associated with the account, providing the following details for each SKU:

Table 47: Interconnect Gateway License SKU Details

Column	Description
SKU Name	Name of the license SKU
SKU UUID	Unique ID for the license SKU within the Megaport account to which it belongs
Gateway Size	Size or form factor of the Interconnect Gateway instance (SML, MED, or LRG)
State	Current state of the license(IN_USE; IN_USE, EXPIRED; AVAILABLE; or EXPIRED)
License End Date	The end date (expiry date) for the license derived from the start date and the term of entitlement
Start Date	The license start date specified while ordering the SKU on Cisco Commerce workspace

Column	Description
Smart Account ID	Smart Account to which the license belongs
Virtual Account ID	Virtual Account to which the license belongs
Subscription ID	Subscription ID associated with the license
Web Order ID	Unique web order ID for the license

7. To view Interconnect Connection licenses, click **INTERCONNECT CONNECTION LICENSES**.

   Cisco SD-WAN Manager displays the Interconnect Connection license SKUs associated with the account, providing the following details for each SKU:

   Table 48: Interconnect Connection License SKU Details

Column	Description
SKU Name	Name of the license SKU
SKU UUID	Unique ID for the license SKU within the Megaport account to which it belongs
State	Current state of the license(IN_USE; IN_USE, EXPIRED; AVAILABLE; or EXPIRED)
License End Date	The end date (expiry date) for the license derived from the start date and the term of entitlement
Start Date	The license start date specified while ordering the SKU on Cisco Commerce workspace
VXC Bandwidth	Configured bandwidth (in Mbps) of the Interconnect Connection
Smart Account ID	Smart Account to which the license belongs
Virtual Account ID	Virtual Account to which the license belongs
Subscription ID	Subscription ID associated with the license
Web Order ID	Unique web order ID for the license

8. To view supplemental licenses, click **SUPPLEMENTAL LICENSES**.

   Cisco SD-WAN Manager displays the supplemental license SKUs associated with the account, providing the following details for each SKU:

   Table 49: Supplemental License SKU Details

Column	Description
SKU Name	Name of the license SKU

Column	Description
SKU UUID	Unique ID for the license SKU within the Megaport account to which it belongs
State	Current state of the license(IN_USE; IN_USE, EXPIRED; AVAILABLE; or EXPIRED)
License End Date	The end date (expiry date) for the license derived from the start date and the term of entitlement
Start Date	The license start date specified while ordering the SKU on Cisco Commerce workspace
Bandwidth	Configured bandwidth (in Mbps) of the AWS hosted connection
Smart Account ID	Smart Account to which the license belongs
Virtual Account ID	Virtual Account to which the license belongs
Subscription ID	Subscription ID associated with the license
Web Order ID	Unique web order ID for the license

Find License SKU Associated with an Interconnect Gateway

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

   Cisco SD-WAN Manager displays all the deployed Interconnect Gateways in a table.
4. Find the Interconnect Gateway of interest.

Tip Search for an Interconnect Gateway using the name you specified for it during configuration.

5. Scroll to the right to view the **License SKU UUID** column.

   On the **Account Licenses** page, use this SKU UUID to view more information about the license SKU.

   The **License End Date** column displays the expiry date for the Interconnect Gateway license.

Related Topics

View Licenses Associated with a Megaport Account, on page 196

Find License SKU Associated with an Interconnect Connection

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

3. From **INTENT MANAGEMENT** under **WORKFLOWS**, click **Interconnect Connectivity**.

   Cisco SD-WAN Manager displays all the configured Interconnect Connections in a table.

4. Find the Interconnect Connection of interest.

Tip Search for the Interconnect Connection using the name you entered for it during configuration.

5. Scroll to the right to view the **Connection License SKU UUID** column. On the **Account Licenses** page, use this SKU UUID to view more information about the license SKU.

   The **License End Date** column displays the expiry date for the Interconnect Connection license.

   For an AWS hosted connection, Cisco SD-WAN Manager displays the following details:

   - The **AWSHC License UUID** column displays the SKU UUID for the supplemental AWS hosted connection license. On the **Account Licenses** page, use this SKU UUID to view more information about the license SKU.
   - the **AWSHC License End Date** column displays the expiry date for the supplemental AWS hosted connection license.

Related Topics

View Licenses Associated with a Megaport Account, on page 196

Configure Cisco Catalyst SD-WAN Multi-Region Fabric

Table 50: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric (also Hierarchical SD-WAN)	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can use Cisco SD-WAN Manager to enable and configure Multi-Region Fabric, which provides the ability to divide the architecture of the Cisco Catalyst SD-WAN overlay network into multiple regional networks that operate distinctly from one another.
Re-Origination Dampening	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	In networks experiencing instability, TLOCs and bidirectional forwarding detection (BFD) tunnels may alternate repeatedly between being available and unavailable. This causes the overlay management protocol (OMP) to repeatedly withdraw and re-originate routes. This churn adversely affects Cisco SD-WAN Controller performance. Adding a delay before re-originating routes that have gone down repeatedly prevents excessive churn, and prevents this type of network instability from diminishing Cisco SD-WAN Controller performance.

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Controller Optimizations	Cisco Catalyst SD-WAN Control Components Release 20.10.1	There are two optimizations of Cisco SD-WAN Controller performance: • Cisco SD-WAN Controller optimization of outbound control policy: This feature helps to optimize Cisco SD-WAN Controller performance by streamlining the evaluation of outbound control policies. The controller evaluates the policy only once for all peers rather than reevaluating for each peer. • Cisco SD-WAN Controller resistance to TLOC flapping: When TLOCs cycle between unavailable and available, called flapping, they cause Cisco SD-WAN Controllers to continually readvertise the list of routes to devices in the network. This degrades the performance of Cisco SD-WAN Controllers and devices in the network. To address this and improve performance, Cisco SD-WAN Controllers isolate the disruption to devices that use the same control policy, leaving other devices unaffected.

Enable Multi-Region Fabric

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Multi-Region Fabric** area, enable Multi-Region Fabric.

Note In Cisco SD-WAN Manager Releases 20.7.x and 20.8.x, this area was labeled **Hierarchical SDWAN**.

Assign a Role and Region to a Device Using Cisco SD-WAN Manager

Before You Begin

- Plan the Multi-Region Fabric architecture, and decide on the roles (edge router or border router) and regions for each device in the network.
- This procedure uses a feature template to assign a role. For full information about configuring devices using templates, see Configure Devices.
- For information about the number of interfaces that are supported for each device, see the scale limitations in Restrictions for Multi-Region Fabric.

- From Cisco vManage Release 20.9.1, use Network Hierarchy and Resource Management to create the region that you will use in the following procedure. Creating the region includes assigning a region ID to the region. For information about creating a region, see the Network Hierarchy and Resource Management chapter in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x*.

Assign a Role and Region to a Device

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Select the device type to display the templates available for the device.
5. Click the **System** template.
6. In the **Template Name** field, enter a name for the template.
7. In the **Basic Configuration** section, configure the following fields:

Field	Description
Region ID	Choose a value between 1 and 63 for a region. **Note** From Cisco vManage Release 20.9.1, enter the number of the region that you created for the device using Network Hierarchy and Resource Management, as described in Before You Begin. **Note** By default, all interfaces on the device use the region configured here. For a border router, configure one or more TLOC interfaces to connect to the core region. Other TLOC interfaces on the border router use the region configured here. See Assign Border Router TLOCs to the Core Region Using Cisco vManage.
Role	Choose **Edge Router** or **Border Router**. **Note** Only Cisco IOS XE Catalyst SD-WAN devices can have the **Border Router** role.

8. For a border router, enable the device to function in the core region.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

c. Click **Add Template**.

d. Select the device type to display the templates available for the device.

e. Click the **Cisco VPN Interface Ethernet** template.

f. In the **Tunnel** section, in the **Tunnel Interface** field, click **On** to enable tunnels.

g. In the **Enable Core Region** field, click **On** to enable connections to the core region.

Assign Border Router TLOCs to the Core Region Using Cisco SD-WAN Manager

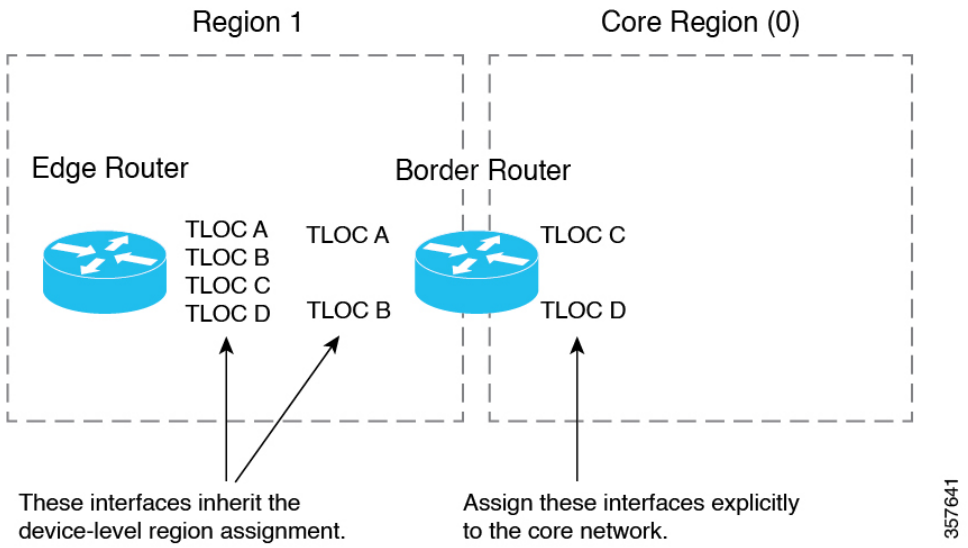
Before You Begin

- Assign the role of border router to the device and assign the device to a region. By default, all interfaces on a device use the region configured for the device. See Assign a Region and Role to a Device Using Cisco vManage.

  For a border router, configure one or more TLOC interfaces to connect to the core region. Other TLOC interfaces on the border router use the region configured for the device.

- This procedure creates a template that assigns interfaces of a specified color to the core region. Before creating the template, configure a color for the interfaces that you want to assign to the core region, or verify that they have a color configured already.

Figure 1: TLOC Interface Region Assignments



Assign Border Router TLOCs to the Core Region

1. Create a Cisco VPN Interface Ethernet template for the TLOC interfaces that you want to connect to the core region.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

   c. Click **Add Template**.
   d. In the **Template Name** field, provide a template name.
   e. In the **Tunnel** section, in the **Tunnel Interface** field, click **On**.
   f. In the **Color** field, specify a color that identifies the interfaces that you want to assign to the core region.
   g. Click **Advanced Options**.
   h. In the **Settings** section, in the **Enable Core Region** field, click **On**.
   i. In the **Basic Configuration** section, in the **Interface Name** field, enter an interface name.
   j. Click **Save**.

2. Add the Cisco VPN Interface Ethernet template that you created in the previous step to a device template.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

   c. Click **Create Template** and choose **From Feature Template**.
   d. In the **Transport & Management VPN** section, locate the **Additional Cisco VPN 0 Templates** list and click **Cisco VPN Interface Ethernet**.

      This adds a new line to the **Transport & Management VPN** section, labelled **Cisco VPN Interface Ethernet**, with a menu for selecting an interface.
   e. In the new **Cisco VPN Interface Ethernet** line, click the menu and select the Cisco VPN Interface Ethernet template that you created in an earlier step.
   f. Click **Update**.

3. Apply the device template to the border router device.

Assign Regions to a Cisco Catalyst SD-WAN Controller Using Cisco SD-WAN Manager

Before You Begin

- Plan the Multi-Region Fabric architecture, and decide on the roles (edge router or border router) and regions for each device in the network. Plan which Cisco SD-WAN Controllers should serve each region.
- This procedure uses a feature template to assign a role. For full information about configuring devices using templates, see Configure Devices.
- For restrictions that apply to Cisco SD-WAN Controllers, see Restrictions for Multi-Region Fabric.

Assign Regions to a Cisco SD-WAN Controller

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. For the device type, select **vSmart**.
5. Click the **System** template.
6. In the **Template Name** field, enter a name for the template.
7. In the **Basic Configuration** section, in the **Region ID List** field, enter a region or region list.
8. Apply the template to the Cisco SD-WAN Controller.

View OMP Peers Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** at the right of the desired border router and choose **Real Time**.
3. In the left pane, click **Real Time**.
4. In the **Device Options** field, enter **OMP Peers**.

   A table shows peer information, similarly to the **show sdwan omp peers** CLI command. In the output, check the **REGION ID** column, which shows one of the following for each peer.

   - **None**: A Cisco SD-WAN Controller that has not been configured to operate with Multi-Region Fabric. This includes the default region Cisco SD-WAN Controllers configured before migration to Multi-Region Fabric.
   - **0**: Core region Cisco SD-WAN Controllers.
   - *access-region-id*: Access region Cisco SD-WAN Controllers.

Verify Connectivity Between Devices Using Cisco SD-WAN Manager

Use this procedure to trace the route between two devices, such as two edge devices in different regions to verify connectivity between the devices.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** adjacent to the desired border router and choose **Real Time**.
3. In the left pane, click **Troubleshooting**.
4. Click **Trace Route**.
5. In the **Destination IP** field, enter an IP address for the endpoint of the route tracing.
6. Click the **VPN** drop-down list and choose the VPN for the route tracing.

Verify That a Border Router is Re-Originating Routes Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** adjacent to the desired border router and choose **Real Time**.
3. In the left pane, click **Real Time**.
4. In the **Device Options** field, enter **OMP Received Routes**.

Locate the rows of the table that show 0.0.0.0 in the **Peer** column. These rows correspond to routes from the border router itself. If the border router is re-originating routes, then in those rows, the **Region Path** column shows two numbers for the route, including a 0 for the core region, and the **Status** column shows **BR-R** (border router re-originated).

Use Regions With a Centralized Policy

Create a Region List Using Cisco SD-WAN Manager

Region lists are useful when creating a region match condition for a centralized policy.

Create a Region List

1. In the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. Click **Add Policy**.
4. In the list area, click **Region**.
5. Click **New Region List**.
6. Enter the following:
    - **Region List Name**: Name for the new list.

- **Add Region**: One or more region numbers in the range of 1 to 63, using to the instructions in the field.

7. Click **Add**.

Add a Region Match Condition to a Centralized Policy

After you configure regions for Multi-Region Fabric, you can specify a region or region list as a match condition when configuring centralized route policy.

For complete information about working with centralized policy, see the Centralized Policy section of the Cisco SD-WAN Policies Configuration Guide.

Add a Region Match Condition to a Centralized Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options** and in the **Centralized Policy** section, choose **Topology**.
3. Click **Add Topology** and choose **Custom Control**.
4. Click **Sequence Type** and choose **Route**.
5. Click **Sequence Rule**.
6. Click **Match**.
7. Click **Region**.
8. In the **Match Conditions** area, enter a region or region list.

   See Create a Region List Using Cisco vManage.

Attach a Centralized Policy to a Region

After you configure regions for Multi-Region Fabric, specify a region or region list when attaching a centralized policy.

For complete information about working with centralized policy, see the Centralized Policy section of the Cisco SD-WAN Policies Configuration Guide.

Attach a Centralized Policy to a Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. In the table, locate the policy to attach. In the row of the policy, click **…** and choose **Edit**.

   For the **Topology**, **Application-Aware Routing**, and **Traffic Data** options, you can choose to add a new site or new region.
4. Click **New Site/Region List**.
5. Click **Region**.
6. Enter a region ID or region list.

7. Proceed with attaching the policy.

Secondary Regions

Table 51: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Secondary Regions	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	Secondary regions provide another facet to the Multi-Region Fabric architecture and enable direct tunnel connections between edge routers in different primary access regions. When you assign an edge router a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.

Configure a Secondary Region ID for an Edge Router Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a system template for the device.
   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.
4. In the **Basic Configuration** section, in the **Secondary Region ID** field, enable Global mode and enter the number of the secondary region, in the range 1 to 63.
5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure the Secondary Region Mode for a TLOC Using Cisco SD-WAN Manager

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

Before You Begin

This procedure describes how to configure the secondary region mode for a TLOC using a Cisco VPN Interface Ethernet template. For information about how to use the template in general, including how to specify the interface to which it is applied, see Configure VPN Ethernet Interface in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

Configure the Secondary Region Mode for a TLOC

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a Cisco VPN Interface Ethernet template for the device.
   - In the table, locate the existing Cisco VPN Interface Ethernet template for the device. In the row for the template, click **…** and choose **Edit**.
4. Navigate to the **Tunnel** section, and within that section the **Advanced Options** section.
5. In the **Enable Secondary Region** field, enable Global mode and choose one of the following options:

Option	Description
Only in Secondary Region	Configure the interface to handle only traffic in the secondary region.
Shared Between Primary and Secondary Regions	Configure the interface to handle traffic in the primary and secondary regions.

Note The interface inherits the secondary region assignment configured for the device at the system level.

6. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a Cisco OMP template for the device.
   - In the table, locate the existing OMP template for the device. In the row for the template, click **…** and choose **Edit**.
4. Navigate to the **Best Path** section, and in the **Ignore Region-Path Length During Best-Path Algorithm** field, choose **On**.

   When you select **On**, the template automatically selects **Direct-Tunnel Path** and **Hierarchical Path**.

Note The default value is Off, and by default, OMP gives preference to a direct tunnel path over a hierarchical path because the direct path has fewer hops.

5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Transport Gateways

Table 52: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Transport Gateways	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	An edge router or border router that has connections to two networks that lack direct connectivity can function as a transport gateway. This is helpful for enabling connectivity between routers that are configured to be within the same access region, but which do not have direct connectivity.

Enable Transport Gateway Functionality on a Router Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a system template for the device.
   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.
4. In the **Basic Configuration** section, in the **Transport Gateway** field, choose **On**.
5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure the Transport Gateway Path Preference Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create an OMP template for the device.

- In the table, locate the existing OMP template for the device. In the row for the template, click **...** and choose **Edit**.

4. In the **Best Path** section, in the **Transport Gateway Path Behavior** field, choose Global mode and choose one of the following options:

Option	Description
Do ECMP Between Direct and Transport Gateway Paths	For devices that can connect through a transport gateway and through direct paths, apply equal-cost multi-path (ECMP) to all available paths.
Prefer Transport Gateway Path	For devices that can connect through a transport gateway, use only the transport gateway paths, even if other paths are available.

5. (Optional) From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can click the **Site Types** field and choose one or more site types to which to apply the transport gateway behavior. For information about how the Site Types parameter operates together with the Transport Gateway Path Behavior parameter, see OMP Best Path Logic and Transport Gateway Path Preference.

6. Click **Save** if creating a new template, or **Update** if editing an existing template.

Router Affinity

Table 53: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Router Affinity	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	Often a router has multiple options to choose for the next hop when routing a flow to its destination. When multiple devices can serve as the next hop for a flow, you can specify the order of preference among the devices by configuring router affinity groups. The result is that a router attempts to use a route to the next-hop device of highest preference first, and if that device is not available, it attempts to use a route to the next-hop device of the next lower preference. Affinity groups enable this functionality without requiring complex control policies.
Improved Prioritization of Routes to Peer Devices in the Affinity Group Preference List	Cisco Catalyst SD-WAN Control Components Release 20.9.1	This feature introduces a change to the order in which Cisco SD-WAN Controllers advertise routes to devices. From this release, when Cisco SD-WAN Controllers advertise routes to a device, they (a) give higher priority to routes to peer devices in the affinity group preference list, and (b) lower priority to routes that may have a higher best path score, but are not routes to a device associated with a preferred affinity group. The effect is to prioritize routes to peer devices in preferred affinity groups.

Feature Name	Release Information	Description
Support for Affinity Groups for Service Routes and TLOC Routes	Cisco Catalyst SD-WAN Control Components Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature extends support of affinity group assignments to service routes and TLOC routes. A common use for this is to add further control to routing by using affinity group preference together with control policies that match service routes and TLOC routes.
Set Affinity Group by Control Policy	Cisco Catalyst SD-WAN Control Components Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	You can configure a control policy to match specific TLOCs or routes and assign them an affinity group value, overriding the affinity group that they inherit from the router.

Configure Router Affinity Groups Using Cisco SD-WAN Manager

Configure an Affinity Group or Affinity Group Preference on a Device, Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a system template for the device.
   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.
4. To assign an affinity group to a border router, in the **Advanced** section, in the **Affinity Group** field, change the mode to **Global** and enter an affinity group number, in the range 1 to 63.

   If an affinity group has been configured previously on the device, the new value replaces the previous.
5. To configure an affinity group preference order for a border router or an edge router, in the **Advanced** section, in the **Affinity Group Preference** field, change the mode to **Global** and enter a comma-separated list of affinity group numbers. This determines the order of preference for connecting to border routers. The affinity groups are in the range 1 to 63.

   Example: 10, 11, 1, 5

Note If you configure a Cisco SD-WAN Controller to filter out routes that are not in the affinity group preference list, then the device can only connect to routers in the affinity group. See Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager, on page 212.

6. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager

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

Before You Begin

The last step of this procedure requires logging in to the Cisco SD-WAN Controllers that serve the regions where you are configuring this, to execute a command using the CLI.

Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create an OMP template for a Cisco SD-WAN Controller.
   - In the table, locate the existing OMP template for the Cisco SD-WAN Controller. In the row for the template, click **…** and choose **Edit**.
4. In the **Best Path** section, in the **Enable Filtering Route Updates Based on Affinity** field, choose **Global** mode and choose **On**.
5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the Cisco SD-WAN Controllers using the template.
6. Connect to each Cisco SD-WAN Controller and clear OMP routes to ensure that only the paths in the affinity group preference list are used.

```
Controller#config terminal
Controller(config)#omp
Controller(config-omp)#filter-route outbound affinity-group-preference
Controller(config-filter-route)#exit
Controller(config-omp)#exit
Controller(config)#exit
Controller#clear omp all
```

Multi-Region Fabric Policy

Table 54: Feature History

Feature Name	Release Information	Description
Match Traffic by Destination: Access Region, Core Region, or Service VPN	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can apply a policy to traffic whose destination is any one of the following—access region, core region, service VPN. Use this match condition for data policy or application route policy on a border router.
Match Routes According to Path Type	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	When configuring a control policy for a Multi-Region Fabric architecture, you can match routes according to whether the route uses a hierarchical path, a direct path, or a transport gateway path.
Match Routes by Region and Role in a Control Policy	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco Catalyst SD-WAN Control Components Release 20.8.1	In a control policy, you can match routes according to the region of the device originating the route, or the role (edge router or border router) of the device originating the route.
Match Traffic by Destination Region	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	When creating an application route policy or data policy, you can match traffic according to its destination region. The destination may be a device in the same primary region, the same secondary region, or neither of these.
Specify Path Type Preference	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco Catalyst SD-WAN Control Components Release 20.9.1	When configuring a centralized policy, you can create a preferred color group list, which specifies three levels of route preference, called primary, secondary and tertiary. The route preferences are based on TLOC color and, optionally, on the path type—direct tunnel, multi-hop path, or all paths. Path type is relevant to networks using Multi-Region Fabric.
Subregions in Policy	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Subregions are defined domains within access regions. You can specify subregions when creating region lists, configuring policies, and applying policies.
Enhancements to Match Conditions	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	When configuring match conditions for a policy, you can specify to match to all access regions, or to match according to a subregion.

Configure Multi-Region Fabric Policy Using Cisco SD-WAN Manager

Configure a Data Policy or Application Route Policy to Match Traffic-To Using Cisco SD-WAN Manager

Before You Begin

Configure a VPN list to use when applying the policy.

Configure a Data Policy or Application Route Policy to Match Traffic-To

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policies**.
3. Do one of the following:
   - To create a new policy, click **Add Policy**.
   - To edit an existing policy, click **…** in the row of the policy and click **Edit Policy**.
4. Click **Next**.
5. Click **Next**.
6. Click one of the following to create a traffic policy:
   - **Application Aware Routing**
   - **Traffic Data**
7. Click **Add Policy** and choose **Create New**.

Note To reuse an existing policy, you can choose **Import Existing**.

8. Enter a name and description for the new policy.
9. Click **Sequence Type** and choose **Custom**.
10. Click **Sequence Rule**.
11. Click **Match** (selected by default) and click **Traffic To**.
12. In the **Match Conditions** area, in the **Traffic To** field, choose one of the following:
    - **Access**
    - **Core**
    - **Service**
13. Choose an action for the sequence and complete the configuration of the policy.

    For information about creating traffic policies in general, see Centralized Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.

14. To save the policy, click **Save Application Aware Routing Policy** or **Save Data Policy**, depending on the type of policy that you are creating. A table shows the new policy.
15. Click **Next**.
16. At the **Apply Policies to Sites and VPNs** step, enter the name of the policy to apply.
17. Click one of the following, depending on the type of policy that you are creating and applying:
    - **Application-Aware Routing**
    - **Traffic Data**
18. Click **New Site/Region List and VPN List**.
19. If you are configuring a traffic data policy, choose one of the following options:
    - **From Service**
    - **From Tunnel**
    - **All**
20. Choose one of the following options to configure the sites or Multi-Region Fabric regions to which to apply the policy:
    - **Site List**: Enter a site list.
    - **Region**: Enter a Multi-Region Fabric region ID or select a region list.
21. If you are configuring a data policy, do the following:
    a. In the **Select VPN List** field, choose a VPN list.
    b. Click **Add**.
22. Click **Role Mapping for Regions**.
23. For each region ID or region list, in the **Role** column, choose a role of **Edge** or **Border**. If you do not choose a role, Cisco SD-WAN Manager applies the policy to all routers in the region.

Note For policies that match by Traffic-To, choose **Border**. This match condition has no effect on edge routers.

24. Click **Save Policy**. A table shows the new policy. Optionally, to view the details of the policy, in the row of the policy, click **…** and choose **Preview**.

Configure a Control Policy to Match Region and Role Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policies**.
3. Do one of the following:
    - To create a new policy, click **Add Policy**.

- To edit an existing policy, click **…** in the row of the policy and click **Edit Policy**.

4. Click **Next**.
5. In the **Configure Topology and VPN Membership** step, click **Add Topology** and choose **Custom Control (Route & TLOC)**.
6. Enter a name and description for the new policy.
7. Click **Sequence Rule**.
8. Click **Match** (selected by default) and click **Region**.
9. In the **Match Conditions** area, do one of the following:
   - In the **Region List** field, enter a preconfigured region list name.

Note You can click the field and choose **New Region List** to define a list.

   - In the **Region ID** field, enter a single region ID.

10. (Optional) To specify a router type within the configured regions, click **Role** and choose **Border** or **Edge**.
11. Choose an action for the sequence and complete the configuration of the policy.

    For information about creating traffic policies in general, see Centralized Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.
12. To save the policy, click **Save Control Policy**. A table shows the new policy.
13. Click **Next**.
14. At the **Apply Policies to Sites and VPNs** step, enter the name of the policy to apply
15. Click **Topology**.
16. Click **New Site/Region List**.
17. Choose one of the following options to configure the sites or Multi-Region Fabric regions to which to apply the policy:
    - **Site List**: Enter a site list.
    - **Region**: Enter a Multi-Region Fabric region ID or select a region list.
18. Click **Role Mapping for Regions**.
19. For each region ID or region list, in the **Role** column, choose a role of **Edge** or **Border**. If you do not choose a role, Cisco SD-WAN Manager applies the policy to all routers in the region.

Note For policies that match by Traffic-To, choose **Border**. This match condition has no effect on edge routers.

20. Click **Save Policy**. A table shows the new policy. Optionally, to view the details of the policy, in the row of the policy, click **…** and choose **Preview**.

Match Traffic According to the Destination Region Using Cisco SD-WAN Manager

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

For complete information about configuring an application-aware routing (AAR) policy or traffic data policy, see Configure Centralized Policies Using Cisco vManage in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. The information here only addresses how to use the **Destination Region** match condition.

Use the following procedure for an application-aware policy or a traffic data policy.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Choose **Centralized Policy**, which is selected by default.
3. Click **Add Policy**.
4. Optionally, you can click a list type and define a list.
5. Click **Next**.
6. Optionally, add a topology.
7. Click **Next**.
8. Do one of the following:
   - For an AAR policy, click **Application Aware Routing**, which is selected by default.
   - For a traffic data policy, click **Traffic Data**.
9. Click **Add Policy** and select **Create New**.
10. Do one of the following:
    - For an AAR policy, click **Sequence Type** to create a sequence that matches traffic by destination.
    - For a traffic data policy, click **Sequence Type** and choose **Custom** to create a sequence that matches traffic by destination.
11. Click **Sequence Rule** to create a new rule for the sequence.
12. With the **Match** option selected, click **Destination Region** to add this option to the match conditions area of the sequence rule.
13. In the **Match Conditions** area, click the **Destination Region** field and choose one of the following:
    - **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using the access-region bidirectional forwarding detection (BFD).
    - **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions.

- **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination.

14. Continue to configure the policy as described in Configure Centralized Policies Using Cisco vManage, cited earlier in this section.

Configure the Path Preference for a Preferred Color Group List Using Cisco SD-WAN Manager

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

For complete information about configuring an application-aware routing (AAR) policy, see Configure Centralized Policies Using Cisco vManage in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. The information here only addresses how to configure a path preference as part of a preferred color group.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**, and choose **Centralized Policy**.
2. Click **Add Policy**.
3. Click **Application List**, which is selected by default.
4. Click **Preferred Color Group**.
5. Click **New Preferred Color Group**.
6. Configure the following fields:

Field	Description
Preferred Color Group Name	Enter a name for the color group.
Primary Colors: **Color Preference**	Click the field and select one or more colors for the primary preference.

Field	Description
Primary Colors: **Path Preference**	Click the drop-down list and choose one of the following for the primary preference: • **Direct Path**: Use only a direct path between the source and the destination devices. **Note** Do not use this option in a non-Multi-Region Fabric network. • **Multi Hop Path**: In a Multi-Region Fabric network, use a multi-hop path, which includes the core region, between the source and destination devices, even if a direct path is available. • **All Paths**: Use any path between the source and destination devices. **Note** This option is equivalent to not configuring path preference at all. If you are applying the policy to a non-Multi-Region Fabric network, use this option.
Secondary Colors: **Color Preference** **Path Preference**	Configure the secondary preference using the same method as for the **Primary Colors** options.
Tertiary Colors: **Color Preference** **Path Preference**	Configure the tertiary preference using the same method as for the **Primary Colors** options.

Use a Preferred Color Group in a Policy

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

For complete information about configuring policies, see Configure Centralized Policies Using Cisco vManage in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. The information here only addresses how to use the **Preferred Color Group** action, which incorporates path preference.

Use the following procedure for an application-aware policy or a traffic data policy.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Add Policy**.
3. Choose **Centralized Policy**, which is selected by default.
4. Click **Add Policy**.

5. Optionally, you can click a list type and define a list.
6. Click **Next**.
7. Optionally, add a topology.
8. Click **Next**.
9. Do one of the following:
   - For an AAR policy, click **Application Aware Routing**, which is selected by default.
   - For a traffic data policy, click **Traffic Data**.
10. Click **Add Policy** and select **Create New**.
11. Do one of the following:
    - For an AAR policy, click **Sequence Type** to create a sequence that matches traffic by destination.
    - For a traffic data policy, click **Sequence Type** and choose **Custom** to create a sequence that matches traffic by destination.
12. Click **Sequence Rule** to create a new rule for the sequence.
13. Click **Actions**.
14. For an AAR policy, do the following:
    a. Click **SLA Class List**.
    b. Click the **Preferred Color Group** field and choose a preferred color group.
15. For an traffic control policy, do the following:
    a. Click **Accept**.
    b. Click **Preferred Color Group**.
    c. Click the **Preferred Color Group** field and choose a preferred color group.

Configure Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN Devices

Table 55: Feature History

Feature Name	Release Information	Description
Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy the Cisco ThousandEyes Enterprise agent on supported Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager

Feature Name	Release Information	Description
Cisco ThousandEyes Support for Cisco 1000 Series Integrated Services Routers	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco ISR 1100X-6G devices. You can install and activate the Cisco ThousandEyes Enterprise agent through Cisco SD-WAN Manager.
Cisco ThousandEyes Support for Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers. You can install and activate the Cisco ThousandEyes Enterprise agent through Cisco SD-WAN Manager.

Upload Cisco ThousandEyes Enterprise Agent Software to Cisco SD-WAN Manager

1. Download the latest version of Cisco ThousandEyes Enterprise agent software from the Cisco ThousandEyes Agent Settings page.
2. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
3. Click **Virtual Images**.
4. Click **Upload Virtual Image** and click **vManage**.
5. In the **Upload VNF's Package to vManage** dialog box, browse to the location of the downloaded Cisco ThousandEyes Enterprise agent software file and select the file.

   Alternatively, drag and drop the Cisco ThousandEyes Enterprise agent software file.
6. Enter a description for the file.
7. (Optional) Add desired tags.
8. Click **Upload**.

Provision Cisco ThousandEyes Enterprise Agent in Transport VPN (VPN 0)

You can provision the Cisco ThousandEyes Enterprise agent in VPN 0 for more visibility into the performance of underlay networks beyond the Cisco Catalyst SD-WAN fabric. The Cisco ThousandEyes Enterprise agent does not probe the Cisco Catalyst SD-WAN fabric when provisioned in VPN 0.

Prerequisites

- Ensure that the appropriate DNS and NAT configuration exists to enable the Cisco ThousandEyes Enterprise agent to discover and connect to the Cisco ThousandEyes application.
- Upload Cisco ThousandEyes Enterprise agent software to Cisco SD-WAN Manager.

Note If you have uploaded more than one version of the Cisco ThousandEyes Enterprise agent software to the Cisco SD-WAN Manager software repository, while provisioning the agent, Cisco SD-WAN Manager installs and activates the latest version of the agent software.

Procedure

1. Create feature template for the Cisco ThousandEyes Enterprise agent:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

   c. Choose the supported devices to which you want to apply this template.
   d. In the **Other Templates** section, click **ThousandEyes Agent**.
   e. **Template Name**: Enter a name for the template. Ensure that the template name is unique.
   f. **Description**: Enter a description for the template.
   g. In the **BASIC CONFIGURATION** section, enter the Cisco ThousandEyes **Account Group Token**.
   h. In the **ADVANCED** section, enter the IP address of your preferred **Name Server**.

Note From Cisco vManage Release 20.7.1 and Cisco IOS XE Release 17.7.1a, this step is optional.

   i. Click **Save**.

2. Attach the ThousandEyes Agent feature template to device template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

   c. Find the device template for the target device.
   d. For this template, click **…** and then click **Edit**.
   e. Click **Additional Templates**.
   f. In the **Additional Templates** section, choose the **ThousandEyes Agent** feature template created earlier.

g. Click **Update**.

h. Update necessary variables, if any, and click **Next**.

i. Review the configuration and click **Configure Devices**.

3. Repeat **Step 2** for each device on which you want to deploy the Cisco ThousandEyes Enterprise agent.

The Cisco ThousandEyes Enterprise agent is deployed on the chosen devices. The agent registers with and establishes secure communication with the cloud-based Cisco ThousandEyes application to receive necessary updates and configuration. You can configure various tests and see resultant network and application telemetry data on the Cisco ThousandEyes portal.

Provision Cisco ThousandEyes Enterprise Agent in a Service VPN

You can provision the Cisco ThousandEyes Enterprise agent in a service VPN for more visibility into the performance of the Cisco Catalyst SD-WAN overlay and underlay networks.

Prerequisites

- Ensure that the appropriate DNS and NAT configuration exists to enable the Cisco ThousandEyes Enterprise agent to discover and connect to the Cisco ThousandEyes application.
- Upload Cisco ThousandEyes Enterprise agent software to Cisco SD-WAN Manager.

Note If you have uploaded more than one version of the Cisco ThousandEyes Enterprise agent software to the Cisco SD-WAN Manager software repository, while provisioning the agent, Cisco SD-WAN Manager installs and activates the latest version of the agent software.

Procedure

1. Create feature template for the Cisco ThousandEyes Enterprise agent:

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

   b. Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

   c. Choose the supported devices to which you want to apply this template.

   d. In the **Other Templates** section, click **ThousandEyes Agent**.

   e. **Template Name**: Enter a name for the template. Ensure that the template name is unique.

   f. **Description**: Enter a description for the template.

   g. In the **BASIC CONFIGURATION** section, configure the following:

Account Group Token	Enter the Cisco ThousandEyes Account Group Token.
VPN	1. Set the VPN configuration as a **Global** or a **Device Specific** setting. 2. Enter the ID of the service VPN in which you want to provision the Cisco ThousandEyes Enterprise agent.
Agent IP Address	Enter an IP address for the Cisco ThousandEyes Enterprise agent. This IP Address should be unique within the fabric and should not overlap with the IP addresses of other branch agents.
Agent Default Gateway	Enter a default gateway address. This IP address is assigned to the virtual port group of the router.

Tip You can create and allocate a service subnet for the agent network. Two usable IP addresses are required to provision the Cisco ThousandEyes Enterprise agent on each Cisco IOS XE Catalyst SD-WAN device. One of the IP addresses must be assigned to the agent and second IP address to the router virtual port group.

h. In the **ADVANCED** section, configure the following:

Name Server	(Optional parameter from Cisco vManage Release 20.7.1 and Cisco IOS XE Release 17.7.1a) Enter the IP address of your preferred DNS server. This server can exist within or outside the Cisco Catalyst SD-WAN fabric but must be reachable from the service VPN.
Hostname	(Optional) Enter the hostname that the agent must use when registering with the Cisco ThousandEyes portal. By default, the agent uses the Cisco IOS XE Catalyst SD-WAN device's hostname.
Web Proxy Type	(Optional) If the Cisco ThousandEyes Enterprise agent must use proxy server for external access, choose one of the following as proxy type: • **Static** • **PAC** Static proxy settings: • **Proxy Host**: Set the configuration as a **Global** setting and enter the hostname of the proxy server. • **Proxy Port**: Set the configuration as a **Global** setting and enter the port number of the proxy server. PAC settings: • **PAC URL**: Set the configuration as a **Global** setting and enter the URL of the proxy auto-configuration (PAC) file.

i. Click **Save**.

2. Attach the ThousandEyes Agent feature template to device template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

   c. Find the device template for the target device.
   d. For this template, click **…**, and click **Edit**.
   e. Click **Additional Templates**.
   f. In the **Additional Templates** section, choose the **ThousandEyes Agent** feature template created earlier.
   g. Click **Update**.
   h. Update necessary variables, if any, and click **Next**.
   i. Review the configuration and click **Configure Devices**.
3. Repeat **Step 2** for each device on which you want to deploy the Cisco ThousandEyes Enterprise agent.

The Cisco ThousandEyes Enterprise agent is deployed on the chosen devices. The agent registers with and establishes secure communication with the cloud-based Cisco ThousandEyes application to receive necessary updates and configuration. You can configure various tests and see resultant network and application telemetry data on the Cisco ThousandEyes portal.

Upgrade Cisco ThousandEyes Enterprise Agent Software

Note You cannot upgrade the Cisco ThousandEyes Enterprise agent software on Cisco IOS XE Catalyst SD-WAN devices that do not have external storage. In such devices, the bootflash is used to install and launch the agent. Bootflash does not have the storage capacity to support agent software upgrade. Instead of upgrading the agent software, you can uninstall the existing software and provision the new version of the software.

1. Download a new version of Cisco ThousandEyes Enterprise agent software and upload the software to Cisco SD-WAN Manager. See *Upload Cisco ThousandEyes Enterprise Agent Software to Cisco SD-WAN Manager*.
2. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
3. Select the Cisco IOS XE Catalyst SD-WAN devices on which you want to upgrade the Cisco ThousandEyes Enterprise agent software.
4. Click **Upgrade Virtual Image**.
5. In the **Virtual Image Upgrade** dialog box, choose the new version of the Cisco ThousandEyes Enterprise agent software from the drop-down list. Click **Upgrade**.

6. On the **Maintenance** > **Software Upgrade** page, select the Cisco IOS XE Catalyst SD-WAN devices on which you upgraded the Cisco ThousandEyes Enterprise agent software.
7. Click **Activate Virtual Image**.

Uninstall Cisco ThousandEyes Enterprise Agent Software

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

3. Find the device template for the device from which the Cisco ThousandEyes agent software must be removed.
4. For this template, click **…** and then click **Edit**.
5. Click **Additional Templates**.
6. In the **Additional Templates** section, for **ThousandEyes Agent** choose **None** from the drop-down list.
7. Click **Update**.
8. Update necessary variables, if any, and click **Next**.
9. Review the configuration and click **Configure Devices**.

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

Table 56: Feature History

Feature Name	Release Information	Description
Azure Government Cloud Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can now configure the geographical regions based on the **Environment** settings of Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.
AWS Government Cloud Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can now configure the geographical regions based on **Environment** settings of Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

Configure Default AAR and QoS Policies Using Cisco SD-WAN Manager

Table 57: Feature History

Feature Name	Release Information	Description
Configure Default AAR and QoS Policies	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure Default AAR and QoS policies.

Follow these steps to configure default AAR, data, and QoS policies using Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Add Default AAR & QoS**.

   The **Process Overview** page is displayed.
3. Click **Next**.

   The **Recommended Settings based on your selection** page is displayed.
4. Based on the requirements of your network, move the applications between the **Business Relevant**, **Default**, and **Business Irrelevant** groups.

Note When customizing the categorization of applications as Business-relevant, Business-irrelevant, or Default, you can only move individual applications from one category to another. You cannot move an entire group from one category to another.

5. Click **Next**.

   On the **Path Preferences (optional)** page, choose the **Preferred** and **Preferred Backup** transports for each traffic class.
6. Click **Next**.

   The **App Route Policy Service Level Agreement (SLA) Class** page is displayed.

   This page shows the default settings for **Loss**, **Latency**, and **Jitter** values for each traffic class. If necessary, customize **Loss**, **Latency**, and **Jitter** values for each traffic class.
7. Click **Next**.

   The **Enterprise to Service Provider Class Mapping** page is displayed.

   a. Select a service provider class option, based on how you want to customize bandwidth for different queues. For further detials on QoS queues, refer to the section **Mapping of Application Lists to Queues**

   b. If necessary, customize the bandwidth percentage values for each queues.

8. Click **Next**.

   The **Define prefixes for the default policies and applications lists** page is displayed.

   For each policy, enter a prefix name and description.

9. Click **Next**.

   The **Summary** page is displayed. On this page, you can view the details for each configuration.

   You can click **Edit** to edit the options that appeared earlier in the workflow. Clicking edit returns you to the relevant page.

10. Click **Configure**.

    Cisco SD-WAN Manager creates the AAR, data, and QoS policies and indicates when the process is complete.

    The following table describes the workflow steps or actions and their respective effects:

    Table 58: Workflow Steps and Effects

Workflow Step	Affects the Following
Recommended Settings based on your selection	AAR and data policies
Path Preferences (optional)	AAR policies
App Route Policy Service Level Agreement (SLA) Class: • Loss • Latency • Jitter	AAR policies
Enterprise to Service Provider Class Mapping	Data and QoS policies
Define prefixes for the default policies and applications	AAR, data, QoS policies, forwarding classes, application lists, SLA class lists

11. To view the policy, click **View Your Created Policy**.

Note To apply the default AAR and QoS policies to the devices in the network, create a centralized policy that attaches the AAR and data policies to the required site lists. To apply the QoS policy to the Cisco IOS XE Catalyst SD-WAN devices, attach it to a localized policy through device templates.

Mapping of Application Lists to Queues

The following lists show each service provider class option, the queues in each option, and the application lists included in each queue. The application lists are named here as they appear on the Path Preferences page in this workflow.

4 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data
- Default
  - Best effort
  - Scavenger

5 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data

- General data
  - Scavenger
- Default
  - Best effort

6 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Video
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
- Mission Critical
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data
- General data
  - Scavenger
- Default
  - Best effort

8 QoS class

- Voice
  - VoIP telephony
- Net-ctrl-mgmt
  - Internetwork control
- Interactive video

    - Multimedia conferencing
    - Real-Time interactive
- Streaming video
    - Broadcast video
    - Multimedia streaming
- Call signaling
    - Signaling
- Critical data
    - Transactional data
    - Network management
    - Bulk data
- Scavengers
    - Scavenger
- Default
    - Best effort

Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS

Points to Consider

- Transit VPCs provide the connection between the Cisco overlay network and the cloud-based applications running on host VPCs. You can provision up to four pairs of redundant Cisco Catalyst SD-WAN cloud devices within each VPC dedicated to function as a transit point for traffic from the branch to host VPCs. The individual Cisco Catalyst SD-WAN devices of each redundant pair are deployed within a different availability zone in the AWS region of the transit VPC. Multiple Cisco Catalyst SD-WAN devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two Cisco Catalyst SD-WAN cloud devices, the transport VPN (VPN 0) connects to a branch router, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.
- The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VPCs to a transit VPC. To add the public IP address of the WAN interface, configure the VPN interface ethernet template with GigabitEthernet2 interface for the devices used in Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. In Cisco CSR1000V and Cisco Catalyst 8000V devices, the tunnel interface is on the GigabitEthernet2 interface. .

- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS supports autoscale for AWS. To use the AWS autoscale feature, ensure that you associate one to four pairs of Cisco Catalyst SD-WAN cloud devices with a transit VPC.
- Host VPCs are virtual private clouds in which your cloud-based applications reside. When a transit VPC connects to an application or application provider, it's simply connecting to a host VPC.
- All host VPCs can belong to the same AWS account, or each host VPC can belong to a different account. You can map a host that belongs to one AWS account to a transit VPC that belongs to a different account. You configure cloud instances or cloud accounts by using the Cloud OnRamp configuration wizard.

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

If you're configuring Cisco Catalyst SD-WAN Cloud OnRamp for IaaS the first time, no cloud instances appear in the screen. A cloud instance corresponds to an AWS account with one or more transit VPCs created within an AWS region.

Step 2 Click **Add New Cloud Instance**.

Step 3 Click the **Amazon Web Services (AWS)** radio button.

Step 4 In the next pop-up window, perform the following:

a) To log in to the cloud server, click **IAM Role** or **Key**. We recommend that you use IAM Role.

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

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

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

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

```
{

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

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]

}
```

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

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

2. Create an IAM role on an AWS account that you want to use for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

   a. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require external ID** and pasting the external Id that you noted in Step 4(b).

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

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

      In the **Summary** window, note the **Role ARN**.

      Note You can enter this role ARN value when you choose the IAM role in Step 4(b).

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

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

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

c) If you click the **Key** radio button:

1. In the **API Key** field, enter your Amazon API key.
2. In the **Secret Key** field, enter the password associated with the API key.
3. From the **Environment** drop-down list, choose **commercial** or **govcloud**.

   By default, commercial environment is selected. You can choose the geographical regions based on the environment specifications.

Step 5 Click **Login** to log in to the cloud server.

The cloud instance configuration wizard appears. This wizard consists of three screens that you use to select a region, add a transit VPC, discover host VPCs, and map host VPCs to transit the VPC. A graphic on each wizard screen illustrates the steps in the cloud instance configuration process. The steps that aren't yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

Step 6 Select a region:

From the **Choose Region** drop-down list, choose a region where you want to create the transit VPC.

Step 7 Add a transit VPC:

a) In the **Transit VPC Name** field, enter the transit VPC name.

The name can contain 128 alphanumeric characters, hyphens (–), and underscores (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VPC:

1. In the **WAN Edge Version** drop-down list, choose the software version of the Cisco Catalyst SD-WAN cloud device to run on the transit VPC.
2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of the Cisco Catalyst SD-WAN cloud devices that run on the transit VPC.
   - See the Supported Instance Types topic for Cisco CSR1000V devices of the *Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services*.
   - See the Supported Instance Types topic for Cisco Catalyst 8000V in the *Deploying Cisco Catalyst 8000V on Amazon Web Services*.

   Note We recommend that you choose the following size:

   For Cisco CSR1000V and Cisco Catalyst 8000V, choose c5 instance type with four or more than four vCPUs, such as c5.xlarge (4 vCPU).
3. In the **Max. Host VPCs per Device Pair** field, select the maximum number of host VPCs that can be mapped to each device pair for the transit VPC. Valid values are 1–32.
4. To set up the transit VPC devices for Direct Internet Access (DIA), click one of the following:
   - **Disabled**: No Internet access.
   - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.
   - **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.
5. In the **Device Pair 1#** field, choose the serial numbers of each device in the pair. To remove a device serial number, click **X** that appears in the field.

   The serial numbers of the devices that appear are associated with a configuration template and supports the Cisco Catalyst SD-WAN WAN edge version that you selected in Step 1.
6. To add more device pairs, click  .

   To remove a device pair, click  .

   A transit VPC can be associated with one to four device pairs. To enable the autoscale feature on AWS, associate at least two device pairs with the transit VPC.
7. Click **Advanced**, if you wish to enter more specific configuration options:
   a. In the **Transit VPC CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16. There must be sufficient address space to create six subnets within the CIDR block.
   b. (Optional) In the **SSH PEM Key** drop-down list, choose a PEM key pair to log into an instance. The key pairs are region-specific. See the AWS Documentation for instructions about creating key pairs.

8. To complete the transit VPC configuration, click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

   With this cloud instance, a single transit VPC with two Cisco Catalyst SD-WAN cloud devices has been created. You can configure multiple transit VPCs within a single cloud instance (AWS account within a region). When multiple transit VPCs exist within a cloud instance, you can map host VPCs to any one of the transit VPCs.

9. Discover host VPCs:

   a. In the **Select an account to discover** field, choose the AWS account from which you wish to discover host VPCs.

      Alternatively, to add a new AWS account from which you wish to discover host VPCs, click **New Account**.

   b. Click **Discover Host VPCs**.

      A table appears that display the VPCs, which are available to be mapped to a transit VPC. Only the host VPCs in the selected AWS account and within the same AWS region as the transit VPC appears.

   c. In the table that appears, check one or more hosts to map to the transit VPC.

      To filter the search results, use the Filter option in the search bar and display only host VPCs that match specific search criteria.

      Click the **Refresh** icon to update the table with current information.

      Click the **Show Table Columns** icon to specify which columns to be displayed in the table.

10. Map the host VPCs to a transit VPC:

    a. In the table with all host VPCs, choose the desired host VPCs.

    b. Click **Map VPCs**. The Map Host VPCs pop-up opens.

    c. In the **Transit VPC** drop-down list, choose the transit VPC to map to the host VPCs.

    d. In the **VPN** drop-down list, choose a service VPN in the overlay network in which to place the mapping.

    e. Enable the **Route Propagation** option if Cisco SD-WAN Manager automatically propagates route to the host VPC routes table.

       By default, **Route Propagation** is disabled.

    f. Click **Map VPCs**.

After a few minutes, the **Task View** screen appears, confirming that the host VPC has been mapped to the transit VPC.

Note When configuring the VPN feature template for VPN 0 for the two Cisco Catalyst SD-WAN cloud devices that form the transit VPC, ensure that the color you assign to the tunnel interface is a public color, and not a private color. The following are the public colors:

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure

In the configuration process, map one or more host VNets to a single transit VNet. When mapping, you're configuring the cloud-based applications that branch users can access.

The mapping process establishes IPsec and BGP connections between the transit VNet and each host VNet. The IPsec tunnel that connects the transit and host VNet runs IKE to provide security for the connection. For Azure, the IPsec tunnel uses IKE version 2. The BGP connection that is established over the secure IPsec tunnel allows the transit and host VNet to exchange routes. The BGP connections or the BGP routes are then re-distributed into OMP within the Cisco Catalyst SD-WAN cloud devices, which then advertises the OMP routes to the Cisco SD-WAN Controller in the domain. The transit VNet can then direct traffic from the branch to the proper host VNet and to the proper cloud-based application.

During the mapping process, the IPsec tunnels and BGP peering sessions are configured and established automatically. After establishing the mappings, you can view the IPsec and BGP configurations in the VPN Interface IPsec and BGP feature configuration templates, and modify them as necessary.

Points to Consider:

To configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Azure, create Azure transit VNets, each of which consist of a pair of routers. Then, map the host VNets to transit VNets that exist in the Azure cloud. All VNets reside in the same resource group.

- Transit VNets provide the connection between the overlay network and the cloud-based applications running on the host VNet. Each transit VNet consists of two cloud devices that reside in their own VNet. Two cloud devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two cloud devices, the transport VPN (VPN 0) connects to the simulated branch device, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.
- The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VNets to a transit VNet. To add the public IP address of the WAN interface, configure the VPN Interface Ethernet template with GigabitEthernet2 interface for the devices used in Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. In Cisco CSR1000V and Cisco Catalyst 8000V, the tunnel interface is on the GigabitEthernet2 interface.
- Host VNets are virtual private clouds in which your cloud-based applications reside. When a transit VNet connects to an application or application provider, it's simply connecting to a host VNet.

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

Step 2 Click **Add New Cloud Instance**

Step 3 Click the **Microsoft Azure** radio button.

Step 4 In the next pop-up screen, perform the following:

a) In the **Subscription ID** field, enter the ID of the Microsoft Azure subscription you want to use as part of the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow.

b) In the **Client ID** field, enter the ID of an existing application or create a new application. To create an application, go to your **Azure Active Directory** > **App Registrations** > **New registration**. See Microsoft Azure documentation for more information on creating an application.

c) In the **Tenant ID** field, enter the ID of your account. To find the tenant ID, go to your Microsoft Azure Active Directory and click **Properties**.

d) In the **Secret Key** field, enter the password associated with the client ID.

e) In the **Environment** field, choose **commercial** or **GovCloud**.

By default, commercial environment is selected. You can choose the geographical locations based on the environment specifications.

f) Click **Login**.

The cloud instance configuration wizard opens.

The wizard consists of three screens that you use to select a location, add a transit VNet, discover host VNets, and map host VNets to the transit VNet. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. The steps not yet completed are shown in light gray. The current step is highlighted within a blue box. All completed steps are indicated with a green checkmark and are shown in light orange.

Step 5 From the **Choose Location** drop-down list, choose a location where you want to create the transit VNet.

The locations available are based on the commercial cloud or GovCloud selection.

Step 6 Add a transit VNet:

a) In the **Transit VNet Name** field, type a name for the transit VNet.

The name can contain 32 alphanumeric characters, hyphens (–), and underscore (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VNet:

1. In the **WAN Edge Version** drop-down list, choose the software version to run on the transit VNet. The drop-down list includes the published versions of the device software in the Microsoft Azure marketplace.
2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of theCisco Catalyst SD-WAN cloud devices that run on the transit VNet.
   - See Supported Instance Types for Cisco CSR1000V in the *Cisco CSR 1000v Deployment Guide for Microsoft Azure*.
   - See Supported Instance Types for Cisco Catalyst 8000V in the *Deploying Cisco Catalyst 8000V on Microsoft Azure*.

   Note We recommend that you choose the following size:

   For Cisco CSR1000V and Cisco Catalyst 8000V, choose DS3 instance type with four or more than four vCPUs such as, Standard DS3 v2 (4vCPU).

3. To set up the transit VNet devices for Direct Internet Access (DIA), click one of the following:
   - **Disabled**: No Internet access.
   - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.
   - **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.
4. In the **Device 1** drop-down list, choose the serial number of the first device.
5. In the **Device 2** drop-down list, choose the serial number of the second device in the device pair.
6. Click **Advanced** if you wish to enter more specific configuration options.
7. In the **Transit VNet CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you leave this field empty, the Transit VNet is created with a default CIDR of 10.0.0.0/16.

c) To complete the transit VNet configuration. click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

Step 7 Map host VNets to transit VNets:

a) In the **Select an account to discover** drop-down list, choose your Azure subscription ID.

Alternatively, to add a new Azure account from which you wish to discover host VNets, click **New Account**.

b) Click **Discover Host VNets**.
c) In the **Select a VNet** drop-down list, choose a desired host VNet.
d) Click **Next**.
e) From the table of host VNets, choose a desired host VNet.
f) Click **Map VNets**. The Map Host VNets pop-up appears.
g) In the **Transit VNet** drop-down list, choose the transit VNet to map to the host VNets.
h) In the **VPN** drop-down list, choose a VPN in the overlay network in which to place the mapping.

i) In the IPSec Tunnel CIDR section, to configure IPSec tunnels to reach the Azure virtual network transit, enter two pairs of interface IP addresses and a pair of loopback IP addresses for each of the Cisco CSR1000V or Cisco Catalyst 8000V devices . Ensure that the IP addresses are network addresses in the /30 subnet, unique across the overlay network, and they aren't part of the host VNet CIDR. If they are part of the host VNet CIDR, Microsoft Azure returns an error when attempting to create VPN connections to the transit VNet.

Note The IP addresses aren't part of the host VNet and Transit VPC CIDR.

Microsoft Azure supports single Virtual Private Gateway (VGW) configuration over IPSec tunnels with redundancy provided over a single tunnel. Therefore, Cisco Catalyst SD-WAN Cloud OnRamp for IaaS supports two VGWs for redundancy. During a planned maintenance or an unplanned event of a VGW, the IPSec tunnel from the VGW to the cloud devices get disconnected. This loss of connectivity causes the cloud devices lose BGP peering with Cisco SD-WAN Manager over IPSec tunnel. To enable BGP peering with the cloud routers rather than the IP address of the IPSec tunnel, provide the loopback addresses for each cloud device.

Note The loopback option for BGP peering supports single and multiple Virtual Gateways, or Customer Gateway configuration or both on Azure cloud. The loopback option applies only to the new host VNets mapped to transit VNets and not on the existing VNets.

j) In the Azure Information section:

1. In the **BGP ASN** field, enter the ASN that you configure on the Azure Virtual Network Gateway, which is brought up within the host VNet. Use an ASN that isn't part of an existing configuration on Azure. For acceptable ASN values, refer to Microsoft Azure documentation.
2. In the **Host VNet Gateway Subnet** field, enter a host VNet subnet in which the Virtual Network Gateway can reside. We recommend you use a /28 subnet or higher. Ensure not to provide a subnet that is already created in the VNet.

   Note Ensure that there's an unused CIDR inside the host VNet CIDR.

k) Click **Map VNets**.
l) Click **Save and Complete**.

Note When configuring the VPN feature template for VPN 0 for the two Cisco Catalyst SD-WAN cloud devices that form the transit VNet, ensure that the color you assign to the tunnel interface is a public color, and not a private color. Public colors are:

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

The **Task View** screen appears, confirming that the host VNet has been mapped to the transit VNet successfully.

The creation of VNet Gateway can take up to 45 minutes.

Configure Google Cloud Integration with Cisco vManage

Table 59: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Cloud Gateway with Google Cloud	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure Cisco Catalyst SD-WAN cloud gateways with Google Cloud using the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager.

Feature Name	Release Information	Description
Cisco SD-WAN and Google Service Directory Integration and Support for Cloud State Audit and Cloud Resource Inventory	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Using the Cisco SD-WAN Manager Cloud onRam for Multicloud workflow, you can enable Google Service Directory Lookup, use the Audit option to check whether the state of your objects in Google Cloud are in sync with Cisco SD-WAN Manager state, and view your Google Cloud resource inventory.
Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway	Cisco vManage Release 20.9.1	With this feature, you can deploy between two and eight Cisco Catalyst 8000V instances as part of a cloud gateway in a particular region. In earlier releases, you can deploy exactly two Cisco Catalyst 8000V instances as part of a cloud gateway, with each instance deployed in a different zone of a region.
Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways	Cisco vManage Release 20.9.1	With this feature, you can configure some cloud gateways to support site-to-site and site-to-cloud connectivity, and other cloud gateways to support only site-to-cloud connectivity. This configuration flexibility is particularly beneficial in some Google Cloud regions that do not yet support site-to-site connectivity. In earlier releases, connectivity type is a global configuration. You configure all the cloud gateways to support site-to-site and site-to-cloud connectivity, or to support only site-to-cloud connectivity.

Configure Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud

This section describes how to configure the Cisco Catalyst SD-WAN cloud gateways with Google Cloud feature using Cisco SD-WAN Manager. The section also lists the prerequisites that should be met to be able to configure the feature.

Configuration Prerequisites

- You should have a subscription to Google Cloud. You need your Google Cloud account details to associate your account with Cisco SD-WAN Manager.
- To be able to register you Google Cloud service account in Cisco SD-WAN Manager, ensure that you have at least the following roles configured for your Google Cloud account:
  - Service Account User
  - Compute Instance Admin (v1)
  - Compute Network Admin
  - Compute Public IP Admin
  - Compute Security Admin
  - Hub & Spoke Admin
  - Spoke Admin
- Ensure that following Google Cloud APIs are enabled in the relevant project:
  - Compute API,
  - Billing API,
  - Network Connectivity Center Alpha API
- Ensure that Cisco SD-WAN Manager is connected to the internet and is able to communicate with Google Cloud to authenticate your account.
- Ensure that Cisco SD-WAN Manager has two Cisco Catalyst 8000V instances that are free to use for creating the WAN VPC. For throughput requirements that exceed 250 Mbps, Cisco Catalyst 8000V license is required.
- Ensure that all Cisco SD-WAN Control Components (Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator) run Cisco SD-WAN Release 20.5.1 or later, and that Cisco Catalyst 8000V instances run Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or later.
- Ensure that two Cisco Catalyst 8000V instances are attached to the device template. For more information, see Attach Device to a Device Template.

Note Ensure that you attach the Cisco Catalyst 8000V to the factory default template for Google Cloud (Default_GCP_C8000V_Template_V01).

- Ensure that Cisco Catalyst SD-WAN TCP and UDP ports are open. For more information, see Firewall Ports for Cisco SD-WAN Deployments.

Attach Cisco Catalyst 8000V Instances to a Device Template

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

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

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

   A list of default templates is displayed.

4. Choose the factory default template for Google Cloud (Default_GCP C8000V_Template_V01).

5. Attach two Cisco Catalyst 8000V instances that are free to use, to the device template. For more information, see Attach Device to a Device Template.

Note After you attach the instances, you should not specify **private1** as the color of the transport location (TLOC) because **private1** is used only for site-to-site communication.

Associate Your Google Cloud Account with Cisco SD-WAN Manager

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

Field	Description
Cloud Account Name	Enter a name for your Google Cloud account.
Description (optional)	Enter a description for the account.
Use for Cloud Gateway	Choose **Yes** to create a cloud gateway in your account. The option **No** is chosen by default.
Billing ID	(Optional) Enter the billing ID associated with your Google Cloud service account. If you provide a billing ID, it goes through an automatic validation process. **Note** This field is visible only if you choose the **Yes** option for the **Use for Cloud Gateway** field.
Service Directory Lookup **Note** This field is available in Cisco vManage Release 20.6.1 and later only.	Choose **Enabled** to allow Cisco SD-WAN Manager to discover services or applications in the Google Service Directory associated with the Cloud Account. The option **Disabled** is chosen by default.

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

5. Click **Add**.

Configure Cloud Global Settings

Cloud global settings for a cloud provider apply to cloud gateways for the provider, unless you customize the settings on the **Create Cloud Gateway** page.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. On the **Cloud OnRamp for Multicloud** window, click **Cloud Global Settings** in the Setup area.
2. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
3. To add global settings, click **Add**. If the cloud global settings are already configured, click **Edit** to modify them.
4. In the **Software Image** field, choose the software image of the WAN edge device for the WAN VPC. This should be a preinstalled Cisco Catalyst 8000V instance.
5. In the **Instance Size** field, from the drop-down list, choose an instance based on your requirements.
6. In the **IP Subnet Pool** field, specify the IP subnet pool for the SD-WAN cloud gateway in Google Cloud. This subnet pool needs prefixes between /16 and /21.
7. In the **Cloud Gateway BGP ASN Offset** field, specify the autonomous system number (ASN) for the cloud gateway for BGP peering. This is the starting offset for the allocation of ASNs for the cloud gateways and Google Cloud routers. Starting from the offset, 10 ASN values are reserved for allocating to the cloud gateways.

Attention This offset value cannot be modified after a cloud gateway is created.

8. For **Intra Tag Communication**, choose **Enabled**. This ensures that VPCs with the same tag can communicate with each other.
9. For **Site-to-Site Communication**, choose **Enabled** for site-to-site transit connectivity using Google global network. Otherwise, choose **Disabled**.
10. In the **Site-to-Site Tunnel Encapsulation Type** field, choose the encapsulation from the drop-down list.
11. For **Service Directory Lookup Capable**, choose **Enabled** to allow Cisco SD-WAN Manager to discover Google Service Directory applications associated with this Google account. **Disabled** is chosen by default.

Note This field is available for Cisco vManage Release 20.6.1 and later only.

12. In the **Service Directory Poll Timer Value** field, the value is set to 20 minutes by default.

    This field is available for Cisco vManage Release 20.6.1 and later only.

13. In the **Network Service Tier** field, choose one of the Google Cloud service tiers.
    - PREMIUM: Provides high-performing network experience using Google global network.
    - STANDARD: Allows control over network costs.

14. Click **Save** or **Update**.

Discover Host VPCs and Create Tags

After you associate your Google Cloud account with Cisco SD-WAN Manager, you can discover your host VPCs in the regions associated with your Google Cloud account. This workflow shows your cloud infrastructure at a VPC level. You can create new tags for the discovered VPCs, or modify or delete existing tags. Tags are used to manage connectivity between the VPCs and Cisco Catalyst SD-WAN branch VPNs.

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

   A list of discovered host VPCs displays in a table with the following columns: Cloud Region, Account Name, Host VPC Name, Host VPC Tag, Account ID, and Host VPC ID.
4. Click the **Tag Actions** drop-down list to do any of the following:
   - **Add Tag:** Create a tag for a VPC or a group of VPCs.
   - **Edit Tag:** Change the selected VPCs for an existing tag.
   - **Delete Tag:** Delete the tag for the selected VPC.

Create and Manage Cloud Gateways

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

This procedure describes how to create a Cisco Catalyst SD-WAN cloud gateway with Google Cloud.

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

Note Ensure that the name is in lowercase letters. See the Google Cloud documentation for information about Naming resources and Naming convention.

5. (Optional) Enter a **Description**.
6. In the **Account Name** field, chose your Google Cloud account name from the drop-down list.
7. In the **Region** field, choose a Google region from the drop-down list.
8. (Minimum release: Cisco vManage Release 20.9.1) **Involved in Site-to-site communication**: If the cloud gateway will participate in site-to-site communication, click **Yes**. If the cloud gateway will not participate in site-to-site communication, click **No**.

Note This field is enabled for configuration only when **Site-to-site Communication** is enabled in the global settings. When **Site-to-site Communication** is disabled in the global settings, this field is dimmed.

9. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.
10. (Optional) In the **Settings** section, enter the requested information.

Note You can use either the cloud global settings or customize settings for individual cloud gateways using the fields below.

   a. In the **Software Image** field, choose the software image of the WAN edge device to be instantiated in the WAN VPC to connect your site to Google Cloud.
   b. In the **Instance Size** field, choose an instance size for Cisco Catalyst 8000V, based on your requirements.
   c. In the **IP Subnet Pool** field, specify the IP subnet pool to be used for the Google Cloud WAN VPC. This subnet pool needs prefixes between /16 and /21.

Note The IP subnet pool must not overlap with the IP subnet pool specified in Cloud Global Settings.

   d. In the **Network Service Tier** field, choose one of the Google Cloud network service tiers from the drop-down list.
      - PREMIUM: Provides high-performing network experience using Google Cloud global network.
      - STANDARD: Allows control over network costs.

11. **UUID (specify 2)**:

    Cisco vManage Release 20.8.1 and earlier: Choose two Cisco Catalyst 8000V licenses from the drop-down list.

Cisco vManage Release 20.9.1 and later: Choose a minimum of two and a maximum of eight Cisco Catalyst 8000V licenses from the drop-down list.

Note

- All the Cisco Catalyst 8000v instances in a cloud gateway must be of the same instance type. Vertical scaling is not supported.
- From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

Choose the UUIDs that you attached to the default Google Cloud template.

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

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

13. Click **Add**.

Map VPC Tags and Branch Network VPNs

To enable VPC to VPN mapping, discover a set of VPCs in one or multiple Google regions and create a tag. Then select the service VPNs that you want to map the VPCs to using the same tags.

How Mapping and Connectivity Work

- You don't have to explicitly create connectivity. Based on VPC tags, connectivity is automatically established when cloud gateways are instantiated in a certain region or when tagging operations take place.
- Connectivity intent for inter-tag and intra-tag mapping can be defined independent of the presence of cloud gateways in various cloud regions. The intent is preserved and mapping is realized when a new cloud gateway or mapping change is discovered.
- When cloud gateways are instantiated in different regions, the mapping intents in those regions are automatically realized.
- Inter-tag and intra-tag mapping is based on VPC peering and automatically enables bidirectional connectivity only.
- Only one service VPN can be mapped to one or more tags.
- You can perform only a single cloud operation, such as, tagging, mapping, or, creation or deletion of a cloud gateway, at a time. When one operation is being performed, the others are locked.
- All cloud operations are time bound. For example, mapping operations time out after 60 minutes. On timeout, the operations are declared as failed. Timeout values cannot be configured.
- The Intent Management page doesn't autorefresh when a new mapping intent is being realized.

Prerequisites for Successful Mapping

- VPCs that are involved in mapping (as part of tags) require at least one subnet.

- Mapping relies on VPC peering. Subnets in peering VPCs must be compliant with RFC1918.
- VPCs cannot have overlapping classless interdomain routing (CIDR) addresses. Overlapping CIDR addresses leads to mapping failure.

View or Edit Connectivity

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Intent Management**, click **Cloud Connectivity**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.

   The window displays a connectivity matrix showing source VPNs, and their destinations. The following legend provides information about the status of the intent:

   - Blue: Intent Defined
   - Green: Intent Realized
   - Red: Intent Realized With Errors

   Click any of the cells in the matrix to get a more detailed status information.
4. To define or record a new intent, click **Edit**.
5. Choose the cells that correspond to a VPN and the VPC tags associated with it, and click **Save**.

Monitor Connectivity

When you create a new cloud gateway, you can verify the bring-up and reachability of the Cisco Catalyst 8000V instances provisioned inside the cloud gateway.

Option 1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Cloud**, the **Network Snapshot** displays a summary of the cloud gateways, host VPCs, and WAN edge devices for various cloud providers.

   The upward arrow next to the WAN edge devices indicates the number of devices that are up. Click the arrow to view additional details of the devices.

Option 2

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Workflows** section, click **Cloud Connectivity** under **Intent Management**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
4. Click any cell on the page to view the connectivity status of VPNs and VPC tags.

Service Directory Lookup and Traffic Policies with Discovered Apps

To use services or applications from your Google Cloud account in Cisco SD-WAN Manager traffic policies, you need to first enable Service Directory Lookup in Cisco SD-WAN Manager, and then use the applications discovered from this lookup to create traffic policies.

Enable Service Directory Lookup

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Google Service Directory has been integrated with the Cisco Catalyst SD-WAN solution. With this integration, Cisco SD-WAN Manager can perform a lookup of the Google Service Directories that are part of your Google Cloud Account that is associated with Cisco SD-WAN Manager. Cisco SD-WAN Manager displays the applications or services in your Service Directory as custom applications, which can be used to define routing policies.

For Cisco SD-WAN Manager to be able to search through your Google Service Directory, you need to enable Service Directory Lookup in Cisco SD-WAN Manager.

Naming of Cloud-Discovered Custom Applications

Service Directory Lookup queries Google Cloud for services that you have defined in Google Cloud. Cisco SD-WAN Manager automatically creates custom applications in Cisco Catalyst SD-WAN for the services. To create the name of the custom application, Cisco SD-WAN Manager uses a combination of the following fields, as defined in Google Cloud: Google Cloud account name, Google Cloud region name, service name and namespace. The maximum length for the cloud-discovered custom application name is 59 characters, due to a limitation of the SD-AVC component.

You can view the application list page, showing the custom applications in Cisco SD-WAN Manager. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**, then click **Custom Options** and choose **Lists**. To view the custom applications that Cisco SD-WAN Manager has generated from the services discovered by Cloud OnRamp for Multicloud, click **Cloud Discovered**.

- Cisco SD-WAN Manager 20.6.x handles the 59-character limit as follows: When Cisco SD-WAN Manager uses the four fields described above to create a name for a custom application, if the name exceeds 59 characters, it truncates the name. Truncating the name may lead to name collisions.

  The account name and region name lengths are variable, so it is difficult to predict how many characters remain available for the service name and namespace, while remaining within the 59-character limit.

  To avoid exceeding the character limit, we recommend that when you define services in Google Cloud, use short names for service and name space names. The available length of these names depends on the combined length of the Google Cloud account name and Google Cloud region name.

  - The following example has long account and region names, requiring short service and name space names:

    Account name: gcp-organization-sw-dev
    Region name: australia-southeast1
    Service name: serv1
    Namespace name: nspace1

  - The following example has shorter account and region names, enabling longer service name and name space names:

    Account name: cisco
    Region name: us-west

Service name: service-xyz
Namespace name: dev-team

- Beginning with Cisco SD-WAN Manager 20.7.x, you can use longer, more meaningful names for the namespace and service name fields for a service defined in Google Cloud. If necessary, to meet the 59-character maximum, Cisco SD-WAN Manager may truncate part of the service name.

  Cisco SD-WAN Manager applies a limit of 12 characters for the Google Cloud account name, a limit of 23 characters for the Google Cloud region name, and a limit of 8 characters for the namespace. Three (3) characters are used for a separator (-) in the custom application name. To remain within the 59-character limit without a truncated service name, use a maximum of 13 characters when providing a service name for a service in Google Cloud. If you use a longer name and the combination of these fields exceeds 59 characters, Cisco SD-WAN Manager truncates the name. If truncating the name causes a name collision with a previously defined custom application, Cisco SD-WAN Manager displays an alarm on the application list page. (Instructions for opening the application list page appear above.)

Before You Begin

Ensure that SD-AVC is enabled in Cisco SD-WAN Manager.

- Enable SD-AVC in Cisco SD-WAN Manager:
  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
  2. For the desired Cisco SD-WAN Manager instance, click **...**, choose **Edit**, and check the **Enable SD-AVC** check box.
- Ensure that Service Directory APIs are enabled for your Google Cloud account.

Enable Service Directory Lookup

1. Enable Service Directory Lookup from the **Associate Cloud Account** window in the **Cloud OnRamp for Multicloud** workflow.

   For more information, see the *Associate Your Google Cloud Account with Cisco SD-WAN Manager* topic in this chapter.
2. Under **Cloud Global Settings** enable the Google Account associated with Cisco SD-WAN Manager as **Service Directory Lookup Capable**, and configure the **Service Directory Poll Timer Value**.

   For more information, see Configure Cloud Global Settings.

Create Traffic Policies Using Cloud Discovered Apps

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options**.
3. Under **Centralized Policy**, click **Lists**.

   You are redirected to the **Application** section under **Policies**.
4. Click **Cloud Discovered**.

   A list of applications discovered from Google Service Directory Lookup is displayed.

5. Click **Map Traffic Profiles**. In the dialog box that appears, you can set or modify the traffic profiles for the discovered service.
6. For each of the traffic profiles, click **vManage SLA Classes** and choose an SLA class to map the application to.
7. Click **Save**.
8. Next, create an application list to include the cloud discovered applications. For more information, see Configure Application List.
9. To create a traffic policy using the discovered applications, click **Custom Options** > **Traffic Policy**, and then click **Add Policy**.

   To configure traffic rules on the application list for the cloud discovered applications, see Configure Traffic Rules in Application-Aware Routing.

Audit

Starting from Cisco vManage Release 20.6.1, the **Audit** option in the **Cloud OnRamp for Multicloud** workflow is enabled for Google Cloud. Use this option to verify whether the Google Cloud state is in sync with Cisco SD-WAN Manager state. As part of the audit, if the cloud state is identified as out of sync with Cisco SD-WAN Manager state, Cisco SD-WAN Manager automatically tries to resolve the issues and bring parity in the states.

As part of the audit mechanism, the existence of cloud objects, their interrelationships, and their states are all verified against the connectivity intent defined in Cisco SD-WAN Manager. Cisco SD-WAN Manager then takes corrective action is taken if a mismatch is identified.

Types of Errors Identified by the Audit Option

Recoverable Errors

These are errors that Cisco SD-WAN Manager can take an action on and resolve. Cisco SD-WAN Manager can resolve errors in any objects that are created by Cisco SD-WAN Manager. The Audit option detects and tries to resolve the following errors automatically by recreating the missing resources in the following scenarios:

- Deletion of the hub or the spokes
- Deletion of Google cloud routers—primary, secondary, or both
- Deletion of site-to-cloud peering of VPCs mapped to VPNs in Cisco SD-WAN Manager
- Deletion of VPC peering of VPCs that are mapped to other VPCs in Cisco SD-WAN Manager
- Missing custom routes
- Missing BGP sessions
- Stale BGP sessions

Irrecoverable Errors

These are errors that Cisco SD-WAN Manager cannot resolve, and require manual intervention.

- Removal of a cloud gateway or any of its components
- Issues with host VPCs with overlapping CIDRs

- Issues with site-to-site VPCs
- Issues with site-to-cloud VPCs
- Issues with WAN VPCs

Periodic Audit

Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background and resolves any recoverable issues.

Cisco SD-WAN Manager does not display the results of this audit, but logs events related to the periodic audit.

On-Demand Audit

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** .
2. In the **Intent Management** area, click **Audit**.
3. For the **Cloud Provider** field, choose **Google Cloud**.

   The window displays the status for various Google Cloud objects.
4. If the status shows as Out of Sync for any of the objects, click **Fix Sync issues**. This option resolves any recoverable errors.

Note When the user clicks **Fix Sync Issues**, if an issue can't be fixed, a task update is shown indicating the same. Irrecoverable errors require manual intervention.

View Cloud Resource Inventory

Starting from Cisco vManage Release 20.6.1, you can use the **Cloud Resource Inventory** option in Cisco SD-WAN Manager is enabled for Google Cloud. Use this option to view details of the cloud objects and their identifiers for the Google Cloud account associated with Cisco SD-WAN Manager.

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

   Your existing cloud gateways are displayed.
3. For the desired cloud gateway, click **…** and choose **Cloud Resource Inventory**.

The Cloud Resource Inventory options retrieves the following information for the selected cloud gateway:

- VPCs: WAN, site-to-site, and site-to-cloud VPCs.
- VPC Subnets: WAN, site-to-site, and site-to-cloud in each Google Cloud region associated with the Google Cloud account.
- VMs: A pair of Cisco Catalyst 8000V instances in each Google Cloud region.

- Google Cloud Routers: A pair each of site-to-cloud and site-to-site Google Cloud routers in each region.
- Hubs: An instance each of site-to-site and site-to-cloud Google Global Network hubs.
- Spokes: A pair of spokes from each region that is connected to the site-to-site and site-to-cloud hub.

Configure Cloud onRamp for SaaS

Table 60: Feature History

Feature Name	Release Information	Description
Support for Specifying Office 365 Traffic Categories for Cloud OnRamp for SaaS on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	Using Cloud OnRamp for SaaS, you can select specific SaaS applications and interfaces, and let Cisco Catalyst SD-WAN determine the best performing path for each SaaS applications. For Cisco IOS XE Catalyst SD-WAN devices, you can also limit the use of best path selection to some or all Office 365 traffic, according to the Office 365 traffic categories defined by Microsoft.
Application Feedback Metrics for Office 365 Best Path Selection on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature adds new metrics as inputs to the best-path selection algorithm for Office 365 traffic. The new inputs include best-path metrics from Microsoft Cloud Services. You can enable collection of the metrics, and you can view a log of all of the metrics that factor into the best-path determination for Microsoft Office 365 traffic.
Load Balancing Across Multiple Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature adds the ability to balance traffic for cloud applications across multiple DIA interfaces.

Feature Name	Release Information	Description
Support for Cloud OnRamp for SaaS Probing through VPN 0 Interfaces at Gateway Sites	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Cloud OnRamp for SaaS tests the performance of (probes) routing paths to find the best routing path for specific cloud application traffic. Using the best routing path for the traffic of a cloud application optimizes the performance of the application. This feature enables Cloud OnRamp for SaaS to probe through VPN 0 interfaces at gateway sites as part of determining the best path to use for the traffic of specified cloud applications. This extends the best path probing to include more of the available interfaces connected to the internet. Using this feature, Cloud OnRamp for SaaS can probe interfaces at a gateway site, whether they use service VPNs (VPN 1, VPN 2, and so on) or the transport VPN (VPN 0). This is helpful when a branch site connects to the internet, exclusively or in part, through a gateway site that uses a VPN 0 interface to connect to the internet.
Cloud OnRamp for SaaS Support for Webex	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature adds Webex to the list of cloud applications for which Cloud OnRamp for SaaS can determine the best network path to the cloud server. Cisco SD-WAN Manager periodically downloads a list of Webex servers organized by geographic region. Cloud OnRamp for SaaS uses this server list to help calculate the best network path for Webex traffic in different regions. You can update the Webex server information that Cloud OnRamp for SaaS uses for the Webex application.
Support for Using Microsoft Telemetry Metrics for Microsoft 365 SharePoint and Teams Traffic.	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1	This feature adds support for using Microsoft telemetry metrics for Microsoft 365 SharePoint and Teams. Cloud OnRamp for SaaS uses the metrics data when determining the best path for Office 365 traffic.
View Details of Microsoft Telemetry and View Application Server Information for Office 365 Traffic	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	In Cisco SD-WAN Manager, you can view the cloud application server information that Cisco Catalyst SD-WAN collects over time for Office 365 traffic. This information can be helpful when troubleshooting performance issues with Office 365 traffic.
Configure the Traffic Category and Service Area for Specific Policies	Cisco vManage Release 20.9.1 Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	You can now configure the traffic category and service Area for specific policies using Cisco vManage.

Feature Name	Release Information	Description
Enable Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites	Cisco vManage Release 20.9.1 Cisco IOS XE Release 17.2.1	You can now configure AAR policy to enable Cloud OnRamp operation on specific applications at specific sites using Cisco vManage.
Improved Visibility for Microsoft 365 Traffic	Cisco vManage Release 20.9.1 Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	You can now monitor the details of Microsoft 365 traffic processed by Cloud OnRamp for SaaS with better visibility.
Option to Include or Exclude Microsoft Telemetry Data from Best Path Decision for Microsoft 365 Traffic	Cisco vManage Release 20.9.1	You can now choose whether Cloud OnRamp for SaaS should factor in the Microsoft telemetry data in the best path decision or not.
Improved Visibility and Control of Webex Traffic	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	When enabling the Webex application, you can click the **Enable Application Telemetry** link to enable Cloud OnRamp for SaaS to receive server-side metrics from Webex.

Enable Cloud OnRamp for SaaS

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit**, next to **Cloud OnRamp for SaaS**.
3. In the **Cloud OnRamp for SaaS** field, click **Enabled**.
4. Click **Save**.

Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager

Table 61: Feature History

Feature Name	Release Information	Description
Service Area Mapping	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	To specify the service area that your Microsoft 365 application belongs to, choose an option from the **Service Area** drop-down list.

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

     or

   - In Cisco SD-WAN Manager, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** window displays all SaaS applications.
3. Optionally, you can filter the list of applications by clicking an option in the **App Type** field.
   - **Standard**: Applications included by default for Cloud OnRamp for SaaS.
   - **Custom**: User-defined SaaS application lists (see Information About SaaS Application Lists).
4. Enable applications and configure.

Column	Description
Applications	Applications that can be used with Cloud OnRamp for SaaS. If you enable the **Office 365** application, you can click the **Enable Application Feedback** link to enable Cloud OnRamp for SaaS to receive server-side metrics from Microsoft. For information, see Enable Application Feedback Metrics for Office 365 Traffic. If you enable the **Webex** application, you can click the **Enable Application Telemetry** link to enable Cloud OnRamp for SaaS to receive server-side metrics from Webex. For information, see Enable Webex Server-Side Metrics, on page 269.
Monitoring	**Enabled**: Enables Cloud OnRamp for SaaS to initiate the Quality of Experience probing to find the best path. **Disabled**: Cloud OnRamp for SaaS stops the Quality of Experience probing for this application.
VPN	(Cisco vEdge devices) Specify one or more VPNs.

Column	Description
Policy/Cloud SLA	(Cisco IOS XE Catalyst SD-WAN devices) Select **Enable** to enable Cloud OnRamp for SaaS to use the best path for this application. **Note** You can select **Enable** only if there is a centralized policy that includes an application-aware policy has been activated.
	(Cisco IOS XE Catalyst SD-WAN devices) For Microsoft 365 (M365), select one of the following to specify which types of M365 traffic to include for best path determination: • **Optimize**: Include only M365 traffic categorized by Microsoft as "optimize" – the traffic most sensitive to network performance, latency, and availability. • **Optimize and Allow**: Include only M365 traffic categorized by Microsoft as "Optimize" or "Allow". The "Allow" category of traffic is less sensitive to network performance and latency than the "Optimize" category. • **All**: Include all M365 traffic.
	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can choose the service area that your M365 application belongs to. This allows you to apply the policy to only those applications in the specified service area. Microsoft allows the following service area options: • **Common**: M365 Pro Plus, Office in a browser, Azure AD, and other common network endpoints. • **Exchange**: Exchange Online and Exchange Online Protection. • **SharePoint**: SharePoint Online and OneDrive for Business. • **Skype**: Skype for Business and Microsoft Teams. See the Microsoft documentation for information about updates to the service areas.

5. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** window appears, showing the application-aware policy for the current active centralized policy.

   - You can select the application-aware policy and click **Review and Edit** to view the policy details. The match conditions of the policy show the SaaS applications for which monitoring has been enabled.
   - For an existing policy, you cannot edit the site list or VPN list.
   - You can create a new policy for sites that are not included in existing centralized policies. If you create a new policy, you must add a VPN list for the policy.
   - You can delete one or more new sequences that have been added for the SaaS applications, or change the order of the sequences.

6. Click **Save Policy and Next**. This saves the policy to the Cisco Catalyst SD-WAN Controller.

Configure Client Sites

To configure Cloud OnRamp for SaaS on client sites that access the internet through gateways, configure Cloud OnRamp for SaaS both on the client sites and on the gateway sites.

Note You cannot configure Cloud OnRamp for SaaS with Point-to-Point Protocol (PPP) interface on the gateway sites.

Client sites in the Cloud OnRamp service choose the best gateway site for each application to use for accessing the internet.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**. The **Cloud OnRamp for SaaS** Dashboard appears.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Client Sites**. The page displays the following elements:
   - Attach Sites: Add client sites to Cloud OnRamp for SaaS service.
   - Detach Sites: Remove client sites from Cloud OnRamp for SaaS service.
   - Client sites table: Display client sites configured for Cloud OnRamp for SaaS service.
3. On the **Cloud OnRamp for SaaS** > **Manage Sites** window, click **Attach Sites**. The **Attach Sites** dialog box displays all sites in the overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
4. Choose one or more client sites from **Available Sites** and move them to **Selected Sites**.
5. Click **Attach**. The Cisco SD-WAN Manager saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
6. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS** to return to the Cloud OnRamp for SaaS Dashboard screen.
7. Click **Manage Cloud OnRamp for SaaS** and choose **Gateways**. The page displays the following elements:
   - Attach Gateways: Attach gateway sites.
   - Detach Gateways: Remove gateway sites from the Cloud OnRamp service.
   - Edit Gateways: Edit interfaces on gateway sites.
   - Gateways table: Display gateway sites configured for Cloud OnRamp service.
8. In the **Manage Gateways** window, click **Attach Gateways**. The **Attach Gateways** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
9. In the **Device Class** field, choose one of the following operating systems:

- **Cisco OS**: Cisco IOS XE Catalyst SD-WAN devices
- **Viptela OS (vEdge)**: Cisco vEdge devices

10. Choose one or more gateway sites from **Available Sites** and move them to **Selected Sites**.
11. (Cisco vEdge devices for releases before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a) To specify GRE interfaces for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.

    (Cisco vEdge devices for releases from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a) To specify the VPN 0 interfaces or service VPN interfaces in gateway sites for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.

Note If you do not specify interfaces for Cloud OnRamp for SaaS to use, the system selects a NAT-enabled physical interface from VPN 0.

    a. Click **Add interfaces** to selected sites (optional), located in the bottom-right corner of the **Attach Gateways** window.
    b. Click **Select Interfaces**.
    c. From the available interfaces, choose the GRE interfaces to add (for releases before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a), or the VPN 0 interfaces or service VPN interfaces to add (for releases from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a).
    d. Click **Save Changes**.

12. (Cisco IOS XE Catalyst SD-WAN devices) To configure the routers at a gateway site, perform the following steps.

Note If you don't specify interfaces for Cloud OnRamp for SaaS, an error message indicates that the interfaces aren't VPN 0.

    a. Click **Add interfaces to selected sites**.
    b. The **Attach Gateways** window shows each WAN edge router at the gateway site.

       Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, you can choose Service VPN or VPN 0 if the gateway uses Cisco IOS XE Catalyst SD-WAN devices.

       - If the routers at the gateway site connect to the internet using service VPN connections (VPN 1, VPN 2, …), choose **Service VPN**.
       - If the routers at the gateway site connect to the internet using VPN 0, choose **VPN 0**.

Note

- Correctly choosing **Service VPN** or **VPN 0** requires information about how the gateway site connects to the internet.
- All WAN edge routers at the gateway site must use either service VPN or VPN 0 connections for internet access. Cloud OnRamp for SaaS does not support a mix of both.

c. Do one of the following:

- If you chose **Service VPN**, then for each WAN edge router, choose the interfaces to use for internet connectivity.
- If you chose **VPN 0**, then either choose **All DIA TLOC**, or choose **TLOC list** and specify the colors to include in the TLOC list.

d. To enable load balancing for cloud application traffic across multiple interfaces on the WAN edge device, check the **Enable Load Balancing** check box. (See Load Balancing Across Multiple Interfaces.)

e. Configure the load-balancing options:

Option	Description
Loss (%)	After determining the best path interface for a cloud application, Cloud OnRamp compares the performance statistics for other interfaces. To use another interface for load balancing, the packet loss value of the interface cannot vary from the packet loss value of the best path interface by more than this configured value. You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface. For example, if the best path interface has a packet loss value of 2% and the **Loss** value is 10, then another interface can be used for load balancing only if its packet loss value is no more than 12%. Range: 0 to 100 Default: 10
Latency (milliseconds)	To use another interface for load balancing, the latency value of the interface can't vary from the latency of the best path interface by more than this number of milliseconds. You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface. For example, if the best path interface has a latency of 5 milliseconds, and the **Latency** value is set to 50, then another interface can be used for load balancing only if its latency is no more than 55 milliseconds. Range: 1 to 1000 Default: 50
Source IP based Load Balancing	To ensure that all traffic from a single host uses a single interface, enable this option. For example, to ensure that DNS and application traffic use the same path, enable this option.

f. Click **Save Changes**.

13. Click **Attach**. Cisco SD-WAN Manager saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
14. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

Configure Direct Internet Access (DIA) Sites

Note Cloud OnRamp for SaaS requires an SD-WAN tunnel to each physical interface to enable SaaS probing through the interface. For a physical interface configured for DIA only, without any SD-WAN tunnels going to the SD-WAN fabric, configure a tunnel interface with a default or any dummy color in order to enable use of Cloud OnRamp for SaaS. Without a tunnel interface and color configured, no SaaS probing can occur on a DIA-only physical interface.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. From the **Manage Cloud OnRamp for SaaS** drop-down list, located to the right of the title bar, choose **Direct Internet Access (DIA) Sites**.

   The **Manage DIA**window provides options to attach, detach, or edit DIA sites, and shows a table of sites configured for the Cloud OnRamp service.
3. Click **Attach DIA Sites**. The **Attach DIA Sites** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
4. In the **Device Class** field, select one of the following:
   - **Cisco OS**: Cisco IOS XE Catalyst SD-WAN devices
   - **Viptela OS (vEdge)**: Cisco vEdge devices
5. Choose one or more DIA sites from **Available Sites** and move them to **Selected Sites**.
6. (For Cisco vEdge devices) By default, if you don't specify interfaces for Cloud OnRamp for SaaS to use, the system selects all NAT-enabled physical interfaces from VPN 0. Use the following steps to specify particular interfaces for Cloud OnRamp for SaaS.

Note You can't select a loopback interface.

   a. Click the link, **Add interfaces to selected sites** (optional), located in the bottom-right corner of the window.
   b. In the **Select Interfaces** drop-down list, choose interfaces to add.
   c. Click **Save Changes**.
7. (For Cisco IOS XE Catalyst SD-WAN devices, optional) Specify TLOCs for a site.

Note Configuring Cloud OnRamp for SaaS when using a loopback as a TLOC interface is not supported.

Note If you do not specify TLOCs, the **All DIA TLOC** option is used by default.

a. Click the **Add TLOC to selected sites** link at the bottom-right corner of the **Attach DIA Sites** dialog box.

b. In the **Edit Interfaces of Selected Sites** dialog box, choose **All DIA TLOC**, or **TLOC List** and specify a TLOC list.

c. Click **Save Changes**.

8. Click **Attach**. The Cisco SD-WAN Manager NMS saves the feature template configuration to the devices. The **Task View** window displays a Validation Success message.
9. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

Configure Cloud OnRamp for SaaS Over SIG Tunnels

Table 62: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for SaaS Over SIG Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature lets you to connect to Cloud OnRamp for SaaS by means of a SIG tunnel.

Configure Cloud OnRamp for SaaS over SIG Tunnels Using DIA

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. From **Manage Cloud OnRamp for SaaS**drop-down lsit, choose **Direct Internet Access (DIA) Sites**.
3. Click **Attach DIA Sites**.

   The **Attach DIA Sites** dialog box displays all the sites in your overlay network, with the available sites highlighted.
4. In **Device Class**, select:

   Cisco OS (cEdge)
5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow.
6. Click **Add TLOC to selected sites**.
7. Click **Secure Internet Gateway (SIG) Interfaces**.

8. Click **All Auto SIG Interfaces** or **SIG Interface List** from **Attach DIA Sites** window, and then choose from the list of tunnels that are configured from the Cisco Secure Internet Gateway template.

Note The Tunnel1000X entry in the **SIG Interface List** field refers to the interface name, the equivalent of the IPSec interface name entered when configuring a SIG template.

9. Click **Save Changes**.
10. Click **Attach**.

    Cisco SD-WAN Manager pushes the feature template configuration to the devices, and the **Task View** window displays a **`Validation Success`** message.

Configure Cloud OnRamp for SaaS over SIG Tunnels Using a Gateway

To configure Cloud OnRamp for SaaS over SIG tunnels a Gateway, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. From **Manage Cloud OnRamp for SaaS** drop-down list, choose **Gateways**.
3. Click **Attach Gateways**.

    The **Attach Gateways** pop-up window displays all the sites in your overlay network, with available sites highlighted.
4. In **Device Class**, select:

    Cisco OS (cEdge)
5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow
6. Click **Add interfaces to selected sites**.
7. Click **VPN 0**.
8. Click **Secure Internet Gateway (SIG) Interfaces**.
9. Click **All Auto SIG Interfaces**, or **SIG Interface List** from **Attach Gateways** window, and then choose from the list of tunnels that are configured from the Cisco Secure Internet Gateway template.

Note The Tunnel1000X entry in the **SIG Interface List** field refers to the interface name, the equivalent of the IPSec interface name entered when configuring a SIG template.

10. Click **Save Changes**.
11. Click **Attach**. Cisco SD-WAN Manager pushes the feature template configuration to the devices, and the **Task View** window displays a **`Validation Success`** message.

View Details of Monitored Applications

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

     or

   - In Cisco SD-WAN Manager, click the cloud icon at the top right and click **Cloud OnRamp for SaaS**.

   The page includes a tile for each monitored application, with the following information:

   - How many sites are operating with Cloud OnRamp for SaaS.
   - A color-coded rating of the Quality of Experience (vQoE) score for the application (green=good score, yellow=moderate score, red=poor score) on the devices operating at each site.

2. Optionally, you can click a tile to show details of Cloud OnRamp for SaaS activity for the application, including the following:

Field	Description
vQoE Status	A green checkmark indicates that the vQoE score for the best path meets the criteria of an acceptable connection. The vQoE is calculated based on average loss and average latency. For Office 365 traffic, other connection metrics are also factored in to the vQoE score.

Field	Description
vQoE Score	For each site, this is the vQoE score of the best available path for the cloud application traffic. The vQoE score is determined by the Cloud OnRamp for SaaS probe. Depending on the type of routers at the site, you can view details of the **vQoE Score** as follows: • Cisco IOS XE Catalyst SD-WAN devices: To show a chart of the vQoE score history for each available interface, click the chart icon. In the chart, each interface vQoE score history is presented as a colored line. A solid line indicates that Cloud OnRamp for SaaS has designated the interface as the best path for the cloud application at the given time on the chart. You can place the cursor over a line, at a particular time on the chart, to view details of the vQoE score of an interface at that time. From Cisco vManage Release 20.8.1, for the Office 365 application, the chart includes an option to show the vQoE score history for a specific service area, such as Exchange, Sharepoint, or Skype. For each service area, a solid line in the chart indicates the interface chosen as the best path at a given time. If you have enabled Cloud OnRamp for SaaS to use Microsoft traffic metrics for Office 365 traffic, the choice of best path takes into account the Microsoft traffic metrics. • Cisco vEdge devices: To show a chart of the vQoE score history, click the chart icon. The chart shows the vQoE score for the best path chosen by Cloud OnRamp for SaaS.
DIA Status	The type of connection to the internet, such as local (from the site), or through a gateway site.
Selected Interface	The interface providing the best path for the cloud application. **Note** If the DIA status is Gateway, this field displays **N/A**.
Activated Gateway	For a site that connects to the internet through a gateway site, this indicates the IP address of the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.
Local Color	For a site that connects to the internet through a gateway site, this is the local color identifier of the tunnel used to connect to the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.
Remote Color	For a site that connects to the internet through a gateway site, this is the remote (gateway site) color identifier of the tunnel used to connect to the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.

Field	Description
SDWAN Computed Score	This field is applicable only if the site uses Cisco IOS XE Catalyst SD-WAN devices. It does not apply for Cisco vEdge devices. From Cisco vManage Release 20.8.1, for the Microsoft Office 365 application, an **SDWAN Computed Score** column provides links to view charts of the path scores (OK, NOT-OK, or INIT) provided by Microsoft telemetry for each Microsoft service area, including Exchange, Sharepoint, and Skype. The chart shows the scores over time for each available interface. The scores are defined as follows: • **OK**: Acceptable path • **NOT-OK**: Unacceptable path • **INIT**: Insufficient data These charts provide visibility into how Cloud OnRamp for SaaS chooses a best path for each type of Microsoft Office 365 traffic. A use case for viewing the path score history is for determining whether Microsoft consistently rates a particular interface as NOT-OK for some types of traffic, such as Skype traffic.

Enable Application Feedback Metrics for Office 365 Traffic

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can enable the following types of application feedback from additional sources. Cloud OnRamp for SaaS can use these metrics to help determine the best path for Office 365 traffic.

- Enable telemetry with Microsoft Exchange cloud servers, which can provide best path metrics for Office 365 traffic on specifically configured interfaces. This involves use of a Microsoft service called Microsoft 365 informed network routing. To understand this feature better, see the information available in the Microsoft 365 informed network routing document.
- Enable application response time (ART) metrics, which configures network devices to report ART metrics.

Before You Begin

- Enable monitoring for Office 365 traffic.
- Configure a policy for Office 365, for Cisco IOS XE SD-WAN devices.
- To enable NetFlow metrics, enable Cloud Services.

  (From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Cloud Services**)
- To enable NetFlow metrics for devices in the network, enable the **NetFlow** and **Application** options in the localized policy for each device.

  (From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies** > **Localized Policy** > **Policy template**, **Policy Settings** section)

- Enable Cisco SD-WAN Analytics. See Cisco vAnalytics Insights.

Enable Application Feedback Metrics for Office 365 Traffic

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.
3. In the **Office 365** row, click the **Enable Application Feedback for Path Selection** link.

   The **Application Feedback** dialog box opens.
4. In the **Application Feedback** dialog box, enable traffic metrics:
   - **Telemetry**: Enable Telemetry with Microsoft Exchange cloud servers to receive traffic metrics for Office 365 traffic over specific configured interfaces.

     If the option is disabled and the dialog box shows a message requesting sign-in to a Microsoft account, copy the code provided in the message and click the link to sign in. Provide the code on the Microsoft page that is displayed and log in with your Microsoft tenant account credentials when prompted. After signing in, the **Telemetry** option in the dialog box is enabled.
   - **Traffic Steering**: From Cisco vManage Release 20.9.1, check this check box to allow Cloud OnRamp for SaaS to factor in the Microsoft telemetry data in the best path decision. If you disable this, you can still view the Microsoft telemetry data in the Cisco SD-WAN Analytics dashboard, but the telemetry does not affect the best path decision.
   - (Optional) **Application Response Time (ART)**: Enable ART metrics.

Note Enabling ART automatically configures devices to report ART metrics.

5. Click **Save**.

Configure the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

Before You Begin

To edit the service area and traffic category, you must enable **Monitoring** and **Policy/Cloud SLA** for the Microsoft 365 application with a minimum of one service area. For information, see Configure Applications for Cloud OnRamp for SaaS Using Cisco vManage.

Configure the Traffic Category and Service Area

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

     Or

- In Cisco SD-WAN Manager, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.

2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** page displays all the Cloud OnRamp for SaaS applications.

3. Click the edit icon from the **Policy/Cloud SLA** column for the Microsoft 365 application.

   The **Policy/Cloud SLA Settings** pop-up window opens.

4. Perform one of the following in the **Policy/Cloud SLA Settings** pop-up window.

   - Click **Yes**. Select a minimum of one service area and traffic category.
   - If you have already selected a service area and traffic category, click **No** and edit the Microsoft 365 categories or service area.

5. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** page opens. A list of AAR policies in the current active centralized policy appears.

6. Select the AAR policy that you wish to edit and click **Review and Edit**.

   The **Review Policy** page opens.

7. Select the Microsoft 365 sequence you wish to edit, to change the service area or traffic category, and click the edit icon.

8. Edit the service area and traffic category, and click **Save Match And Actions**.

9. Click **Save Policy and Next**. This saves the policy.

Configure AAR Policy to Enable Cloud OnRamp Operation on Specific Applications at Specific Sites Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

1. Open Cloud OnRamp for SaaS.

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

     Or

   - In Cisco SD-WAN Manager menu, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.

2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** page displays all the Cloud OnRamp for SaaS applications.

3. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** page opens, showing the application-aware policies in the current active centralized policy.

4. Select the policy you wish to edit and click **Review and Edit** to view the policy details.

5. You can now delete one or more sequences that have been added by Cloud OnRamp for SaaS for specific applications or change the order of the sequences.
6. Click **Save Policy and Next**. This pushes the updated policy to the Cisco SD-WAN Controller.

Note Note: When you enable an application on the **Applications and Policy** page, by default, Cloud OnRamp for SaaS is enabled for all AAR policies that are part of the current active centralized policy.

Enable Application Visibility and Flow Visibility

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

Enable Visibility and Flow Visibility Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. Continue clicking **Next** until the **Policy Settings** page appears.
5. Check the **Netflow and Applications** check box.
6. Click **Save Policy**.

   Application visibility and flow visibility are now enabled.

Enable Application Visibility and Flow Visibility Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Enable Webex Server-Side Metrics

Minimum releases: Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Webex integrations enable an application, such as Cisco SD-WAN Manager, to request information from Webex servers, using an application programming interface (API).

1. Using your Webex account, create an integration for Cisco SD-WAN Manager. For information about creating the integration, see Webex for Developers documentation, Integrations & Authorization.

   Creating the Webex integration requires a redirect URI, which includes the IP address of your Cisco SD-WAN Manager server, in the following format:

   https://*vManage-ip-address*:*port*/dataservice/webex/redirect

   At the end of the process of creating the Webex integration, the Webex for Developers site provides you with a client ID and client secret.

Note The details for creating an integration app in the Webex for Developers site are beyond the scope of this document.

2. When you enable Webex in Cloud OnRamp for SaaS, use the client ID and client secret that you received in the previous step to enable Cisco SD-WAN Manager to use the WebEx integration.
   a. Open Cloud OnRamp for SaaS:
      - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

        Or
      - In Cisco SD-WAN Manager, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.

   b. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

      The **Applications and Policy** page displays the Cloud OnRamp applications.

   c. Adjacent to **Webex**, click **Enable vAnalytics Webex Telemetry**.

   d. In the pop-up window, check the **Enable Webex Telemetry** checkbox.

   e. Enter the client ID and client secret for the Webex integration, and click **Save**.

   f. When prompted, enter your **Webex** account credentials.

Note You must use the credentials for the Webex account associated with the Webex integration you used in the previous step. This enables Webex telemetry for that Webex account.

   g. Click **Save Applications and Next** to save the Webex telemetry configuration on Cisco SD-WAN Manager and push the updates to edge devices and to Cisco SD-WAN Analytics.

Configure Visibility for Microsoft 365 SaaS traffic Using Cisco vManage

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

Enable a Device to Provide Data for the Visualization of Microsoft 365 Traffic

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. The **On Demand Troubleshooting** page opens.
2. Click the **Select Device** drop-down list and choose a device.
3. Click the **Select Data Type** drop-down list and choose the data type **DPI**.
4. Select a time range from **Data Backfill Time Period**.
5. Click **Add** to queue the device for processing.
6. Wait until the **Status** column shows **Completed**.

View Office 365 Application Logs

You can view a log of the metrics that factor into the best-path determination for Office 365 traffic. The metrics appear in a Cisco vAnalytics page specifically designed to display this information. The logs provide detailed information regarding status, but are not necessary for using Cloud onRamp for SaaS.

Beginning with Cisco vManage Release 20.8.1, you can view the path score history in a chart form. See View Details of Monitored Applications, on page 264.

Prerequisites

- Enable Microsoft traffic metrics.
- Enable monitoring for Office 365 traffic.

Procedure

1. In Cisco vManage, open **Configuration** > **Cloud onRamp for SaaS**.
2. Click the **Office 365** box.

Note The box appears only if monitoring is enabled for Office 365 traffic.

3. In the **Office 365** window, click the **View Application Logs** link.
4. Log in using Cisco vAnalytics credentials. See Cisco vAnalytics Insights.

   A **Cisco SD-WAN vAnalytics** page opens. This is a Cisco vAnalytics view designed specifically for Cloud onRamp for SaaS, and only provides access to the Cloud onRamp for SaaS metrics for Office 365 traffic. It does not provide other Cisco vAnalytics functionality
5. Select an option from the cloud icon in the left pane to display various logs. Use the filter and interval options above the table to determine what log data to include.

Log Type	Description
Path Scores (**Cloud icon** > **Path Score**)	(This is the default display.) Shows a table with a log of path scores, according to interface. Each line shows the scores and related information for a specific interface at a given time. **Note** The Microsoft Teams service may appear in the table as Skype. The **Score** area includes the following columns: • **MSFT**: Path score determined by Microsoft. • **SDWAN**: Path score determined by all metrics (ART, Cloud OnRamp for SaaS path probing metrics, and Microsoft telemetry metrics). This is the score that primarily determines whether a path is acceptable for traffic. In the **MSFT** and **SDWAN** columns, the table shows the status as one of the following: • **OK**: Acceptable path • **NOT-OK**: Not acceptable path • **INIT**: Insufficient data

View Server Information Using the SD-AVC Cloud Connector

Before You Begin

- Enable SD-AVC (**Administration** > **Cluster Management**, click **…** and choose **Edit**, and choose **Enable SD-AVC**).
- Enable the SD-AVC Cloud Connector. See Enable Cisco SD-AVC Cloud Connector in the *Cisco Catalyst SD-WAN Getting Started Guide*.

View Server Information

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **SD-AVC Cloud Connector**.
2. In the **Application** field, choose an application.
   - For the Office 365 application, the **SD-AVC Cloud Connector** page shows the following information collected from Microsoft Cloud about the Microsoft application servers that handle Office 365 traffic:

Field	Description
Domain tab	
Application Name	Name of the application producing the traffic. Network-Based Application Recognition (NBAR), a component of Cisco IOS XE, provides the application name.

Field	Description
Domain	Destination domain of the traffic. This is the application server handling the cloud application traffic.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates traffic that does not have a defined category.
Service Instance	Service instance information, as defined by Microsoft, for the server. Examples of service instances are China, Germany, USGovGCCHigh, and USGovDoD.
IP Address tab	
IP	Destination IP of the traffic. This is the IP address of the application server handling the cloud application traffic.
Port	Destination port of the traffic.
L4 Protocol	Transport protocol of the traffic, such as TCP or UDP.
Application	Name of the application producing the traffic. NBAR, a component of Cisco IOS XE, provides the application name.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates that traffic does not have a defined category.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.
Service Instance	Service instance information, as defined by Microsoft, for the server. Examples of service instances are China, Germany, USGovGCCHigh, and USGovDoD.

- (Minimum release: Cisco vManage Release 20.10.1) For the Webex application, the **SD-AVC Cloud Connector** page shows the following information collected from Webex cloud servers:

Field	Description
IP Address tab	
Application Name	Name of the application producing the traffic.
Service Area	Type of Webex traffic: meeting, calling, or teams.
IP Address	Destination IP address of the traffic. This is the IP address of the application server handling the cloud application traffic.
Port	Destination port or ports of the traffic.
L4 Protocol	Transport protocol of the traffic, such as TCP or UDP.

Field	Description
Quality of Service	QoS classification for the Webex traffic, as defined by Webex, such as default or optimizemedia.
Primary or Fallback	Category of Webex traffic.
Region	Region of the Webex server data center, such as ap-south-1, ap-northeast-1, and ap-southeast-1.

3. Optionally, you can use the search field to filter the information in the table. For example, you can filter by an application name or by a domain name.

View Application Usage

Minimum releases (for Microsoft 365 traffic): Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Minimum releases (for Webex traffic): Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

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

     Or

   - In Cisco SD-WAN Manager, click the cloud icon near the top right and select **Cloud OnRamp for SaaS**.
2. Click **Manage Cloud OnRamp for SaaS**.
3. Click the **Microsoft 365** application or the **Webex** application. A list of devices that are attached to a DIA or gateway is shown.
4. In the **Application Usage** column of a device, click **View Usage**.

   For the Webex application, the usage information is shown according to Webex region.
5. The **CoR SaaS Application Usage** page displays the information for each type of traffic. To limit the traffic information that is displayed, click the **Search** field, and choose **All CoR SaaS Traffic**, **DIA**, **Gateway**, or **Non CoR SaaS**.

Note The information presented in the above graphs or logs is for an individual device. You can view the information related to only one device at a time. The graphs or logs are only shown for those devices for which on-demand troubleshooting is enabled. For information about on-demand troubleshooting, see On-Demand Troubleshooting.

Verify Changes to the Configuration of the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

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

   A list of devices is displayed.
3. For the device you wish to verify, click **…** and click **Running Configuration**. The **Running Configuration** window opens, displaying the running configuration.
4. Verify that the running configuration reflects any changes that you have made to AAR policies.

Or

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

   The **Policies** page displays the policies.
2. For the policy, you wish to verify, click **…** and click **Preview**.

   The **Policy Configuration Preview** pop-up window appears, providing a preview of the running configuration.
3. Verify that the policy preview reflects any changes that you have made to AAR policies.

Verify Which Applications Are Enabled for Specific Devices Using Cisco vManage

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.2.1

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

   A list of devices is displayed.
3. For the device you wish to verify, click **…** and click **Running Configuration**. The **Running Configuration** window opens, displaying the running configuration.
4. Verify that the running configuration reflects any changes that you have made to AAR policies.

Verify Which Applications Are Enabled for a Specific Policy Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

   The **Policies** window displays the policies.
2. For the policy, you wish to verify, click **…** and click **Preview**.

   The **Policy Configuration Preview** page appears, providing a preview of the running configuration.

3. Verify that the policy reflects any changes that you have made to AAR policies.

Application Lists

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

Table 63: Feature History

Feature Name	Release Information	Description
User-Defined SaaS Application Lists	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	In Cisco SD-WAN Manager, you can define lists of one or more SaaS applications, together with the relevant application server. Cloud OnRamp for SaaS handles these lists in the same way that it handles the predefined set of SaaS applications that it can monitor. When you enable a user-defined list, Cloud OnRamp for SaaS probes for the best path to the application server and routes the application traffic for applications in the list to use the best path.

Create a User-Defined SaaS Application List Using Cisco SD-WAN Manager

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

1. Open the Cloud OnRamp for SaaS page, using one of the following methods:
   - From the Cisco SD-WAN Manager main menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     or

   - From the Cisco SD-WAN Manager menu, click the cloud icon near the top right and select **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **SaaS Application Lists**.
3. Click **New Custom Application List**.
4. Enter a name for the list.
5. To add applications to the list, click the **Search** field and choose applications. The list includes standard applications and any custom applications that you have defined.

   Optionally, you can enter text in the **Search** field to filter for specific applications.

The applications that you choose are added to the **Application** field, which shows each application in the list.

6. Optionally, to create a new custom application within this workflow, click the **Search** field and then click **New Custom Application**. Creating a custom application on this page is equivalent to defining a custom application in the centralized policy workflow, as described in Define Custom Applications. See Define Custom Applications Using Cisco vManage for information about the what information is required for defining a custom application, the use of wildcard characters, the logic applied when matching traffic to the attributes that you enter, and so on.
7. In the **SaaS Probe Endpoint Type** area, define the probe endpoint, which is the server that Cloud OnRamp for SaaS probes to determine a best path for the traffic in the SaaS application list.
   - Choose an endpoint type from the following options:
     - **IP Address**: Enter an IP address. Cloud OnRamp for SaaS probes the server using port 80.
     - **FQDN**: Enter a fully qualified domain name.
     - **URL**: Enter a URL using HTTP or HTTPS. Cloud OnRamp for SaaS probes the server using port 80 or port 443, depending on the URL provided.
   - Enter an endpoint value, based on the endpoint type that you choose.

     Examples: 192.168.0.1, https://www.example.com
8. Click **Add**. The new SaaS application list appears in the table of application lists.

View SaaS Application Lists

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

1. Open the Cloud OnRamp for SaaS page, using one of the following methods:
   - From the Cisco SD-WAN Manager main menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     or
   - From the Cisco SD-WAN Manager menu, click the cloud icon near the top right and select **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **SaaS Application Lists**.

   A table shows the details of each SaaS application list. Optionally, you can click an icon in the **Action** column to edit or delete a list.

Configure Controller Certificate Authorization Settings

Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the Cisco SD-WAN Manager that you generate these certificates and install them on the controller devices—Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers. You can use certificates signed by Symantec, or you can use enterprise root certificates.

The controller certification authorization settings establish how the certification generation for all controller devices will be done. They do not generate the certificates.

You need to select the certificate-generation method only once. The method you select is automatically used each time you add a device to the overlay network.

To have the Symantec signing server automatically generate, sign, and install certificates on each controller device:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Symantec Automated** (Recommended). This is the recommended method for handling controller signed certificates.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to confirm that you wish to have the Symantec signing server automatically generate, sign, and install certificates on each controller device.
4. Enter the first and last name of the requester of the certificate.
5. Enter the email address of the requester of the certificate. This address is required because the signed certificate and a confirmation email are sent to the requester via email; they are also made available though the customer portal.
6. Specify the validity period for the certificate. It can be 1, 2, or 3 years.
7. Enter a challenge phrase. The challenge phrase is your certificate password and is required when you renew or revoke a certificate.
8. Confirm your challenge phrase.
9. In **Certificate Retrieve Interval**, specify how often the Cisco SD-WAN Manager server checks if the Symantec signing server has sent the certificate.
10. Click **Save**.

To manually install certificates that the Symantec signing server has generated and signed:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Symantec Manual**.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to manually install certificates that the Symantec signing server has generated and signed.
4. Click **Save**.

To use enterprise root certificates:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Enterprise Root Certificate**.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to confirm that you wish to use enterprise root certificates.
4. In the **Certificate** box, either paste the certificate, or click **Select a file** and upload a file that contains the enterprise root certificate.

5. By default, the enterprise root certificate has the following properties: To view this information, issue the **show certificate signing-request decoded** command on a controller device, and check the output in the Subject line. For example:

   - Country: United States
   - State: California
   - City: San Jose
   - Organizational unit: ENB
   - Organization: CISCO
   - Domain Name: cisco.com
   - Email: cisco-cloudops-sdwan@cisco.com

```
vSmart# show certificate signing-request decoded
    ...
    Subject: C=US, ST=California, L=San Jose, OU=ENB, O=CISCO, CN=vsmart-uuid
.cisco.com/emailAddress=cisco-cloudops-sdwan@cisco.com
    ...
```

   To change one or more of the default CSR properties:

   a. Click **Set CSR Properties**.
   b. Enter the domain name to include in the CSR. This domain name is appended to the certificate number (CN).
   c. Enter the organizational unit (OU) to include in the CSR.
   d. Enter the organization (O) to include in the CSR.
   e. Enter the city (L), state (ST), and two-letter country code (C) to include in the CSR.
   f. Enter the email address (emailAddress) of the certificate requester.
   g. Specify the validity period for the certificate. It can be 1, 2, or 3 years.

6. Click **Import & Save**.

Configure CUBE

Table 64: Feature History

Feature Name	Release Information	Description
Cisco Unified Border Element Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure Cisco Unified Border Element functionality by using Cisco IOS XE Catalyst SD-WAN device CLI templates or CLI add-on feature templates.

Feature Name	Release Information	Description
Secure SRST Support on Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature enables you to configure Cisco Survivable Remote Site Telephony (SRST) commands on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates. The feature also provides additional Cisco Unified Border Element (CUBE) commands that are qualified for use in Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates.

To configure a device to use the CUBE functionality, create a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template for the device.

For information about device CLI templates, see CLI Templates for Cisco IOS XE Catalyst SD-WAN Device Routers.

For information about CLI add-on feature templates, see CLI Add-On Feature Templates.

For information about CUBE configuration and usage, see *Cisco Unified Border Element Configuration Guide*.

For information about the CUBE commands that Cisco Catalyst SD-WAN supports for use in a CLI template, see CUBE Commands .

The following example shows a basic CUBE configuration using a CLI add-on template:

```
voice service voip
 ip address trusted list
  ipv4 10.0.0.0.255.0.0.0
  ipv6 2001:DB8:0:ABCD::1/48
  !
 allow-connections sip to sip
 sip
  no call service stop
  !
dial-peer voice 100 voip
  description Inbound LAN side dial-peer
  session protocol sipv2
  incoming called number .T
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 101 voip
  description Outbound LAN side dial-peer
  destination pattern [2-9].........
  session protocol sipv2
  session target ipv4:10.10.10.1
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 200 voip
  description Inbound WAN side dial-peer
  session protocol sipv2
```

```
 incoming called-number .T
 voice-class codec 1
 dtmf-relay rtp-nte
 !
dial-peer voice 201 voip
 description Outbound WAN side dial-peer
 destination pattern [2-9].........
 session protocol sipv2
 session target ipv4:20.20.20.1
 voice-class codec 1
 dtmf-relay rtp-nte
```

Configure Custom Applications Using Cisco SD-WAN Manager

Prerequisites

Install Cisco SD-AVC as a component of Cisco Catalyst SD-WAN. For information on how to enable SD-AVC on Cisco SD-WAN Manager, see Information on how to enable SD-AVC for Cisco SD-WAN devices.

Perform the following steps to configure custom applications:

1. In Cisco SD-WAN Manager, select **Configuration** > **Policies**.
2. Select **Centralized Policy**.
3. Click **Custom Options** and select **Centralized Policy** > **Lists**.
4. Click **Custom Applications**, and then click **New Custom Application**.
5. To define the application, provide an application name and enter match criteria. The match criteria can include one or more of the attributes provided: server names, IP addresses, and so on. You do not need to enter match criteria for all fields.

   The match logic follows these rules:

   - Between all L3/L4 attributes, there is a logical AND. Traffic must match all conditions.
   - Between L3/L4 and Server Names, there is a logical OR. Traffic must match either the server name or the L3/L4 attributes.

Field	Description
Application Name	(mandatory) Enter a name for the custom application. Maximum length: 32 characters
Server Names	One or more server names, separated by commas. You can include an asterisk wildcard match character (*) only at the beginning of the server name. Examples: *cisco.com, *.cisco.com (match www.cisco.com, developer.cisco.com, …)
L3/L4 Attributes	

Field	Description
IP Address	Enter one or more IPv4 addresses, separated by commas. Example: 10.0.1.1, 10.0.1.2 **Note** The subnet prefix range is 24 to 32.
Ports	Enter one or more ports or port ranges, separated by commas. Example: 30, 45-47
L4 Protocol	Select one of the following: TCP, UDP, TCP-UDP

6. Click **Add**. The new custom application appears in the table of custom applications.

Note To check the progress of creating the new custom application, click **Tasks** (clipboard icon). A panel opens, showing active and completed processes.

Example Custom Application Criteria

Criteria	How to configure fields
Domain name	**Server Names**: cisco.com
Set of IP addresses, set of ports, and L4 protocol	**IP Address**: 10.0.1.1, 10.0.1.2 **Ports**: 20, 25-37 **L4 Protocol**: TCP-UDP
Set of ports and L4 protocol	**Ports**: 30, 45-47 **L4 Protocol**: TCP

Configure Tunnels

Table 65: Feature History

Feature	Release Information	Description
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. You can also configure weights for multiple GRE/IPSEC tunnels for distribution of traffic among multiple tunnels based on the configured weights.
Support for Zscaler Automatic IPSec Tunnel Provisioning	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature automates the provisioning of tunnels from Cisco Catalyst SD-WAN routers to Zscaler. Using your Zscaler partner API credentials, you can automatically provisions tunnels to Zscaler Internet Access (ZIA) Public Service Edges. You can choose **Zscaler** in the Cisco Security Internet Gateway (SIG) and SIG credentials feature templates to automate tunnel provisioning. You can configure provisioning of tunnels from Cisco Catalyst SD-WAN routers.

Feature	Release Information	Description
SIG Integration Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	**Source-Only Load Sharing**: When you configure two or more active tunnels to a Secure Internet Gateway (SIG), different traffic flows from the same source IP address, with different destination public IP addresses, may be mapped to use different tunnels. With this feature, you can configure all traffic flows from a particular source IP address, irrespective of the destination IP address, to be routed to the SIG through only one of the active tunnels. You can configure source-only load sharing using the **ip cef load-sharing algorithm src-only** in a CLI Add-On template.
Layer 7 Health Check for Manual Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can create and attach trackers to manually created GRE or IPSec tunnels to a SIG endpoint. Trackers help failover traffic when a SIG tunnel is down. You can configure the trackers using the SIG feature template.
Automatic GRE Tunnels to Zscaler	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, use the Secure Internet Gateway (SIG) feature template to provision automatic GRE tunnels to Zscaler SIGs. In earlier releases, the SIG template only supported the provisioning of automatic IPSec tunnels to Zscaler SIGs.
Global SIG Credentials Template	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, create a single global Cisco SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a Cisco SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global Cisco SIG Credentials template to the device template.

Feature	Release Information	Description
Monitor Automatic SIG Tunnel Status and Events	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	Monitor security events related to automatic SIG tunnels using the **Security Events** pane on the **Monitor** > **Security** page, and the **Events** dashboard on the **Monitor** > **Logs** page. Monitor automatic SIG tunnel status using the **SIG Tunnel Status** pane on the **Monitor** > **Security** page, and the **SIG Tunnels** dashboard on the **Monitor** > **Tunnels** page.
Configure SIG Tunnels in a Security Feature Profile	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	You can configure Security feature profile and associate with other configuration groups. You can also configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels.
Cisco Umbrella Multi-Org Support	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature supports management of multiple organizations through a single parent organization. With this feature, Cisco Catalyst SD-WAN Umbrella for SIG support security policy requirements for different regions of the SD-WAN network.

Configure Automatic Tunnels Using Cisco SD-WAN Manager

Prerequisites

To configure automatic tunneling to a SIG, complete the following requisites:

- Cisco Umbrella: To configure automatic tunnels to Cisco Umbrella, you can do one of the following
  - For Cisco SD-WAN Manager to fetch the API keys, specify Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**. Your Cisco Smart Account is the account that you use to log in to the Cisco Smart Software Manager (CSSM) portal.
  - To manually specify the API keys, generate Umbrella Management API keys. See *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

    Specify the generated keys in the Cisco SIG Credentials template.

- Zscaler Internet Access (ZIA): To configure automatic tunnels to Zscaler, do the following:

  1. Create partner API keys on the ZIA Partner Integrations page.

2. Add the Partner Administrator role to the partner API keys.
3. Create a Partner Administrator.
4. Activate the changes.

For more information, see *Managing SD-WAN Partner Keys* on the Zscaler Help Center.

Specify the generated keys in the Cisco SIG Credentials template.

Create Cisco Umbrella SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 289, on selecting Umbrella as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Cisco Umbrella SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 66: Cisco SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Umbrella Global Credentials
Description	(Read only) Global credentials for Umbrella

Configure Cisco Umbrella Credentials

1. In the **Basic Details** section, do one of the following:
   - Enable Cisco SD-WAN Manager to fetch credentials from the Cisco Umbrella portal:
     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

        Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.

     b. Click **Get Keys**.

   - Enter Cisco Umbrella credentials:

Field	Description
SIG Provider	(Read only) Umbrella
Organization ID	Enter the Cisco Umbrella parent organization ID for your organization. For more information, see *Find Your Organization ID* in the Cisco Umbrella SIG User Guide.

Field	Description
Registration Key	Enter the Umbrella Management API Key. It is part of DNS security policy under unified security policy. For more information, see *Management and Provisioning > Getting Started > Overview* in the Cloud Security API documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret.

2. To save the template, click **Save**.

Create Zscaler SIG Credentials Template

Minimum release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 289, on selecting Zscaler as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Zscaler SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 67: Cisco SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Zscaler-Global-Credentials
Description	(Read only) Global credentials for Zscaler

1. In the **Basic Details** section, enter the Zscaler credentials:

Table 68: Zscaler Credentials

Field	Description
SIG Provider	(Read only) Zscaler
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help > Getting Started > Admin Portal > About the Company Profile*.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.

Field	Description
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help* > *Partner Integrations* > *Managing SD-WAN Partner Keys*.

2. To save the template, click **Save**.

Create Cisco SIG Credentials Template

Applicable releases: Cisco vManage Release 20.8.x and earlier releases.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **Other Templates**, click **Cisco SIG Credentials**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. In **Basic Details** section, do the following:
   a. **SIG Provider**: Click **Umbrella** or **Zscaler**.
   b. For Cisco Umbrella, enter the following registration parameters or click **Get Keys** to have Cisco SD-WAN Manager fetch these parameters from the Cisco Umbrella portal.
      - **Organization ID**
      - **Child Org**
      - **Child Org List**
      - **Registration Key**
      - **Secret**

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

To fetch the parameters, Cisco SD-WAN Manager uses your Smart Account credentials to connect to the Cisco Umbrella portal. To manually enter the parameters, generate the values in your Umbrella account as described here.

c. For Zscaler, enter the following details:

Field	Description
Organization	The name of the organization in Zscaler cloud. To find this information in Zscaler, see **Administration** > **Company Profile**.
Child Org	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Enter the child organization information in the SIG template.
Child Org List	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Select the child org from the **Child Org List** drop-down list.
Partner base URI	This is the Zscaler Cloud API that Cisco SD-WAN Manager uses to connect to Zscaler. To find this information in Zscaler, see **Administration** > **API Key Management**.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	The partner API key. To find the key in Zscaler, see **Zscaler Cloud Administration** > **Partner Integrations** > **SD-WAN**.

9. Click **Save**.

Create Automatic Tunnels Using a Cisco SIG Feature Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **VPN**, click **Cisco Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. (From Cisco vManage Release 20.9.1) **SIG Provider**: Click **Umbrella** or **Zscaler**.

From Cisco vManage Release 20.9.1, on selecting **Umbrella** or **Zscaler** as the SIG provider, Cisco SD-WAN Manager prompts you to create the corresponding global SIG credentials template if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Cisco Umbrella or Zscaler SIG credentials template.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

9. To create one or more trackers to monitor tunnel health, do the following in the **Tracker** section:

Note From Cisco IOS XE Release 17.6.2 and Cisco vManage Relase 20.6.2 , you can create customized trackers to monitor the health of automatic tunnels. If you do not customize the SLA parameters, Cisco SD-WAN Manager creates a default tracker for the tunnel.

a. **Source IP Address**: Enter a source IP address for the probe packets.

b. Click **New Tracker**.

c. Configure the following:

Table 69: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds.
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds

Field	Description
Multiplier	Enter the number of times the probes are resent before determining that a tunnel is down. **Note** When tunnel status changes continuously within a short period of time, the tunnel goes to the flapping state. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, to avoid flapping of tunnels, the tracker waits for the duration equal to the product of multiplier * interval to declare the status of the tunnel. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.

d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

10. To create tunnels, do the following in the **Configuration** section:

a. (Cisco 20.8.x and earlier releases) **SIG Provider**: Click **Umbrella** or **Zscaler**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Table 70: Basic Settings

Field	Description
Tunnel Type	Click **ipsec** or **gre**. **Note** Automatic GRE tunnels are supported from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 and only to Zscaler ZIA.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec template.
Description	Enter a description for the interface.

Field	Description
Tracker	By default, a tracker is attached to monitor the health of automatic tunnels to Cisco Umbrella or Zscaler. If you configured a customized tracker in step **8**, choose the tracker. **Note** From Cisco IOS XE Release 17.6.2 and Cisco vManage Relase 20.6.2, you can create customized trackers to monitor the health of automatic tunnels.
Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Source Public IP	Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. **Default**: Auto. We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.

d. (Optional) Under **Advanced Options**, configure the following:

Table 71: General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 72: IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1

Field Name	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 73: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM

Field	Description
Perfect Forward Secrecy	• Specify the PFS settings to use on the IPsec tunnel. • Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: None

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

11. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 74: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.

Field	Description
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

12. (Optional) Modify the default configuration in the **Advanced Settings** section:

Table 75: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 76: Zscaler

Field	Description
Primary Data-Center	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels (Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1): Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.
Secondary Data-Center	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels (Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1): Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.

Field	Description
Zscaler Location Name	Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 (Optional) Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Display Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off

Field	Description
Refresh Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
First Time AUP Block Internet Access	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Force SSL Inspection	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
AUP Frequency	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0

13. Click **Save**.

Create Manual Tunnels Using Cisco SIG Feature Template

From Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, all SIG related workflows for automatic and manual tunnels have been consolidated into the Cisco SIG template. If you are using Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, or later, use the Cisco SIG template to configure GRE or IPSec tunnels to a third-party SIG, or GRE tunnels to a Zscaler SIG.

For a software release earlier than Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, see *Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager*.

Layer 7 Health Check: The option to create trackers and monitor the health of manually created tunnels is available from Cisco IOS XE Release 17.8.1a, Cisco vManage Relase 20.8.1. In earlier releases, the Layer 7 Health Check feature is only available if you use VPN Interface GRE/IPSEC templates, and not with Cisco SIG templates.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **VPN**, click **Cisco Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. (Optional) To create one or more trackers to monitor tunnel health, do the following in the Tracker section:

Note The option to create trackers and monitor tunnel health is available from Cisco IOS XE Release 17.8.1a, Cisco vManage Relase 20.8.1.

   a. **Source IP Address**: Enter a source IP address for the probe packets.
   b. Click **New Tracker**.
   c. Configure the following:

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel. **Note** Both HTTP and HTTPS API URLs are supported.

   d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To create tunnels, do the following in the **Configuration** section:

a. **SIG** Provider: Click **Generic**.

Cisco vManage Release 20.4.x and earlier: Click **Third Party**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Field	Description
Tunnel Type	Based on the type of tunnel you wish to create, click **ipsec** or **gre**.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template or the Cisco VPN Interface GRE feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec or GRE templates.
Description	(Optional) Enter a description for the interface.
Source Type	Click **INTERFACE**. Cisco IOS XE Catalyst SD-WAN devices, **INTERFACE** is the only supported **Source Type**.
Tracker	(Optional) Choose a tracker to monitor tunnel health. **Note** From Cisco IOS XE Release 17.8.1a and Cisco vManage Relase 20.8.1, you can create trackers to monitor tunnel health.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.
Tunnel Destination IP Address/FQDN	Enter the IP address of the SIG provider endpoint.
Preshared Key	This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

d. (Optional) Under **Advanced Options**, configure the following:

Table 77: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None

Table 78: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 0 to 65535 seconds **Default**: 10
DPD Retries	Specify how many unacknowledged packets to send before declaring an IKE peer to be dead and then removing the tunnel to the peer. **Range**: 0 to 255 **Default**:3

Table 79: (Tunnel Type: ipsec) IKE

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. Choose one of the following: • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 16 4096-bit modulus
IKE ID for Local Endpoint	If the remote IKE peer requires a local end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's source IP address
IKE ID for Remote Endpoint	If the remote IKE peer requires a remote end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's destination IP address

Table 80: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: NULL SHA 512
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: Group-16 4096-bit modulus

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

10. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 81: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

11. Click **Save**.

Redirect Traffic to a SIG

You can redirect traffic to a SIG in two ways:

- Using Data Policy. For more information, see Action Parameters in the Policies Configuration Guide.
- Using the Service route to SIG. For more information, see Modify Service VPN Template, on page 305

Modify Service VPN Template

To ensure that the device connects to the SIG, you must modify the Cisco VPN template to include a service route to the SIG.

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

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. For the Cisco VPN template of the device, click **Edit**.
4. Click **IPv4 Route**.
5. Click the delete icon on any existing IPv4 route to the internet.
6. Click **Service Route**.
7. Click **New Service Route**.
8. Enter a Prefix (for example, 10.0.0.0/8).
9. For the service route, ensure that **SIG** is chosen.
10. Click **Add**.
11. Click **Update**.

Create Device Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device** .

3. Click **Create Template** and click **From Feature Template**.
4. From the **Device Model** drop-down list, choose the device model for which you are creating the template.

   Cisco SD-WAN Manager displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is chosen by default.
5. From the **Device Role** drop-down list, choose **SDWAN Edge**.
6. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.
8. Click **Transport & Management VPN**.

9. In the **Transport & Management VPN** section, under **Additional Cisco VPN 0 Templates**, click **Cisco Secure Internet Gateway**.
10. From the **Cisco Secure Internet Gateway** drop-down list, choose the Cisco SIG feature template that you created earlier.
11. Click **Additional Templates**.
12. In the **Additional Templates** section,
    a. Automatic tunneling:

       (Cisco vManage Release 20.8.x and earlier) From the **Cisco SIG Credentials** drop-down list, choose the relevant Cisco SIG Credentials feature template.

       (From Cisco vManage Release 20.9.1) Cisco SD-WAN Manager automatically chooses the applicable global Cisco SIG Credentials feature template based on the Cisco SIG feature template configuration.

Note If there are any changes to the SIG credentials, for these changes to take effect, you must first remove the SIG feature template from the device template and push the device template. Thereafter, re-attach the SIG feature template and then push the template to the device. For information on pushing the device template, see Attach the SIG Template to Devices.

    b. Manual tunneling: No need to attach a **Cisco SIG Credentials** template.
13. Click **Create**.

    The new configuration template is displayed in the **Device Template** table. The **Feature Templates** column shows the number of feature templates that are included in the device template, and the **Type** column shows **Feature** to indicate that the device template was created from a collection of feature templates.

Attach Template to Devices

To attach one or more devices to the device template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and choose the template that you created.

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

3. For the desired template, click **...** and click **Attach Devices**.

   The Attach Devices dialog box displays.
4. In the **Available Devices** column, choose a group and search for one or more devices, choose a device from the list, or click **Select All**.
5. Click the arrow pointing right to move the device to the **Selected Devices** column.
6. Click **Attach**.

7. If the template contains variables, enter the missing variable values for each device in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking **...** in the row and clicking **Edit Device Template**. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
   - Click **Import File** to upload a CSV file that lists all the variables and defines each variable value for each device.
8. Click **Update**.

Monitor SIG Tunnels

Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage 20.9.1

Monitor the status of automatic SIG tunnels using the following Cisco SD-WAN Manager GUI components:

- **SIG Tunnel Status** pane on the **Monitor** > **Security** page
- **SIG Tunnels** dashboard on the **Monitor** > **Tunnels** page

SIG Tunnel Status

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

   The **SIG Tunnel Status** pane shows the following information using a donut chart:
   - total number of SIG tunnels that are configured
   - the number of SIG tunnels that are up
   - the number of SIG tunnels that are down
   - the number of SIG tunnels that are in a degraded state (Degraded state indicates that the SIG tunnel is up but the Layer 7 health of the tunnel as detected by the tracker does not meet the configured SLA parameters. Therefore, the traffic is not routed through the tunnel.)
2. (Optional) Click a section of the donut chart to view detailed information about tunnels having a particular status.

   Cisco SD-WAN Manager displays detailed information about the tunnels in the **SIG Tunnels** dashboard.
3. (Optional) Click **All SIG Tunnels** to view the **SIG Tunnels** dashboard.

SIG Tunnels Dashboard

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**.
2. Click **SIG Tunnels**.

   Cisco SD-WAN Manager displays a table that provides the following details about each automatic tunnel created to a Cisco Umbrella or a Zscaler SIG:
   - Host Name: Host name of the Cisco IOS XE Catalyst SD-WAN device or edge device.

- Site ID: ID of the site where the WAN edge device is deployed
- Tunnel ID: Unique ID for the tunnel defined by the SIG provider
- Transport Type: IPSec or GRE
- Tunnel Name: Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
- HA Pair: Active or Backup
- Provider: Cisco Umbrella or Zscaler
- Destination Data Center: SIG provider data center to which the tunnel is connected

Note Supported for Cisco Umbrella SIG endpoints. Yet to be supported for Zscaler ZIA Public Service Edges.

- Tunnel Status (Local): Tunnel status as perceived by the device
- Tunnel Status (Remote): Tunnel status as perceived by the SIG endpoint

Note Supported for Cisco Umbrella SIG endpoints. Yet to be supported for Zscaler ZIA Public Service Edges.

- Events: Number of events related to the tunnel set up, interface state change, and tracker notifications. Click on the number to display an Events slide-in pane. The slide-in pane lists all the relevant events for the particular tunnel.

Note If you delete an automatic SIG tunnel from a GRE or IPSec interface and later configure an automatic SIG tunnel from the same interface, the newly configured SIG tunnel has the same name as the tunnel that you deleted earlier. As a result, when you configure the new tunnel, you may see SIG-tunnel-related events that were historically reported for the tunnel that was deleted earlier, if these events are not yet purged.

- Tracker: Enabled or disabled during tunnel configuration

3. (Optional) By default, the table displays information for the past 24 hours. To modify the time period, hover the mouse pointer over **24 Hours** and choose a desired time period from the drop-down list.
4. (Optional) To download a CSV file containing the table data, click **Export**.

   The file is downloaded to your browser's default download location.
5. (Optional) Hide or display table columns: Click on the gear icon adjacent to **Export** to display the **Table Settings** slide-in pane. Toggle the columns that you wish to display or hide and click **Apply**.

Monitor SIG Events

Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage 20.9.1

Monitor security events related automatic SIG tunnels using the following Cisco SD-WAN Manager GUI components:

- **Security Events** pane on the **Monitor** > **Security** page
- **Events** dashboard on the **Monitor** > **Logs** page

Security Events

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

   The **Security Events** pane shows how many critical, major, and minor security events Cisco IOS XE Catalyst SD-WAN devices have reported to Cisco SD-WAN Manager during a specified time period. The information is displayed in a bar chart.

   Cisco IOS XE Catalyst SD-WAN devices notify security events to Cisco SD-WAN Manager using NETCONF. The security events include events related to automatic SIG tunnel creation.

2. (Optional) By default, the pane displays security event information for the past 24 hours. To modify the time period, hover the mouse pointer over **24 Hours** and choose a desired time period from the drop-down list.

3. (Optional) **View Details**: Click **View Details** to display the **Monitor** > **Logs** > **Events** page, with information filtered for the **Security** component.

Events Dashboard

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

2. Click **Events**.

   Cisco SD-WAN Manager displays any events that WAN edge devices and controllers have notified in the past three hours.

3. Click **Filter** and configure the following:

Field	Description
Component	Choose the **Security** component.
Severity	Choose one or more of **Critical**, **Major**, and **Minor**. If you do not select specific severities, events of all three severites are displayed.
System IP	To view events notified by specific WAN edge devices, choose the system IP of the devices.

Field	Description
Event name	To view information about one or more specific SIG tunnel events, choose the corresponding event names. **Tip** To view Cisco Umbrella SIG tunnel events, search for events that have `ftm-tunnel` in the event name. To view Zscaler SIG tunnel events, search for events that have `ftm-zia` in the event name.

Click **Apply**.

If the target devices or controllers notified any of the chosen events, Cisco SD-WAN Manager displays information about the same.

4. (Optional) To modify the time range, click **3 hours**, select a time range, and click **Apply.**

   Cisco SD-WAN Manager displays event information for the modified time range.

5. (Optional) Click **Export** to download a CSV file containing the table data.

   The file is downloaded to your browser's default download location.

6. (Optional) Click on the gear icon adjacent to **Export** to display the **Table Settings** slide-in pane. Toggle the columns that you wish to display or hide and click **Apply**.

Configure Source-Only Load Sharing

Minimum supported releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1.

Create CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Under **Select Devices**, choose the devices for which you are creating the template.
5. Under **Select Template**, scroll down to the **OTHER TEMPLATES** section.
6. Click **CLI Add-On Template**.
7. **Template Name**: Enter a name for the feature template.This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
8. **Description**: Enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.
9. Under **CLI CONFIGURATION**, enter the following command: **ip cef load-sharing algorithm src-only**
10. Click **Save**.

Add CLI Add-On Template to Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.
3. Find the device template to which you wish to add the CLI add-on feature template.
4. For the device template, click **...** and click **Edit**.
5. Scroll down to **Additional Templates**.
6. From the **CLI Add-On Template** drop-down list, choose the CLI add-on feature template that you created earlier.
7. Click **Update**.

Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager

Table 82: Feature History

Feature Name	Release Information	Description
Manual Configuration for GRE Tunnels and IPsec Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature lets you manually configure a GRE tunnel by using the Cisco VPN Interface GRE template or an IPSec tunnel by using the Cisco VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.

Note From Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, all SIG related workflows for Automatic and Manual Tunnels have been consolidated into the SIG template. If you are using Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, or later, configure GRE or IPSec tunnels to a generic SIG, or GRE tunnels to a Zscaler SIG, using the SIG template.

Configure SIG Tunnels in a Security Feature Profile

Table 83: Feature History

Feature	Release Information	Description
Configure SIG Tunnels in a Security Feature Profile	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	You can configure Security feature profile and associate with other configuration groups. You can also configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels.

From Cisco vManage Release 20.10.1 and Cisco IOS XE SD-WAN Release 17.10.1, configure SIG tunnels in a configuration group and deploy the configuration to redirect traffic to SIG endpoints.

To configure SIG tunnels and redirect traffic to SIG endpoints, do the following:

1. For automatic tunnels, configure SIG provider credentials.
2. Create a Security feature profile or choose an exiting Security feature profile and associate it with the configuration group.
3. In the Security feature profile, configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels.

   For automatic tunnels, if you've not configured the SIG provider credentials, you are prompted to do so when you configure the Secure Internet Gateway feature.
4. For desired service VPNs, redirect traffic to SIG using data policies or by adding service routes in the service VPN feature configuration.
5. Deploy the configuration group on the desired WAN edge devices to create SIG tunnels from the devices to the configured SIG endpoints and redirect traffic to the SIG.

Configure SIG Credentials

Before you create automatic SIG tunnels, configure Cisco Umbrella or Zscaler credentials to enable Cisco SD-WAN Manager to create the tunnels to Cisco Umbrella or Zscaler endpoints. If you do not configure the SIG credentials on the **Administration** > **Settings** page before you configure the Secure Internet Gateway feature in the Security feature profile, Cisco SD-WAN Manager prompts you to enter the credentials when you configure the the Secure Internet Gateway feature. After you have configured the SIG credentials, you can modify the credentials on the **Administration** > **Settings** page.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. For the **Secure Internet Gateway (SIG) Credentials** setting, click **Edit**.
3. Choose **Umbrella** or **Zscaler**.
4. For **Umbrella**, do one of the following:
   - Enable Cisco SD-WAN Manager to fetch credentials from the Cisco Umbrella portal:
     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

        Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.
     b. Click **Get Keys**.

        Cisco SD-WAN Manager obtains the following details:
        - Organization ID
        - Registration Key
        - Secret
   - Enter Cisco Umbrella credentials:

Table 84: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Registration Key	Enter the Umbrella Management API Key. For more information, see *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret. For more information, see *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

5. For **Zscaler**, configure the following:

Table 85: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help* > *Getting Started* > *Admin Portal* > *About the Company Profile*.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help* > *ZIA API* > *API Developer & Reference Guide* > *Getting Started*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help* > *Partner Integrations* > *Managing SD-WAN Partner Keys*.

6. Click **Save**.

Associate Security Feature Profile with a Configuration Group

Before you begin: Create a configuration group if you haven't already done so. For more information on creating a configuration group, see Run the Create Configuration Group Workflow.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. In the **Feature Profiles - Unconfigured** area, find the **Security Profile** and click **Start Configuration**.
4. In the **Add Profile** slide-in pane, do one of the following:
   - Create a new Security feature profile:
     a. Click **Create new**.
     b. Enter a unique **Name** and an optional **Description** for the profile.
     c. Click **Save**.
   - Choose an existing Security feature profile:
     a. Click **Choose existing**.
     b. Select an existing Security feature profile. Click the radio button adjacent to the profile name.
     c. Click **Save**.

The Security feature profile is listed under **Associated Profiles**.

Configure Secure Internet Gateway Feature

Before you begin: Create or edit a configuration group and associate the Security feature profile with it.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. Under **Associated Profiles**, find the Security feature profile and expand the profile.
4. Click **Add Feature**.
5. In the **Add Feature** slide-in pane, from the drop-down list, choose the **Secure Internet Gateway** feature.
6. Configure the following details:

Table 86: Name, Description, and SIG Provider

Field	Description
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	(Optional) Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.

Field	Description
SIG Provider	Click one of the following: • **Umbrella**: Configure automatic tunnel to Cisco Umbrella SIG. If you've not configured Umbrella credentials, Cisco SD-WAN Manager prompts you to configure the credentials: **Click here to add Umbrella credentials**. Click, and in the **Add Umbrella Credentials** dialog box, enter the details mentioned in Table 87: Cisco Umbrella Credentials, on page 316 and click **Add**. • **Zscaler**: Configure automatic tunnel to Zscaler SIG. If you've not configured Zscaler credentials, Cisco SD-WAN Manager prompts you to configure the credentials: **Click here to add Zscaler credentials**. Click, and in the **Add Zscaler Credentials** dialog box, enter the details mentioned in Table 88: Zscaler Credentials, on page 316 click **Add**. • **Generic**: Configure manual tunnel to a SIG endpoint.

Table 87: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Registration Key	Enter the Umbrella Management API Key. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

Table 88: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help > Getting Started > Admin Portal > About the Company Profile*.

Field	Description
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help > Partner Integrations > Managing SD-WAN Partner Keys*.

7. To create tunnels, click **Configuration** and do the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. Enter the value when you add a device to the configuration group. To change the default key, type a new string and move the cursor out of the **Enter Key** box.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices.

   a. Click **Add Tunnel**.

   b. In the **Add Tunnel** dialog box, under **Basic Settings** configure the following:

   Table 89: Basic Settings

Field	Description
Tunnel Type	Umbrella: (Read only) **ipsec** Zscaler: Click **ipsec** or **gre**. Generic: Click **ipsec** or **gre**.
Interface Name (1..255)	Enter the interface name.
Description	Enter a description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels. Alternatively, you can create a customized tracker as described in step **7** and choose the tracker.
Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.

Field	Description
Source Public IP	(Automatic GRE tunnels to Zscaler only) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. **Default**: Auto. We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Tunnel Destination IP Address/FQDN	(Manual tunnels only) Enter the IP address of the SIG provider endpoint.
Preshared Key	(Manual tunnels only) This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

c. (Optional) Under **Advanced Options**, configure the following:

Table 90: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None

Table 91: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 92: (Tunnel Type: ipsec) IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds

Field Name	Description
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 93: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512

Field	Description
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM
Perfect Forward Secrecy	• Specify the PFS settings to use on the IPsec tunnel. • Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: None

d. Click **Add**.

8. To create one or more trackers to monitor tunnel health, click **Tracker** and do the following:

a. **Source IP Address**: Enter a source IP address for the probe packets.

b. Click **Add Tracker**.

c. In the **Add Tracker** dialog box, configure the following:

Table 94: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.

Field	Description
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds.
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. **Range**: 1 to 10 **Default**: 3

d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

a. Click **Add Interface Pair**.

b. In the **Add Interface Pair** dialog box, configure the following:

Table 95: High Availability Parameters

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.

Field	Description
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

c. Click **Add**.

d. To add more active and back-up tunnel pairs, repeat sub-step **a** to sub-step **c**.

10. (Optional) To configure advanced settings for Cisco Umbrella or Zscaler, click **Advanced Settings** and configure the following:

Table 96: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 97: Zscaler

Field	Description
Primary Datacenter	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.
Secondary Datacenter	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.
Zscaler Location	(Optional) Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.

Field	Description
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Display Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Refresh Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0

11. Click **Save**.

Redirect Traffic to SIG Using Service VPN Feature

Configure a SIG service route for a service VPN to direct the VPN traffic to SIG.

Note Alternatively, you can also redirect traffic to SIG using Data Policy. For more information, see Action Parameters in the *Policies Configuration Guide*.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. Expand the **Service Profile**, and for the service VPN whose traffic you want to redirect traffic to SIG, click **...** and click **Edit Parcel**.
4. Remove any existing static IPv4 routes to the internet:
   a. Click **Route**.
   b. Under **IPv4 Static Route**, find any routes to the internet and click the delete icon to remove it.
5. Add SIG service route:
   a. Click **Service Route**.
   b. Click **Add Service Route**.
   c. In the **Add Service Route** dialog box, configure the following:

   Table 98: Service Route Parameters

Field	Description
Network Address	Enter the public IPv4 address.
Subnet Mask	Enter the subnet for the IPv4 address.
Service	Choose **SIG** from the drop-down list.
VPN	Enter the VPN over which to direct the traffic. Default: VPN 0

   d. Click **Add**.
6. Click **Save**.

Next steps: Add Devices to Configuration Group and Deploy Devices.

Configure Devices

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

You can create and store configurations for all devices—the Cisco SD-WAN Manager systems themselves, Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and routers— by using Cisco SD-WAN Manager. When the devices start up, they contact Cisco SD-WAN Manager, which then downloads the device configuration to the device. (A device that is starting up first contacts the Cisco Catalyst SD-WAN Validator, which validates the device and then sends it the IP address of Cisco SD-WAN Manager.)

The general procedure for creating configuration for all devices is the same. This section provides a high-level description of the configuration procedure. It also describes the prerequisite steps that must be performed before you can create configurations and configure devices in the overlay network.

Feature Templates

Feature templates are the building blocks of complete configuration for a device. For each feature that you can enable on a device, Cisco SD-WAN Manager provides a template form that you fill out. The form allows you to set the values for all configurable parameters for that feature.

Because device configurations vary for different device types and the different types of routers, feature templates are specific to the type of device.

Some features are mandatory for device operation, so creating templates for these features is required. Also for the same feature, you can create multiple templates for the same device type.

Note In releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you enter < or > special characters in a Cisco SD-WAN Manager feature template definition or description, Cisco SD-WAN Manager generates a 500 exception error while attempting to preview a Cisco SD-WAN Manager feature template.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you enter < or > special characters in a Cisco SD-WAN Manager feature template definition or description, the special characters are converted to their HTML equivalents, **<** and **>**. This applies to all feature templates. You no longer receive a 500 exception error when previewing a Cisco SD-WAN Manager feature template.

Device Configuration Workflow

Devices in the overlay network that are managed by Cisco SD-WAN Manager must be configured from Cisco SD-WAN Manager. The basic configuration procedure is straightforward:

1. Create feature templates.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and click **Add Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

2. Create device templates.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and click **Create Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Attach device templates to individual devices.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose a template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

   c. Click **…**, and select **Attach Devices**.

Template Variables

Within a feature template, some configuration commands and command options are identical across all device types. Others—such as a device system IP address, its geographic latitude and longitude, the timezone, and the overlay network site identifier—are variable, changing from device to device. When you attach the device template to a device, you are prompted to enter actual values for these command variables. You can do this either manually, by typing the values for each variable and for each device, or you can upload an Excel file in CSV format that contains the values for each device.

Configuration Prerequisites

Security Prerequisistes

Before you can configure any device in the network, that device must be validated and authenticated so that Cisco SD-WAN Manager systems, Cisco Catalyst SD-WAN Controllers, and Cisco Catalyst SD-WAN Validators recognize it as being allowed in the overlay network.

To validate and authenticate the controllers in the overlay network—Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco Catalyst SD-WAN Validators—a signed certificate must be installed on these devices.

To validate and authenticate the routers, you receive an authorized serial number file from Cisco, which lists the serial and chassis numbers for all the routers allowed in your network. Then, you upload the serial number file to Cisco SD-WAN Manager.

Variables Spreadsheet

The feature templates that you create most likely contain variables. To have Cisco SD-WAN Manager populate the variables with actual values when you attach a device template to a device, create an Excel file that lists the variable values for each device and save the file in CSV format.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be the following, in this order:

- csv-deviceId—Serial number of the device (used to uniquely identify the device). For routers, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.

  csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).

- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network—Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and routers. You do not need to specify values for all variables for all devices.

Create a Device Template from Feature Templates

Device templates define a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular Cisco Catalyst SD-WAN software feature. Some feature templates are mandatory, indicated with an asterisk (*), and some are optional. Each mandatory feature template, and some of the optional ones, have a factory-default template. For software features that have a factory-default template, you can use either the factory-default template (named Factory_Default_*feature-name*_Template) or you can create a custom feature template.

Create a Device Template from Feature Templates

To create a device template:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click the **Create Template** drop-down list, and select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you wish to create the template.

   Cisco SD-WAN Manager displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.

5. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.

7. To view the factory-default configuration for a feature template, select the desired feature template and click **View Template**.

8. Click **Cancel** to return to the **Configuration Template** screen.

9. To create a custom template for a feature, select the desired factory-default feature template and click **Create Template**. The template form is displayed.

   This form contains fields for naming the template and defining the feature parameters.

10. In the **Template Name** field, enter a name for the feature template.

    This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

11. In the **Description** field, enter a description for the feature template.

    This field is mandatory, and it can contain any characters and spaces.

12. For each field, enter the desired value. You may need to click a tab or the plus sign (+) to display additional fields.

13. When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list of the parameter field and select one of the following:

    Table 99:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Use Variable Values in Configuration Templates. To change the default key, type a new string and move the cursor out of the **Enter Key** box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

14. For some groups of parameters, you can mark the entire group as device-specific. To do this, check the **Mark as Optional Row** check box.

    These parameters are then grayed out so that you cannot enter a value for them in the feature template. You enter the value or values when you attach a device to a device template.

15. Click **Save**.

16. Repeat Steps 6 through 13 to create a custom template for each additional software feature. For details on creating specific feature templates, see the templates listed in **Available Feature Templates**.

17. Click **Create**. The new configuration template is displayed in the Device Template table.

    The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Another way to create device templates from feature templates is to first create one or more custom feature templates and then create device templates. You can create multiple feature templates for the same feature. For a list of feature templates, see **Available Feature Templates**.

1. Click **Feature**.

2. Click **Add Template**.

3. From **Select Devices**, select the type of device for which you wish to create a template.

    You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.

4. Select the feature template. The template form is displayed.

    This form contains fields for naming the template and fields for defining the required parameters. If the feature has optional parameters, then the template form shows a plus sign (+) after the required parameters.

5. In the **Template Name** field, enter a name for the feature template.

    This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the **Description** field, enter a description for the feature template.

    This field is mandatory, and it can contain any characters and spaces.

7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down list of each parameter's value box.

8. Click the plus sign (+) from the required parameters to set the values of optional parameters.

9. Click **Save**.

10. Repeat Steps 2 to 9 for each additional feature template you wish to create.
11. Click **Device**.
12. Click the **Create Template** drop-down list and select **From Feature Template**.
13. From the **Device Model** drop-down list, select the type of device for which you wish to create the device template.

    Cisco SD-WAN Manager displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (*). The remaining templates are optional.
14. In the **Template Name** field, enter a name for the device template.

    This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
15. In the **Description** field, enter a description for the device template.

    This field is mandatory, and it can contain any characters and spaces.
16. To view the factory-default configuration for a feature template, select the desired feature template and click **View Template**.
17. Click **Cancel** to return to the **Configuration Template** screen.
18. To use the factory-default configuration, click **Create** to create the device template. The new device template is displayed in the **Device Template** table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.
19. To modify the factory-default configuration, select the feature template for which you do not wish to use the factory-default template. From the drop-down list of available feature templates, select a feature template that you created.
20. Repeat Step 19 for each factory-default feature template you wish to modify.
21. Click **Create**. The new configuration template is displayed in the **Device Template** table.

    The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Create a Device CLI Template

To create a device template by entering a CLI text-style configuration directly on the Cisco SD-WAN Manager:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click the **Create Template** drop-down list and select **CLI Template**.
4. From the **Device** Type drop-down list, select the type of device for which you wish to create the template.

5. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

6. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.

7. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

8. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.

9. Click **Add**. The new device template is displayed in the Device Template table.

   The **Feature Templates** column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Configure DHCPv6

Table 100: Feature History

Feature Name	Release Information	Description
DHCP for IPv6	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to configure DHCP for IPv6 (DHCPv6) on Cisco IOS XE Catalyst SD-WAN devices to assign IPv6 addresses to hosts on an IPv6-enabled network. A Cisco IOS XE Catalyst SD-WAN device can be configured for DHCPv6 as a DHCP server, DHCP client, or as a DHCP relay agent.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

3. From **Create Template** drop-down, choose **CLI Template**.

Note You can also use the CLI Add-on template to configure DHCP for IPv6 for client and server. For more information, see Create a CLI Add-On Feature Template.

4. From **Device Model**, choose a device model for which you are creating the template.
5. In the **Template Name** field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any character and spaces.
7. In the **CLI Configuration** field, enter the DHCP configuration for IPv6 for client and server by typing it, cutting and pasting it, or uploading a file.
8. Click **Save**.

Configure Disaster Recovery

Table 101: Feature History

Release Name	Release Information	Feature Description
Disaster Recovery for Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b Cisco vManage Release 19.2.1	This feature helps you configure Cisco SD-WAN Manager in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances.
Disaster Recovery for a 6 Node Cisco SD-WAN Manager Cluster.	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature provides support for disaster recovery for a 6 node Cisco SD-WAN Manager cluster.
Disaster Recovery for a Single Node Cisco vManage Cluster	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides support for disaster recovery for a Cisco SD-WAN Manager deployment with a single primary node.
Disaster Recovery User Password Change	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can change the disaster recovery user password for disaster recovery components from the Cisco SD-WAN Manager **Disaster Recovery** window.

Out of the three controllers that make up the Cisco Catalyst SD-WAN solution (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator), Cisco SD-WAN Manager is the only one that is stateful and cannot be deployed in an active/active mode. The goal of the disaster recovery solution is to deploy Cisco SD-WAN ManagerCisco SD-WAN Manager across two data centers in primary/secondary mode.

The disaster recovery option provides automatic failover of the primary cluster to the secondary cluster. Data is replicated from the primary cluster to the secondary cluster.

There are two disaster recovery options. The option that you use depends on the function that you want the arbitrator to perform. An arbitrator is a Cisco SD-WAN Manager cluster that is hosted in a third data center and that monitors the connectivity and reachability of the Cisco SD-WAN Manager clusters that are hosted in data center 1 and data center 2. The arbitrator can detect a failure of the primary Cisco SD-WAN Manager cluster and issue a switchover command to the secondary Cisco SD-WAN Manager cluster so that the secondary cluster assumes the role of the primary cluster.

The disaster recovery options are:

- Manual—If you want to make the clusters active, you can do it manually rather than having the arbitrator do the switchover. You can specify the switchover threshold.
- Automated —Arbitrator does the monitoring of the cluster and performs the necessary action.

  A highly available Cisco Catalyst SD-WAN network contains three or more Cisco SD-WAN Manager systems in each domain. This scenario is referred to as a Cisco SD-WAN Manager cluster, andCisco SD-WAN Manager system in a cluster is referred to as a Cisco SD-WAN Manager instance.

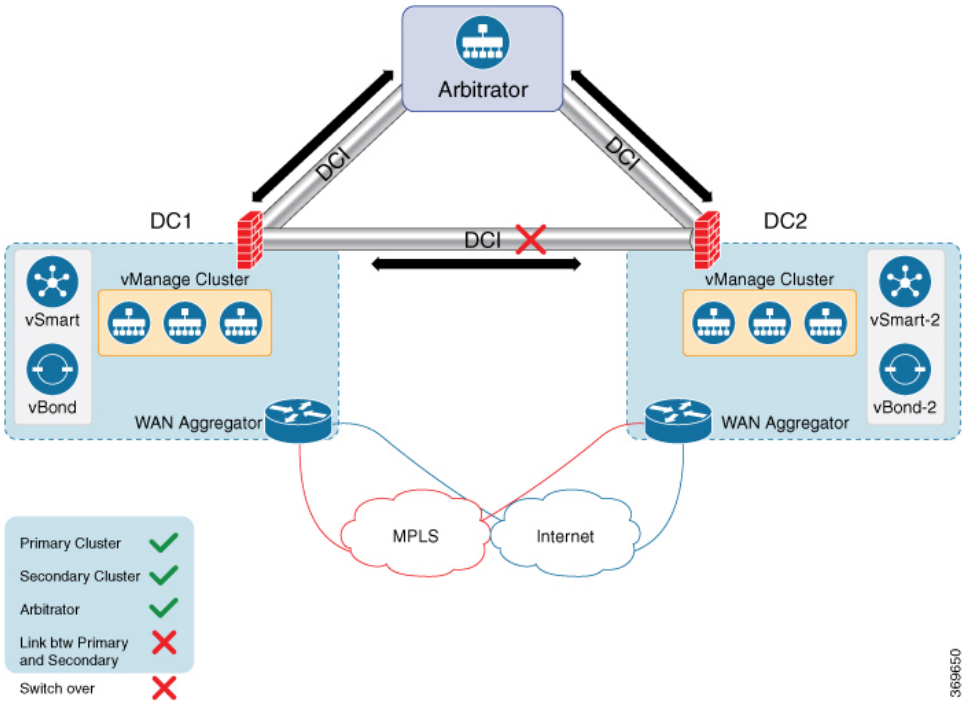
Disaster recovery is validated as follows:

- For releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco SD-WAN Release 20.4.1, disaster recovery is validated for a three-node cluster.
- In Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco SD-WAN Release 20.4.1, disaster recovery is validated for a six-node cluster.
- In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco SD-WAN Release 20.5.1, disaster recovery is validated for a deployment with a single primary node.

Architecture Overview

The following diagram describes the high-level architecture of the disaster recovery solution.

The arbitrator is an additional Cisco SD-WAN Manager cluster that runs in arbitrator mode. The arbitrator monitors the health of the primary and the secondary clusters and performs the necessary actions.



Prerequisites

Before configuring disaster recovery, ensure that you have met the following requirements:

- For manual disaster recover configuration, ensure that you have two Cisco SD-WAN Manager clusters that contain the specific number of nodes as validated for your release. (The validated number of nodes for each release is described earlier in this section.)
- To configure the automated recovery option, ensure that you include an additional Cisco SD-WAN Manager node.
- Ensure that the primary and the secondary cluster are reachable by HTTPS on a transport VPN (VPN 0).
- Ensure that Cisco Catalyst SD-WAN Controllers and Cisco Catalyst SD-WAN Validators on the secondary cluster are connected to the primary cluster.
- Ensure that the nodes in the Cisco SD-WAN Manager primary cluster, the secondary cluster, and the arbitrator node are using the same Cisco SD-WAN Manager version.

Best Practices and Recommendations

- Ensure that you use a netadmin user privilege for Disaster Recovery registration. We recommend that you modify the factory-default password, admin before you start the registration process.
- To change user credentials, we recommend that you use the Cisco SD-WAN Manager GUI, and not use the CLI of a Cisco Catalyst SD-WAN device.
- If Cisco SD-WAN Manager is configured using feature templates, ensure that you create separate feature templates for both the primary cluster and the secondary cluster. Create these templates in the primary

cluster. After templates replicate to the secondary cluster, you can attach devices to templates in the secondary cluster.

- For an on-premises deployment, ensure that you regularly take backup of the Configuration database from the active Cisco SD-WAN Manager instance.

Changing the Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Validator Administrator Password

For releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you use Cisco SD-WAN Manager to change a user password that you entered during disaster recovery registration, first deregister disaster recovery from the Cisco SD-WAN Manager cluster, change the password, and then reregister disaster recovery on the cluster.

Changing the Disaster Recovery User Password for Disaster Recovery Components

During disaster recovery registration, you provide the user name and password of a Cisco SD-WAN Manager or a Cisco Catalyst SD-WAN Validator user for the following disaster recovery components. You can provide the name and password of the same user for each of these components, or you can provide the names and passwords of different users for various components. The user names and passwords that you provide for a component identify the *disaster recovery user* who can access disaster recovery operations on the component.

- Cisco SD-WAN Manager servers in the active (primary) cluster. This component uses the password of a Cisco SD-WAN Manager user.
- Cisco SD-WAN Manager servers in the standby (secondary) cluster. This component uses the password of a Cisco SD-WAN Manager user.
- Arbitrator (applies only to automated disaster recovery). This component uses the password of a Cisco SD-WAN Manager user.
- Each Cisco Catalyst SD-WAN Validator. This component uses the password of a Cisco Catalyst SD-WAN Validator user.

If you change the Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Validator password of a disaster recovery user, you must change the disaster recovery component password for this user to the new password.

To change a password for the disaster recovery user, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Disaster Recovery**.
2. Click **Pause Disaster Recovery**, and then click **OK** in the **Pause Disaster Recovery** dialog box that is displayed.

   Data replication between the primary and secondary data centers stops and this option changes to **Resume Disaster Recovery**.
3. Click **Manage Password**.
4. In the **Manage Password** window, perform these actions:
   a. Click **Active Cluster**, and in the **Password** field that appears, enter the new active cluster password for the disaster recovery user.
   b. Click **Standby Cluster**, and in the **Password** field that appears, enter the new standby cluster password for the disaster recovery user.

c. (For automatic disaster recovery only.) Click **Arbitrator**, and in the **Password** field that appears, enter the new active arbitrator password for the disaster recovery user.

d. Click **vBond**, and in each **Password** field that appears, enter the new Cisco Catalyst SD-WAN Validator password for the disaster recovery user. There is one **Password** field for each Cisco Catalyst SD-WAN Validator.

e. Click **Update**.

The passwords are updated and the **Manage Password** window closes.

5. Click **Resume Disaster Recovery**, and then click **OK** in the **Resume Disaster Recovery** dialog box that is displayed.

Data replication between the primary and secondary data centers restarts.

Enable Disaster Recovery on Day-0:

You need to bring up two separate clusters with no devices being shared, which means do not share any Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, or Cisco SD-WAN Manager device.

On both clusters, configure the following:

Item	Action
Secondary cluster	Bring up the secondary Cisco SD-WAN Manager cluster with three Cisco SD-WAN Manager clusters.
Arbitrator	To assign an IP address for the OOB network, navigate to **Administration > Cluster Management**.
	Ensure reachability between the primary, secondary clusters, and arbitrator on VPN (0) using HTTPS.
	Ensure reachability between the primary cluster, secondary cluster, and Cisco Catalyst SD-WAN Validators.

Verify after Registering for Disaster Recovery on Day-1

- Replication from the primary cluster to the secondary cluster happens at the configured intervals.
- Status check: **Administration > Disaster Recovery**.
- Arbitrator:
  - First health check after 15 minutes. This check provides enough time for all the nodes to be up and running with the configured disaster recovery processes.
  - Health check of the primary cluster, secondary cluster, and the arbitrator every five minutes.
  - Check the */var/log/nms/vmanage-server.log* for the status information on the arbitrator cluster.

Configure Disaster Recovery

1. From the Cisco vManage menu, choose **Administration > Disaster Recovery**.
2. Click **Manage Disaster Recovery**.
3. To configure primary and secondary cluster, on the Cisco SD-WAN Manager Disaster Recovery screen, select an IP address for any Cisco SD-WAN Manager node within the respective cluster.

   If a cluster is behind a load balancer, specify the IP address of the load balancer.
4. Specify the following: **Start Time**, **Replication Interval**, and **Delay Threshold** for replicating data from the primary to the secondary cluster.

   The default value for **Delay Threshold** is 30 minutes.

   The default value for **Replication Interval** is 15 minutes.
5. From the Cisco vManage menu, choose **Administration > Disaster Recovery**, and for Cluster 2 (Secondary), click **Make Primary**.

   It can take 10 to 15 minutes to push all changes from all the devices.
6. You can also decide to pause disaster recovery, pause replication, or delete your disaster recovery configuration.

   After disaster recovery is configured and you have replicated data, you can view the following:

   - when your data was last replicated, how long it took to replicate, and the size of the data that was replicated.
   - when the primary cluster was switched over to the secondary cluster and the reason for the switchover.
   - the replication schedule and the delay threshold.

Disaster Recovery Striking the Primary Data Center

- Switchover happens only when all the nodes in the primary data center are lost.
- The arbitrator detects the loss of all the primary data center members and initiates switchover to the secondary data center.
- Secondary data center updates the Cisco Catalyst SD-WAN Validator:
  - Invalidates old Cisco SD-WAN Manager systems.
  - New Cisco SD-WAN Manager systems from the secondary data center are updated, as valid.
  - Routers reach the Cisco Catalyst SD-WAN Validator after losing control connections.
  - Routers start forming control connections with the new valid Cisco SD-WAN Manager systems.

Troubleshooting Tips

If disaster recovery registration fails, verify the following:

- Reachability to the Cisco Catalyst SD-WAN Validator from all cluster members on the secondary cluster.

- Reachability between the secondary cluster, primary cluster, and the arbitrator on the transport interface (VPN 0).
- Check that you have the correct username and password.

If disaster recovery registration fails due to arbitrator reachability, check the following:

- You must configure the arbitrator in cluster mode. From the Cisco vManage menu, choose **Administration** > **Cluster Management**, and add a Cisco SD-WAN Manager system as the arbitrator.
- If the IP address is not assigned to the correct arbitrator, log on to the arbitrator cluster and do the following:
  - From the Cisco vManage menu, choose **Administration** > **Cluster Management**.
  - Edit the Cisco SD-WAN Manager system.
  - Choose the correct IP address from the drop-down list and save the configuration.

  The disaster recovery consul process uses this IP address for disaster recovery communication. This is set once you configure the Cisco SD-WAN Manager system in cluster mode.

Configure DRE

Table 102: Feature History

Feature Name	Release Information	Description
Traffic Optimization with DRE	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure DRE using the AppQoE feature template in Cisco vManage. Ensure that you select devices supported for DRE.
DRE Profiles	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Apply DRE profiles using the AppQoE feature template in Cisco vManage.
UCS-E Series Server Support for Deploying Cisco Catalyst 8000V	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature introduces support for deploying Cisco Catalyst 8000V instances, on supported routers, using UCS-E series blade server modules. With this feature, the supported routers can be configured as integrated service nodes, external service nodes, or hybrid clusters with both internal and external service nodes.
UCS-E Series Next Generation Support for Deploying Cisco Catalyst 8000V	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature introduces support for deploying Cisco Catalyst 8000V Edge Software on supported routers, using the UCS-E1100D-M6 server module.

Upload DRE Container Image to the Software Repository

Prerequisite

Download the DRE container image from Cisco software downloads page. To download the DRE container image navigate to Catalyst 8000V Edge Software page and select IOS XE SD-WAN Software. You can use the same container image across the Cisco 8000 platform.

Upload the Container Image to Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. Under **Upload Virtual Image**, choose **vManage**.
4. Browse to the downloaded container image on your local machine, and then click **Upload**.

   When the upload is complete, the image appears in the **Virtual Images** window.

Upgrade DRE Container Virtual Image

To upgrade the container image, see Upgrade Software Image on a Device.

Enable DRE Optimization

Configure AppQoE Template for DRE

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose a device that is supported for DRE.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose on of the following device roles:
   - **Controller:** Choose **Controller** if you want to configure the device as a controller with an integrated service node. For devices that support an integrated service node, the **Enable** checkbox is available. This option is grayed out for devices that don't support the integrated service node functionality.
   - **Service Node:** Choose the **Service Node** option if you want to configure the device as an external service node. The **External Service Node** check box is enabled by default.

     The **Service Node** option is not visible if the device that you chose cannot be configured as an external service node.

7. Under **Advanced**, enable **DRE Optimization**.

8.

Note The Resource Profile field is applicable for DRE profiles. The DRE profiles feature was introduced in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. Therefore, this option is not available in previous releases.

(Optional) In the **Resource Profile** field, choose **Global** from the drop-down list. Next, choose a profile size from the options available.

If you don't configure the **Resource Profile**, the default DRE profile size for the device is applied. For more information on the default profiles, see Supported DRE Profiles.

9. (Optional) To optimize HTTPS, FTPS, or any other encrypted traffic, enable **SSL Decryption**.

Note If you enable **SSL Decryption**, you must configure an SSL/TLS decryption security policy so that the TLS service can decrypt the traffic before it is sent to the DRE container, and then encrypted again after the traffic is optimized.

10. Click **Save**.

Create a Centralized Policy for TCP and DRE Optimization

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Under **Centralized Policy**, click **Add Policy**.

Note For more information, see Configure Centralized Policies Using Cisco vManage.

3. In the policy configuration wizard, click **Next** until you are on the **Configure Traffic Rules** window.
4. Click **Traffic Data**, and then click **Add Policy**.
5. Enter a name and description for your policy.
6. Click **Sequence Type** and from the **Add Data Policy** dialog box, choose **Custom**.
7. Click **Add Sequence Rule**.
8. Under the **Match** option, you can choose any match conditions that are applicable to a data policy, such as, Source Data Prefix, Application/Application Family List, and so on.
9. Under the **Actions** option, choose **Accept**. Choose **TCP Optimization** and **DRE Optimization** from the options.

Note Not all actions are available for all match conditions. The actions available to you depend on the match conditions you choose. For more information, see Configure Traffic Rules.

10. Click **Save Match And Actions**.
11. Click **Save Data Policy**.
12. Apply the centralized data policy to the edge devices at the sites between which DRE optimization should be triggered for traffic flows.
13. Activate the centralized policy.

Update Device Template

For the DRE configuration to take effect, attach the AppQoE policy with DRE enabled, to the device template of the device for which you created the AppQoE policy with DRE.

1. To create a new device template or update an existing one, see Create a Device Template from Feature Templates
2. In the **Additional Templates** area, for **AppQoE**, choose the template you created in the Configure AppQoE Template for DRE section.

Note To deactivate the DRE service, detach the AppQoE template from the device template.

Create a Centralized Policy for TCP and DRE Optimization

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Under **Centralized Policy**, click **Add Policy**.

Note For more information, see Configure Centralized Policies Using Cisco vManage.

3. In the policy configuration wizard, click **Next** until you are on the **Configure Traffic Rules** window.
4. Click **Traffic Data**, and then click **Add Policy**.
5. Enter a name and description for your policy.
6. Click **Sequence Type** and from the **Add Data Policy** dialog box, choose **Custom**.
7. Click **Add Sequence Rule**.
8. Under the **Match** option, you can choose any match conditions that are applicable to a data policy, such as, Source Data Prefix, Application/Application Family List, and so on.
9. Under the **Actions** option, choose **Accept**. Choose **TCP Optimization** and **DRE Optimization** from the options.

Note Not all actions are available for all match conditions. The actions available to you depend on the match conditions you choose. For more information, see Configure Traffic Rules.

10. Click **Save Match And Actions**.
11. Click **Save Data Policy**.
12. Apply the centralized data policy to the edge devices at the sites between which DRE optimization should be triggered for traffic flows.
13. Activate the centralized policy.

Configure Cisco Catalyst 8000V on UCS-E Series Server Modules for DRE Optimization

Table 103: Feature History

Feature Name	Release Information	Description
UCS-E Series Server Support for Deploying Cisco Catalyst 8000V	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature lets you deploy Cisco Catalyst 8000V instances, on supported routers, using the UCS-E series blade server modules. With this feature, the supported routers can be configured as integrated service nodes, external service nodes, or hybrid clusters with both internal and external service nodes.

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cisco Catalyst 8000V instances can be installed as external service nodes on supported UCS E-Series servers that reside in specific router models. This functionality enables the routers to act as hybrid clusters with integrated as well as external service nodes.

Configuration Workflow

1. Configure the UCS E-Series server on the supported router.
2. Deploy Cisco Catalyst 8000V on the supported UCS E-Series server.
3. In Cisco SD-WAN Manager, configure AppQoE feature template for Cisco Catalyst 8000V instances on UCS E-Series servers.
4. In Cisco SD-WAN Manager, configure the AppQoE feature template for the service controllers, and add additional configuration using Cisco SD-WAN Manager CLI template and CLI Add-on feature template.

Configure UCS E-Series Server

Before You Begin

Insert the UCS E-Series server module into the supported device and connect two interfaces (TE2 and TE3) from the front panel. For more information, see UCS-E Series Servers Hardware Installation Guide.

Configure UCS E-Series Server on the Supported Router

The following is sample configuration to enable UCS E-Series server on a supported router:

```
Device(config)# ucse subslot 1/0
Device(config-ucse)# imc access-port shared-lom <ge1/te2/te3>
Device(config-ucse)# imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x
Device(config-ucse)# exit
Device(config)# interface ucse1/0/0
Device(config-if)# ip address x.x.x.1 255.255.255.0
```

Deploy Cisco Catalyst 8000V on UCS E-Series Server

Before You Begin

- Install the hypervisor on the UCS-E server module.
- Download the Cisco Catalyst 8000V 17.6.1 OVA file from the Cisco software download page for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and install it..

Configure IP Addresses for Cisco Catalyst 8000V

The following is a sample for configuring IP addresses for Cisco Catalyst 8000V on the UCS E-Series server:

```
Device(config)# interface GigabitEthernet1
Device(config-if)# description Mgmt
Device(config-if)# ip addeess x.x.x.x x.x.x.x
Device(config)# int GigabitEthernet2
Device(config-if)# description WAN-CONTROLLER
Device(config-if)# ip address x.x.x.x x.x.x.x
Device(config-if)# exit
Device(config)# int GigabitEthernet3
Device(config-if)# description UCSE-INTF
Device(config-if)# ip addeess x.x.x.x x.x.x.x
```

Configure AppQoE Feature Template for Cisco Catalyst 8000V Instances

Before You Begin

Cisco Catalyst 8000V instances on UCS E-Series servers should be configured with the app-heavy resource allocation profile. This profile allows the Cisco Catalyst 8000V instances to participate in DRE optimization.

The following example shows how to configure a device as app-heavy using the Cisco SD-WAN Manager CLI Add-on feature template:

```
Device(config)# platform resource app-heavy
```

Enable DRE Optimization for Cisco Catalyst 8000V Instances

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose **C8000v**.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose the **Service Node** option.
7. Under the **Advanced** section, enable **DRE Optimization**.
8. Click **Save**.

Configure the Controller Cluster Types

Add UCS E-Series Server Configuration in Cisco SD-WAN Manager

In Cisco SD-WAN Manager, create a CLI Add-on feature template and update it with UCS E-Series server configuration.

The following is sample configuration for UCS E-Series servers that can be added to the CLI Add-on feature template:

```
ucse subslot 1/0
imc access-port shared-lom te2
imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x

interface ucse1/0/0
vrf forwarding 5
```

Option 1: Configure Service Controller as the Cluster Type

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. In the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Leave the **Integrated Service Node** check box unchecked.

7. In the **Controller IP address** field, enter the IP address of the controller.

   Alternatively, choose **Default** from the drop-down list. The AppQoE controller address is chosen by default.

8. In the **Service VPN** field, enter the service VPN number.

   Alternatively, choose **Default** from the drop-down list. The AppQoE service VPN is chosen by default.

9. In the **Service Nodes** area, click **Add Service Nodes** to add service nodes to the AppQoE service node group.

10. Click **Save**.

11. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

    - CLI Add-on feature template with the UCS E-Series server configuration
    - AppQoE feature template

    For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as the integrated service node separately. For more information, see Enable DRE Optimization.

Option 2: Configure Hybrid as the Cluster Type

Routers that have Cisco Catalyst 8000V instances deployed on their UCS E-Series servers can be configured with cluster types as service-controllers or hybrid.

1. From theCisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.

4. Under **Other Templates**, click **AppQoE**.

5. Enter **Template Name** and **Description**.

6. For the **Integrated Service Node** field, check the **Enable** check box.

7. Click **Save**.

8. Create a CLI template to add the cluster-type hybrid configuration.

   The following is a sample configuration to configure the cluster type as hybrid on the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

```
interface VirtualPortGroup2
 vrf forwarding 5
 ip address 192.168.2.1 255.255.255.0

interface ucse1/0/0
 vrf forwarding 5
 ip address 10.40.17.1 255.255.255.0
```

```
service-insertion service-node-group appqoe SNG-APPQOE
 service-node 192.168.2.2
service-insertion service-node-group appqoe SNG-APPQOE1
 service-node 10.40.17.5
!
service-insertion appnav-controller-group appqoe ACG-APPQOE
 appnav-controller 10.40.17.1 vrf 5

service-insertion service-context appqoe/1
 cluster-type hybrid
 appnav-controller-group ACG-APPQOE
 service-node-group SNG-APPQOE
 service-node-group SNG-APPQOE1
 vrf global
 enable
```

9. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:
   - AppQoE feature template
   - CLI Add-on feature template with the UCS E-Series server configuration
   - CLI template with the hybrid cluster configuration

   For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as integrated service node separately. For more information, see Enable DRE Optimization.

Configure ePBR

Table 104: Feature History

Feature Name	Release Information	Description
Enhanced Policy Based Routing for Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This release extends Enhanced Policy Based Routing (ePBR) to Cisco Catalyst SD-WAN. You can create ePBR policies using CLI add-on templates in Cisco SD-WAN Manager.

To configure ePBR using Cisco SD-WAN Manager, create a CLI add-on feature template and attach it to the device template.

This section provides examples of ePBR configurations that you can add to the CLI add-on template.

Configure ePBR for IPv4

In the following example:

- The extended ACLs define the network or the host.
- Class maps match the parameters in the ACLs.
- Policy maps with ePBR then take detailed actions based on the set statements configured.
- Multiple next-hops are configured. ePBR chooses the first available next-hop.

```
ip access-list extended test300
 100 permit ip any 192.0.2.1 0.0.0.255
ip access-list extended test100
 100 permit ip any 192.0.2.20 0.0.0.255
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test1
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop 10.0.0.2 10.0.40.1 10.0.50.1 ...
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop 10.10.0.2 10.20.20.2 10.30.30.2 ...
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

Configure IPv4 Tracking

This example shows how to configure ePBR along with tracking. In the example:

- IP SLA operations of type ICMP Echo are configured and ACLs are defined.
- Class maps are then used to match parameters in the ACLs and the policy map takes action based on the set statements configured.
- The number 10 in `set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2` represents the sequence number.

```
ip sla 1
  icmp-echo 10.0.0.2
  vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
  icmp-echo 10.10.0.2
  vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip access-list extended test300
 100 permit ip any 10.10.0.2 0.0.0.255
ip access-list extended test100
 100 permit ip any 10.10.0.3 0.0.0.255
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop verify-availability 10.0.0.2 10 track 1
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
```

```
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

Configure ePBR for IPv6

In the following example:

- The extended ACLs define the network or the host.
- Class maps are used to match the parameters in the ACLs.
- Policy maps with ePBR then take detailed actions based on the set statements configured. .
- Single or multiple next-hop addresses can be configured. ePBR selects the first available next-hop address

```
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB81::/32
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001:DB82::/32
!
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop 2001:DB8::1
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop 2001:DB8::2 2001:DB8:FFFF:2 ...
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

Configure IPv6 Tracking

This example shows how to configure ePBR for IPv6 along with tracking enabled. In this example:

- IP SLA operations of type ICMP Echo are configured and ACLs are defined.
- Class maps are then used to match parameters in the ACLs and the policy map takes action based on the set statements configured.
- Tracking is configured such that if the result of the IP SLA is unavailable, the packets aren't sent to the next-hop configured on the class.

```
ip sla 3
  icmp-echo 2001:DB8::1
  vrf 100
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip sla 4
  icmp-echo 2001:DB8::2
  vrf 300
ip sla schedule 4 life forever start-time now
track 4 ip sla 4 state
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB8::/32
ipv6 access-list test100_v6
```

```
 sequence 100 permit ipv6 any  2001:DB8::1/32
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop verify-availability 2001:DB8::2 10 track 4
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop verify-availability 2001:DB8::1 10 track 3
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

Configure ePBR for IPv4 with Multiple Next Hops and SLA Tracking

In the following example:

- IP SLA operations of type ICMP Echo are configured and ACLs are defined.
- Class maps are then used to match parameters in the ACLs and the policy map takes action based on the set statements configured.
- Tracking is configured for next hops such that if the previous IP address isn't reachable, and the IP SLA confirms the next hop as reachable, packets flow to the next hop address.

```
ip sla 1
  icmp-echo 10.0.0.2
  vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
  icmp-echo 10.10.0.2
  vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip sla 3
  icmp-echo 10.20.0.2
  vrf 400
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip access-list extended test300
 100 permit ip any 192.0.2.1  255.255.255.0
ip access-list extended test100
 100 permit ip any 192.0.2.10 255.255.255.0
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
  set ipv4 vrf 400 next-hop verify-availability 10.20.0.2 11 track 3
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop verify-availability 10.0.0.2 10 track 1
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
```

```
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
!
```

Note When next hops are configured along with the tracker, if the next hop is unreachable or if the IP SLA fails, the next available hop is selected. This means that when the tracker is configured, both next hop availability and IP SLA results are checked.

Configure Ethernet CFM using Cisco SD-WAN Manager CLI Template

Table 105: Feature History

Feature Name	Release Information	Description
Ethernet Connectivity Fault Management Support on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can now configure Ethernet Connectivity Fault Management functionality on Cisco IOS XE Catalyst SD-WAN devices using the Add-On feature template in Cisco SD-WAN Manager.

The following commands are used to configure Ethernet CFM.

1. To enable CFM IEEE version of CFM:

   Device(config)# **ethernet cfm ieee**

2. To enable CFM processing globally on the device:

   Device(config)# **ethernet cfm global**

3. To enable caching of CFM data learned through traceroute messages:

   Device(config)# **ethernet cfm traceroute cache**

4. To enable ethernet CFM syslog messages:

   Device(config)# **ethernet cfm logging**

5. To enable SNMP trap generation for ethernet CFM continuity check events:

   Device(config)# **snmp-server enable traps ethernet cfm cc**

6. To enable SNMP trap generation for ethernet CFM continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs:

   csnmp-server enable traps ethernet cfm crosscheck

7. To define an EVC and enter EVC configuration mode:

   Device(config)# **ethernet evc *evc-id***

8. To define a CFM maintenance domain at a particular maintenance level and enter ethernet CFM configuration mode:

   Device(config)# **ethernet cfm domain *domain-name* level *level-id***

9. To include the sender ID TLVs and the attributes containing type, length, and values for neighbor devices:

   Device(config)# **sender-id chassis**

10. To configure a maintenance association within a maintenance domain and enter ethernet CFM service configuration mode:

    Device(config-ecfm)# **service *short-ma-name* evc *evc-name* vlan *vlanid* direction down**

11. To configure offload sampling:

    Device(config)# **offload sampling *sample***

12. To enable the transmission of CCMs:

    Device(config-ecfm-srv)# **continuity-check**

13. To configure the time period between CCMs transmission (the default interval is 10 seconds):

    Device(config-ecfm-srv)# **continuity-check [interval *cc-interval*]**

14. To configure the MEP domain and ID on the interface:

    Device(config)# **interface *interface-name***

    Device(config-if)# **cfm mep domain *domain-name* mpid *id* service *service-name***

For a detailed explanation on the purpose of each command, see Configuring Ethernet CFM.

Example Configurations

The following configuration example shows you how to configure CFM per subinterface for EVC+VLAN maintenance association:

```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet evc USER-SERVICE
 !
 ethernet cfm domain USER level 7
  service USER-SERVICE evc USER-SERVICE vlan 112 direction down
   continuity-check
   continuity-check interval 10s
   continuity-check loss-threshold 3
 !
 ethernet cfm logging
 !
 interface GigabitEthernet0/0/1
  no ip address
  speed 100
  no negotiation auto
  ethernet cfm mep domain USER mpid 1562 service USER-SERVICE
   cos 2
 !
 interface GigabitEthernet0/0/1.112
```

```
  description NAME 2286884663
   encapsulation dot1Q 112
   ip address 192.0.2.1 255.255.255.0
```

The following configuration example shows you how to configure CFM per physical interface for port maintenance association:

```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet cfm traceroute cache
 ethernet cfm domain USER level 1
  sender-id chassis
  service USER-SERVICE port
   continuity-check
   continuity-check interval 1m
   sender-id chassis
 !
 ethernet cfm logging
 !
 interface Ethernet0/1/0
  no ip address
  load-interval 30
  speed [10/100/1000]
  duplex [half/full]
  ethernet oam mode passive
  ethernet oam remote-loopback supported
  ethernet oam
  ethernet cfm mep domain USER mpid 101 service USER-SERVICE
   alarm notification all
 !
 interface Ethernet0/1/0.101
  encapsulation dot1Q 101
  pppoe enable group global
  pppoe-client dial-pool-number 1
  no cdp enable
  ethernet loopback permit external
```

You can use this configuration in the CLI template on Cisco SD-WAN Manager as well as the CLI Add-On template.

For information on CLI Add-On Templates on Cisco SD-WAN Manager, see Create a CLI Add-On Feature Template

Configure Cisco Catalyst SD-WAN EtherChannel

Table 106: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN EtherChannel	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature lets you to configure EtherChannels on Cisco IOS XE SD-WAN devices on the service-side VPN.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

3. From **Create Template** drop-down, choose **CLI Template**.

Note You can also use the CLI Add-on template to configure an EtherChannel. For more information, see Create a CLI Add-On Feature Template.

4. From **Device Model**, choose a device model for which you are creating the template.
5. In the **Template Name** field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any character and spaces.
7. In the **CLI Configuration** field, enter the EtherChannel configuration by typing it, cutting and pasting it, or uploading a file.
8. Click **Save**.

Configure Firewall High-Speed Logging

Table 107: Feature History

Feature Name	Release Information	Feature Description
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.

Table 108: Feature History

Feature Name	Release Information	Feature Description
Firewall High-Speed Logging	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows a firewall to log records with minimum impact to packet processing.

Feature Name	Release Information	Feature Description
Security Logging Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature allows you to configure up to four destination servers to export the syslogs, and an option to specify a source interface for high-speed logging (HSL). The IP addresses for the destination servers can be IPv4, IPv6, or both.

To configure Firewall High-Speed Logging using Cisco SD-WAN Manager, follow the standard firewall Cisco SD-WAN Manager flow to create a firewall policy. For more information, see For more information on creating a firewall policy, see Configure Firewall Policy and Unified Security Policy.

You can configure HSL in the Policy Summary page. For more information about the policy summary page, see Create Unified Security Policy Summary.

Configure Geofencing Using a Cisco System Template

Table 109: Feature History

Feature Name	Release Information	Description
Added Support for Configuring Geofencing Using a **Cisco System** Feature Template	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure the geographical boundary of a device using a **Cisco System** feature template.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device.
5. In the **Select Template** > **Basic Information** section, click **Cisco System**.
6. In the **Template Name** field, enter a name for the template.

   The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the **Template Description** field, enter a description of the template.

   The description can be up to 2048 characters and can contain only alphanumeric characters.
8. In the **Basic Configuration** section of the **Cisco System** template, choose a value from the drop-down list for **Console Baud Rate (bps)**.

Console Baud Rate (bps) is a mandatory field for configuring geofencing.

9. Click **GPS** or navigate to the **GPS** section of the **Cisco System** template.
10. In the **Latitude** field, leave the field set to **Default** for automatic detection of a device.

    The following are the allowed values: -90.0 - 90.0.
11. In the **Longitude** field, leave the field set to **Default** for automatic detection of a device.

    The following are the allowed values: -180.0 - 180.0.

Caution If you manually specify **Latitude** and **Longitude** coordinates, you disable automatic detection of a device.

Automatic detection of a device can fail if a device does not have a last-known valid location.

12. In the **Geo Fencing Enable** field, change the scope from **Default** to **Global**, and click **Yes** to enable geofencing.

    The **Geo Fencing Enable** field is not enabled by default.
13. (Optional) In the **Geo Fencing Range in meters** field, specify a geofencing range unit in meters.

    The geofencing range specifies the radius from the base target location in meters.

    The default geofencing range is 100 meters. You can configure a geofencing range of 100 to 10,000 meters.
14. (Optional) In the **Enable SMS** drop-down list, change the scope to **Global**, and click **Yes** to enable SMS alerts.

    An SMS alert is delivered when a device is determined to be outside the configured geofencing radius of its target location.

Note The presence of a SIM card is mandatory in the Long-Term Evolution PIM for receiving SMS alerts.

15. (Optional) In the **Mobile Number 1** field, add a mobile number for receiving SMS alerts.

Note Mobile numbers must start with a + sign, include a country code, an area code, with no spaces between the country code and the area code, and the remaining digits.

    The following is a sample mobile number: +12344567236.

    You can configure additional mobile phone numbers by clicking the **+** icon.

    You can configure up to a maximum of four mobile numbers.
16. Click **Save**.

Configure Geolocation-Based Firewall Rules

Table 110: Feature History

Feature Name	Release Information	Description
Geolocation-Based Firewall Rules for Allowing or Denying Network Traffic Based on Geolocation	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure firewall rules for allowing or denying network traffic based on the source and destination location instead of IP addresses.

To configure firewall rules, specify the source and destination locations in the security firewall policies in Cisco SD-WAN Manager.

There are two ways to configure geofiltering using Cisco SD-WAN Manager:

- Configure a geolocation list using **Configuration** > **Security** > **Custom Options**.
- Create or add a geolocation list or a geolocation to an existing firewall security policy.

  Prerequisite: You must have an existing security policy for the second bullet item.

Note If you add a geolocation list, you cannot add a geolocation.

Conversely, if you add a geolocation, you cannot add a geolocation list.

Note You cannot configure both a fully qualified domain name (FQDN) and a geo as a source data prefix and as a destination data prefix.

Configure a Geolocation List Using Configuration > Security > Custom Options

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. From the **Custom Options** drop-down menu, choose **Lists**.
3. Click **Geo Location** in the left pane.
4. Click **New Geo Location List**.
5. Enter a name for the geolocation list.
6. Choose one or more geolocations from the drop-down menu.

Note If you choose a continent, you cannot choose any of the countries that are part of the continent. If you want to choose a list of countries, choose the appropriate countries from the list.

7. Click **Add**.

Create a Geolocation List or Add a Geolocation to an Existing Security Firewall Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Choose an existing security policy.
3. For the chosen policy, click **...**, and click **Edit**.

   The **Edit Security Policy** window displays.
4. Click **Firewall**.
5. For the desired policy you want to modify, click **...** and click **Edit**.

   The **Edit Firewall Policy** window displays.
6. Click **Add Rule/Rule Set Rule**.
7. From the drop-down menu, choose **Add Rule**.

   The **New Firewall** window displays.
8. Click **Source Data Prefix** to add a source geolocation list or new geolocations.
9. From the **Geo Location List** drop-down menu, choose a previously configured geolocation list.
10. Alternatively, to create a new geolocation list, choose **New Geo Location**.

    The **Geo Location List** dialog box displays.
    a. In the **Geo Location List Name** field, specify a name for the geolocation list.
    b. From the **Select Geo Location** drop-down menu, choose one or more locations.
    c. Click **Save**.
11. From the **Geo Location** drop-down menu, choose one or more locations.
12. Click **Save**.
13. Click **Destination Data Prefix** to add a destination geolocation list or new geolocations.
14. Repeat Step 9 through Step 12.
15. Click **Save Firewall Policy** to save the security firewall rule.
16. Click **Save Policy Changes**.

Configure GPS Using Cisco SD-WAN Manager

Use the GPS template for all Cisco cellular routers running Cisco Catalyst SD-WAN software.

For Cisco devices running Cisco Catalyst SD-WAN software, you can configure the GPS and National Marine Electronics Association (NMEA) streaming. You enable both these features to allow 4G LTE routers to obtain GPS coordinates.

Note You can configure GPS using Cisco SD-WAN Manager starting from the Cisco vManage Release 20.6.1 and onwards.

Device configuration using the CLI or a CLI template is available starting from the Cisco IOS XE Catalyst SD-WAN Release 17.6.1a only and onwards.

You can configure GPS using a Cisco SD-WAN Manager feature template. For geofencing to work, you need to configure GPS. To configure a GPS feature template, navigate to **Configuration** > **Templates** > **Feature Templates** > **GPS**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

For more information on geofencing, see Configure Geofencing.

Navigate to the Template Screen and Name the Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **Create Template**.
4. From the **Create Template** drop-down list, choose **From Feature Template**.
5. From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.
6. Click **Cellular**.
7. In **Additional Cellular Controller Templates**, click **GPS**.
8. To create a custom template for GPS, click the **GPS** drop-down list and then click **Create Template**. The GPS template form is displayed. This form contains fields for naming the template, and fields for defining the GPS parameters.
9. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
10. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to **Default** (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list to the left of the parameter field and select either **Device Specific** or **Global**.

Configure GPS

To configure GPS parameters for the cellular router, configure the following parameters. Parameters marked with an asterisk are required to configure the GPS feature.

Table 111:

Parameter Name	Description
GPS	Click **On** to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: • **MS-based**—Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, a network data session is used to obtain the GPS satellite locations, resulting in a faster fix of location coordinates. • **Standalone**—Use satellite information when determining position. **Note** Standalone mode is currently not supported for geofencing.
NMEA	Click **On** to enable the use of NMEA streams to help in determining position. NMEA streams data from the router's 4G LTE Pluggable Interface Module (PIM) to any device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address	(Optional) Enter the IP address of the interface that connects to the router's PIM. **Note** This option is not used for configuring geofencing.
Destination Address	(Optional) Enter the IP address of the NMEA server. The NMEA server can be local or remote. **Note** This option is not used for configuring geofencing.
Destination Port	(Optional) Enter the number of the port to use to send NMEA data to the server. **Note** This option is not used for configuring geofencing.

To save the feature template, click **Save**.

Configure Groups of Interest for Centralized Policy

In **Create Groups of Interest**, create new groups of list types as described in the following sections to use in a centralized policy:

Configure Application

1. In the groups of interest list, click **Application** list type.
2. Click **New Application List**.
3. Enter a name for the list.
4. Choose either **Application** or **Application Family**.

Application can be the names of one or more applications, such as **Third Party Control**, **ABC News**, **Mircosoft Teams**, and so on. The Cisco IOS XE Catalyst SD-WAN devices support about 2300 different applications. To list the supported applications, use the **?** in the CLI.

Application Family can be one or more of the following: **antivirus**, **application-service**, **audio_video**, **authentication**, **behavioral**, **compression**, **database**, **encrypted**, **erp**, **file-server**, **file-transfer**, **forum**, **game**, **instant-messaging**, **mail**, **microsoft-office**, **middleware**, **network-management**, **network-service**, **peer-to-peer**, **printer**, **routing**, **security-service**, **standard**, **telephony**, **terminal**, **thin-client**, **tunneling**, **wap**, **web**, and **webmail**.

5. In the **Select** drop-down, in the 'Search' filter, select the required applications or application families.
6. Click **Add**.

A few application lists are preconfigured. You cannot edit or delete these lists.

Microsoft_Apps—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column.

Google_Apps—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.

Configure Color

1. In the groups of interest list, click **Color**.
2. Click **New Color List**.
3. Enter a name for the list.
4. In the **Select Color** drop-down, in the 'Search' filter select the required colors.

   Colors can be: 3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver.
5. Click **Add**.

To configure multiple colors in a single list, you can select multiple colors from the drop-down.

Configure Community

Table 112: Feature History

Feature Name	Release Information	Description
Ability to Match and Set Communities	Cisco SD-WAN Release 20.5.1 Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can create groups of communities to use in a match clause of a route map in Cisco vManage.

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. In the group of interest list, click **Community**.
2. Click **New Community List**.
3. Enter a name for the community list.
4. Choose either **Standard** or **Expanded**.
   - Standard community lists are used to specify communities and community numbers.
   - Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to specify patterns to match community attributes.
5. In the **Add Community** field, enter one or more data prefixes separated by commas in any of the following formats:
   - *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.
   - **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices.
   - **local-as**: Routes in this community are not advertised outside the local AS number.
   - **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.
   - **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.
6. Click **Add**.

Configure Data Prefix

1. In the **Groups of Interest** list, click **Data Prefix**.
2. Click **New Data Prefix List**.
3. Enter a name for the list.
4. Choose either **IPv4** or **IPv6**.
5. In the **Add Data Prefix** field, enter one or more data prefixes separated by commas.
6. Click **Add**.

Configure Policer

1. In the groups of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. Define the policing parameters:

a. In the **Burst** field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.

b. In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. It can be **drop**, which sets the packet loss priority (PLP) to **low**.

   You can use the **remark** action to set the packet loss priority (PLP) to **high**.

c. In the **Rate** field, enter the maximum traffic rate, a value from 0 through $2^{64} – 1$ bits per second (bps).

5. Click **Add**.

Configure Prefix

1. In the groups of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Add Prefix** field, enter one or more data prefixes separated by commas.
5. Click **Add**.

Configure Site

1. In the groups of interest list, click **Site**.
2. Click **New Site List**.
3. Enter a name for the list.
4. In the **Add Site** field, enter one or more site IDs separated by commas.

   For example, 100 or 200 separated by commas or in the range, 1- 4294967295.
5. Click **Add**.

Configure App Probe Class

1. In the groups of interest list, click **App Probe Class**.
2. Click **New App Probe Class**.
3. Enter the probe class name in the **Probe Class Name** field.
4. Select the required forwarding class from the **Forwarding Class** drop-down list.
5. In the **Entries** pane, select the appropriate color from the **Color** drop-down list and enter the **DSCP** value.

   You can add more entries if needed by clicking on the + symbol.
6. Click **Save**.

Configure SLA Class

1. In the groups of interest list, click **SLA Class**.
2. Click **New SLA Class List**.

3. Enter a name for the list.
4. Define the SLA class parameters:
   a. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.
   b. In the **Latency** field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.
   c. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
   d. Select the required app probe class from the **App Probe Class** drop-down list.
5. (Optional) Select the **Fallback Best Tunnel** checkbox to enable the best tunnel criteria.

   This optional filed is available from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a to pick the best path or color from the available colors when SLA is not met. When this option is selected, you can choose the required criteria from the drop-down. The criteria are a combination of one or more of loss, latency, and, jitter values.
6. Select the **Criteria** from the drop-down list. The available criteria are:
   - Latency
   - Loss
   - Jitter
   - Latency, Loss
   - Latency, Jitter
   - Loss, Latency
   - Loss, Jitter
   - Jitter, Latency
   - Jitter, Loss
   - Latency, Loss, Jitter
   - Latency, Jitter, Loss
   - Loss, Latency, Jitter
   - Loss, Jitter, Latency
   - Jitter, Latency, Loss
   - Jitter, Loss, Latency
7. Enter the **Loss Variance (%)**, **Latency Variance (ms)**, and the **Jitter Variance (ms)** for the selected criteria.
8. Click **Add**.

Configure TLOC

1. In the groups of interest list, click **TLOC**.
2. Click **New TLOC List**. The **TLOC List** popup displays.
3. Enter a name for the list.
4. In the **TLOC IP** field, enter the system IP address for the TLOC.
5. In the **Color** field, select the TLOC's color.
6. In the **Encap** field, select the encapsulation type.
7. In the **Preference** field, optionally select a preference to associate with the TLOC.

   The range is 0 to 4294967295.
8. Click **Add TLOC** to add another TLOC to the list.
9. Click **Save**.

Note To use the `set tloc` and `set tloc-list` commands, you must use the set-vpn command.

For each TLOC, specify its address, color, and encapsulation. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the highest preference value is used. If two or more of TLOCs have the highest preference value, traffic is sent among them in an ECMP fashion.

Configure VPN

1. In the groups of interest list, click **VPN**.
2. Click **New VPN List**.
3. Enter a name for the list.
4. In the **Add VPN** field, enter one or more VPN IDs separated by commas.

   For example, 100 or 200 separated by commas or in the range, 1- 65530.
5. Click **Add**.

Configure Region

Minimum release: Cisco vManage Release 20.7.1

To configure a list of regions for Multi-Region Fabric (formerly Hierarchical SD-WAN), ensure that Multi-Region Fabric is enabled in **Administration** > **Settings**.

1. In the groups of interest list, click **Region**.
2. Click **New Region List**.
3. In the **Region List Name** field, enter a name for the region list.

4. In the **Add Region** field, enter one or more regions, separated by commas, or enter a range.

   For example, specify regions 1, 3 with commas, or a range 1-4.

5. Click **Add**.

Click **Next** to move to **Configure Topology and VPN Membership** in the wizard.

Configure Preferred Color Group

Table 113: Feature History

Feature Name	Release Information	Description
Tiered Transport Preference in Application-aware Routing and Data Policy	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature adds support for ranking of Application Aware Routing (AAR) preferred and backup preferred colors. You can configure up to three levels of priority based on the color or path preference on a Cisco IOS XE Catalyst SD-WAN device. You can provide primary, secondary and tertiary priorities based on the color preference in Cisco vManage.

You can configure the order of transport preference to choose the preference order for forwarding traffic.

1. In the groups of interest list, click **Preferred Color Group**.
2. Click **New Preferred Color Group**.
3. In the **Preferred Color Group Name** field, enter a name for the preferred color group.
4. In the **Primary Colors** pane, do the following:
   a. Choose the color preference from the **Color Preference** drop-down list.
   b. Choose the path preference from the **Path Preference** drop-down list.

Field	Description
Preferred Color Group Name	Enter a name of the preferred color group.

Field	Description
Color Preference	Choose the color preference from the drop-down list. The options are: • default • 3g • biz-internet • blue • bronze • custom1 • custom2, and so on You can select multiple colors.
Path Preference	Choose the path preference from the drop-down list. The options are: • Direct Path: Use only a direct path between the source and the destination devices. • Multi Hop Path: In a Multi-Region Fabric network, use a multi-hop path, which includes the core region, between the source and destination devices, even if a direct path is available. • All Paths: Use any path between the source and destination devices. **Note** This option is equivalent to not configuring path preference at all. If you are applying the policy to a non-Multi-Region Fabric network, use this option.

5. In the **Secondary Colors** pane, do the following:
   a. Choose the color preference in the **Color Preference** drop-down list.
   b. Choose the path preference from the **Path Preference** drop-down list.
6. In the **Tertiary Colors** pane, do the following:
   a. Choose the color preference from the **Color Preference** drop-down list.
   b. Choose the path preference from the **Path Preference** drop-down list.
7. Click **Add**.

The following guidelines are helpful when configuring the ranking for colors:

- Primary preference is mandatory, and at each priority level, at least one preference path or color is mandatory. Both can also be configured.
- More than one color can be configured as a preference.
- If path preference is not configured, all paths are constrained by the preferred colors that are available.

- If color preference is not configured within the constraint of the path preference, then all the colors are available.
- The preferences apply in order of priority to determine the path or color for forwarding traffic.

When the primary, secondary, and tertiary colors are down, packets are not dropped. The traffic falls back to the usual routing preference to choose if any other colors are up.

Configure Groups of Interest for Localized Policy

In **Create Groups of Interest**, create lists of groups to use in a localized policy:

In Create Groups of Interest, create new groups of list types as described in the following sections to use in a localized policy:

Configure As Path

1. In the group of interest list, click **AS Path**.
2. Click **New AS Path List**.
3. Enter a name for the list.
4. Enter the AS path, separating AS numbers with a comma.
5. Click **Add**.

   AS Path list specifies one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list separated by commas. To configure multiple AS paths in a single list, include multiple **as-path** options, specifying one AS path in each option.

Configure Community

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. In the group of interest list, click **Community**.
2. Click **New Community List**.
3. Enter a name for the community list.
4. In the **Add Community** field, enter one or more data prefixes separated by commas in any of the following formats:
   - *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.
   - **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices.
   - **local-as**: Routes in this community are not advertised outside the local AS number.

- **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.
- **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.

5. Click **Add**.

Configure Data Prefix

1. In the **Group of Interest** list, click **Data Prefix**.
2. Click **New Data Prefix List**.
3. Enter a name for the list.
4. Enter one or more IP prefixes.
5. Click **Add**.

   A data prefix list specifies one or more IP prefixes. You can specify both unicast and multicast addresses. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

Configure Extended Community

1. In the group of interest list, click **Extended Community**.
2. Click **New Extended Community List**.
3. Enter a name for the list.
4. Enter the BGP extended community in the following formats:
   - **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address.
   - **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.
5. Click **Add**.

Configure Class Map

1. In the group of interest list, click **Class Map**.
2. Click **New Class List**.
3. Enter a name for the class.

4. Select a required queue from the **Queue** drop-down list.
5. Click **Save**.

Configure Mirror

1. In the group of interest list, click **Mirror**.
2. Click **New Mirror List**. The Mirror List popup displays.
3. Enter a name for the list.
4. In the **Remote Destination IP** field, enter the IP address of the destination for which to mirror the packets.
5. In the **Source IP** field, enter the IP address of the source of the packets to mirror.
6. Click **Add**.

   To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets. Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

Configure Policer

1. In the group of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. In the **Burst (bps)** field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes.
5. In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. Select **Drop** (the default) to set the packet loss priority (PLP) to low. Select **Remark** to set the PLP to high.
6. In the **Rate (bps)** field, enter the maximum traffic rate. It can be value from 8 through 2^{64} bps (8 through 100000000000).
7. Click **Add**.

Configure Prefix

1. In the group of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Internet Protocol** field, click either **IPv4** or **IPv6**.
5. Under **Add Prefix**, enter the prefix for the list. (An example is displayed.) Optionally, click the green **Import** link on the right-hand side to import a prefix list.
6. Click **Add**.

Click **Next** to move to **Configure Forwarding Classes/QoS** in the wizard.

Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices

Table 114: Feature History

Feature Name	Release Information	Description
GRE Over IPsec Tunnels Between Cisco IOS XE Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to set up GRE over IPsec tunnels on Cisco IOS XE devices in the controller mode to connect to Cisco IOS XE devices in the autonomous mode.
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This feature allows you to configure an IPv6 GRE or IPSEC tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a service VPN.

Configuring GRE over IPsec tunnels using Cisco SD-WAN Manager is a two-step process:

1. Install Certification Authentication.

   Import the pkcs12 file on the Cisco IOS XE Catalyst SD-WAN device using the **pki import** command. For information, see the **Install Certification Authentication** section in Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI .

2. Prepare the GRE over IPsec tunnel configurations (GRE, IPsec, IKEv2, PKI, OSPFv3 and Multicast) via the Cisco SD-WAN Manager CLI Template, and push it to the Cisco IOS XE Catalyst SD-WAN device. For information about using a device template, see Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN devices.

   See the **Configure GRE Over IPsec Tunnel** section in Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI for a sample configuration for use in the CLI template.

Note Note: Add the **crypto pki trustpoint** configuration command explicitly in the Cisco SD-WAN Manager CLI template.

Configure Interface Based Zones and Default Zone

Table 115: Feature History

Feature Name	Release Information	Description
Configure Interface Based Zones and Default Zone	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enables you to configure an interface-based firewall policy to control traffic between two interfaces or an interface-VPN-based firewall policy to control traffic between an interface and a VPN group. This feature also provides support for default zone where a firewall policy can be configured with a zone pair that consist of a zone and a default zone.

To configure Interface Based Zones and Default Zones in Cisco SD-WAN Manager, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Unified Security Policy**.

   For information on configuring a unified security policy, see Configure Firewall and Unified Security Policy.

   After you have created a firewall policy, click to add a zone pair for the firewall policy.
3. In the **Add NG Firewall Policy** page, click **zoneBasedFW** to create a zone list.

   The **Zone List** page displays
4. Enter a name for the zone.
5. Click a zone type.

   You can choose to configure zones with zone type as **Interface** or as a **VPN**. Based on the zone type you choose, add the interfaces or VPNs to the zones.
6. Click **Save** to save the zone list.
7. In the **Add NG Firewall Policy** page, click **Add Zone-Pairs**.
8. In the **Source Zone** drop-down list, choose the zone that is the source of the data packets.
9. In the **Destination Zone** drop-down list, choose the zone that is the destination of the data packets.

Note Default zone appears in the drop-down list while selecting a zone as part of zone-pair. You can choose default zone for either a source zone or a destination zone, but not both.

10. Click + icon to create a zone pair.
11. Click **Save**.

You configure Interface Based Zones and Default Zone using a CLI device template in Cisco SD-WAN Manager. For information about using a device template, see Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN devices.

To configure Interface Based Zones and Default Zone using the CLI add-on feature template. For information on using the CLI Add-On template, see Create a CLI Add-On Feature Template.

Configure Intra-VPN Service-Side NAT Using a CLI Add-On Template

Table 116: Feature History

Feature Name	Release Information	Description
Intra-VPN Service-Side NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template. Configure the **ip nat outside** command on the LAN interface for which you require translation of the source IP addresses to the outside local addresses.

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Configure Intra-VPN Service-Side NAT Using a CLI Add-On Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device from the device list.
5. Click **CLI Add-On Template** under **OTHER TEMPLATES**.
6. In **CLI Add-On Template** area, enter the configuration.

7. Configure an outside interface using the **ip nat outside** command.
8. Click **Save**.

   The CLI add-on template that you created is displayed in the **CLI Configuration** table.
9. Attach the CLI add-on template to your device.

Configure IPv6 as Preferred Address Family in a Dual Stack Environment

Using Cisco SD-WAN Manager, you can configure Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller to set IPv6 as the default connectivity option for control and data connections.

Table 117: Feature History

Feature Name	Release Information	Description
IPv6 as Preferred Address Family in a Dual Stack Environment	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	This feature allows you to select IPv6 as the preferred address family for control and data connections in a dual stack network environment.

Configure Cisco IOS-XE SD-WAN Devices for IPv6 Connectivity

You can use one of these options to configure an IPv6 connection on Cisco IOS XE Catalyst SD-WAN devices:

- CLI template and CLI add-on template
- Configuration groups
- Quick connect

CLI Template and CLI Add-On Template

Use the CLI template or the CLI add-on template to configure IPv6 for a Cisco IOS XE Catalyst SD-WAN device. The CLI configuration for Cisco IOS XE Catalyst SD-WAN devices is provided in Configure IPv6 as Preferred Address Family in a Dual Stack Environment Using a CLI Template section. For more information about using CLI templates, see CLI Templates and CLI Add-On Feature Templates.

Configuration Groups

To configure an IPv6 connection on Cisco IOS XE Catalyst SD-WAN devices using configuration groups, perform this procedure:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**.

4. Choose one or more Cisco IOS XE Catalyst SD-WAN devices, and then click **Deploy**.
5. In the **Process Overview** window, click **Next**.
6. The **Selected Devices to Deploy** page displays the Cisco IOS XE Catalyst SD-WAN devices you selected previously. Check or uncheck one or more Cisco IOS XE Catalyst SD-WAN devices and then click **Next**.
7. From the **Dual Stack IPv6 Default** drop-down list, choose **True** to set IPv6 as a default connection, and click **Next**.

   The **True** option enables Cisco IOS XE Catalyst SD-WAN devices to establish an IPv6 connection with Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller it is connected to. When you choose **False**, an IPv4 connection is established.

   BFD sessions are established based on the IPv6 option set in local, remote Cisco IOS XE Catalyst SD-WAN devices. In a dual stack environment, when the **True** option is chosen in a local or remote Cisco IOS XE Catalyst SD-WAN device, the BFD session is an IPv6 connection. Otherwise, it is IPv4.

Note The connections from the Cisco IOS XE Catalyst SD-WAN devices to Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual IP stack environment whether the **Dual Stack IPv6 Default** drop-down list options set to **True** or **False.**

8. In the Summary window, click **Deploy**.

For more information on using configuration groups, see Configuration Groups and Feature Profiles.

Quick Connect

To configure an IPv6 connection on Cisco IOS XE Catalyst SD-WAN devices using the quick connect workflow, perform this procedure:

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Quick Connect**.
2. In the **Process Overview** window, click **Next**.
3. Choose an option to sync your devices, and then click **Next**

   For more information, see Quick Connect Workflow
4. In the **Selected devices to bring up** window, check one or more Cisco IOS XE Catalyst SD-WAN devices, and then click **Next**.
5. From the **Dual Stack IPv6 Default** drop-down list, choose **True** to set IPv6 as a default connection and click **Apply**, and then click **Next**.

   The **True** option enables Cisco IOS XE Catalyst SD-WAN devices to establish an IPv6 connection with Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller it is connected to. When you choose **False**, an IPv4 connection is established.

   BFD sessions are established based on the IPv6 option set in local, remote Cisco IOS XE Catalyst SD-WAN devices. In a dual stack environment, If you choose the **True** option in a local or remote Cisco IOS XE Catalyst SD-WAN device, the BFD session is an IPv6 connection. Otherwise, it is IPv4.

Note The connections from the Cisco IOS XE Catalyst SD-WAN devices to Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual IP stack environment whether you choose the **True** or the **False** option.

6. In the Summary window, click **Deploy**.

Configure Cisco SD-WAN Manager and Cisco SD-WAN Controller for IPv6 Connectivity

You can use one of these options to configure an IPv6 connection on Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller:

- CLI template and CLI add-on template
- Feature template

CLI Template

Use the CLI template to configure IPv6 in Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller. The CLI configuration for Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller is provided in Configure IPv6 as Preferred Address Family in a Dual Stack Environment Using a CLI Template. For more information about using CLI templates, see CLI Templates.

Feature Template

To configure an IPv6 connection in Cisco SD-WAN Manager using the feature template, peform this procedure:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and choose **Add Template**.
3. Choose a Cisco SD-WAN controller.
4. Under **BASIC INFORMATION**, click **System**.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain all characters and spaces.
7. Under the **Basic Information** tab, click the **On** radio button adjacent to **Dual Stack IPv6 Default** field to set IPv6 as a default connection.

   The **On** option sets Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller to establish an IPv6 connection with all other Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller instances. When you click the **Off** radio button, an IPv4 connection is established.

Note The connections from Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller to Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual IP stack environment irrespective of whether you click the **On** or **Off** radio button.

8. Click **Save**.

Configure Cisco Catalyst SD-WAN Identity-Based Firewall Policy

Table 118: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Identity-Based Firewall Policy	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature lets you to configure user-identity-based firewall policies for unified security policies.
Cisco Catalyst SD-WAN Identity-Based Firewall Policy Enhancement for SGT Integration	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This feature lets you to configure policies based on Security Group Tags.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW. You can create firewall rules or rulesets with IPv6 as the address type in a unified security policy. For more information, see Create Identity-Based Unified Security Firewall Policy, on page 381.

Perform the following tasks to create an identity-based unified security firewall policy:

1. Configure Cisco ISE for Microsoft Active Directory Services.
2. Configure PxGrid in Cisco ISE for connectivity to Cisco SD-WAN Controller.
3. Configure Cisco ISE in Cisco SD-WAN Manager.
4. Create an identity list.
5. Create an identity-based unified security firewall policy.

Configure Cisco ISE for Microsoft Active Directory Services

Microsoft Active Directory Services must be configured in Cisco ISE to fetch all the user and user group information. For information on configuring Microsoft Active Directory Services in Cisco ISE, see AD Integration for Cisco ISE GUI and CLI Login.

Configure PxGrid in Cisco ISE for Connectivity to Cisco SD-WAN Controller

The **Allow password-based account creation** option for Cisco Platform Exchange Grid (pxGrid) services Services must be enabled in Cisco ISE. This is necessary for connectivity from pxGrid to the Cisco Catalyst SD-WAN Controller because the Cisco Catalyst SD-WAN Controller uses a password-based mechanism to authenticate with pxGrid. For information on configuring pxGrid in Cisco ISE, see pxGrid Settings.

Note Enable the ERS option by choosing **Administration** > **Settings** > **API Settings** > **API Service Settings** in ISE in order to enable pxGrid services for Cisco ISE connectivity to Cisco Catalyst SD-WAN Controller.

Configure Cisco ISE in Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Integration Management.**.
2. Click **Identity Services Engine**.
3. Click **Add Connection**. .

   The **Add ISE Server** window is displayed.
4. Specify an IP address in the **ISE Server IP address** field.
5. Enter a username and password to connect to Cisco ISE.
6. Choose the VPN over which connectivity to Cisco ISE must be established.
7. In the **ISE Server CA** pane, choose a file from your desktop or drag and drop to upload.

Note You can download the Cisco ISE server certificate from Cisco ISE. For details on Cisco ISE certificates, see Generate Certificate Signing Request (CSR).

8. In the **PxGrid Server CA** pane, choose a file from your desktop or drag and drop to upload.

Note You can download the PxGrid server certificate from Cisco ISE. For details on Cisco ISE certificates, see Generate Certificate Signing Request (CSR).

9. (Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1) In the **Feature Subscription** field, select the feature for which you want to retrieve the metadata information from Cisco ISE. The options are:

   - **User/User Groups**

- **Security Group Tag (SGT)**

10. For **User/User Groups**, enter the **AD Joint Point** name and the **AD Domain** name, as defined in Cisco ISE.
11. Click **Submit**.

    A connection to Cisco ISE is initiated. An automatic template push to the Cisco SD-WAN Controller is initiated based on the username and password, Cisco ISE Server IP address, AD domain name, and VPN name. The Cisco SD-WAN Controller then connects to pxGrid using the pxGrid APIs, and opens a web socket connection.

    When the Cisco Catalyst SD-WAN Controller establishes a connection to Cisco ISE, information about user and user groups is retrieved from Cisco ISE and distributed to the Cisco IOS XE Catalyst SD-WAN devices.

    To view the list of users and user groups available in the corresponding domain, choose **Actions** > **View ISE Data**.

Create an Identity List

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Custom Options**.
3. Click **Lists**.
4. Click **Identity**.

Note If you have not completed the integration of Cisco ISE Controller with Cisco SD-WAN Manager, a message instructs you to complete the integration. After you complete this integration, the **Add an Identity list** link is displayed in **Identity List** window.

5. Click **Add an Identity list**.
6. Enter a name for the identity list.
7. Enter a description for the identity list.
8. (Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a)

    In the **Subscription Type** drop-down list, choose one of the following:

    - **User/ User Group**
    - **Security Group Tag (SGT)**

Note You can configure either **User/ User Group** or **Security Group Tag (SGT)** at a given point, not both.

9. If you choose **Security Group Tag (SGT)**, select one or more SGTs and click **Add**.

After you add the SGT identity list, you can use it in a unified security policy to create source-based or destination-based identity security firewall policies.

10. If you choose **User/User Groups**, select the user groups and click **Add**. If the user information is available, the **User Groups** list displays all the user groups. You can select a maximum of 16 user groups.

    After you add the identity list, you can use it in a unified security policy to create a user-identity-based security firewall policy.

Create Identity-Based Unified Security Firewall Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Unified Security Policy**.
3. Click **Add NG Firewall Policy**.
4. Click **Create New**.
5. In the **Name** field, enter a name for the policy.
6. In the **Description** field, enter a description for the policy.
7. Click **Add Rule**.
8. From the **Order** drop-down list, choose the order for the rule .
9. Enter a name for the rule.
10. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type.
11. From the **Action** drop-down list, choose an action for the rule.
    - **Inspect**
    - **Pass**
    - **Drop**
12. (Optional) Check the **Log** check box if you want matches for this rule to be logged.

Note Cisco SD-WAN Manager supports log flow only at the rule level and not at the global level.

13. Choose an advanced inspection profile to attach to the policy. This field is available only if you have chosen the action rule as **Inspect**. If you have created an advanced inspection profile, this field lists all the advanced inspection profiles that you have created. Choose an advanced inspection profile from the list. For information on creating an advanced inspection profile, see Create an Advanced Inspection Profile.
14. Click **Source**, and choose **Identity** as the filter type
15. Click **Destination**, and choose one of the following options:

- **Object Group**: Use an object group for your rule.

  To create a new object group, click **New Object Group List**. Set the filters for matching, and then click **Save**. For information on creating an object group, see Create an Object Group .

- **Type**: You can choose from IPv4 prefixes, IPv6 prefixes, prefix lists, fully qualified domain names (FQDN), lists, or Geo Location based on the IP address type that you choose. When you configure SGT in the list, identity can be a filter type.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Type** field displays the prefix options.

16. Click **Save**.
17. Click **Protocol** to configure a protocol for the rule.
18. Click **Application List** to configure a list of applications you want to include in the rule. An application is subject to inspection, dropped, or allowed to pass, based on the application list you configure, and the other filters that you set for the rule.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and Cisco vManage Release 20.6.1, the applications are attached directly to a rule the way other filters are. If configured as part of access control lists (ACLs), they are attached to a class map along with the source and destination.

19. Click **Save** to save the rule.
20. Click **Save Unified Security Policy**.
21. Click **Add Zone Pair** to apply the policy to a zone pair. For information, see Add a Zone Pair.
22. To edit or delete a unified security policy, click **…**, and choose an option.
23. Click **Next** to configure the next security block in the wizard in which have the option to configure DNS Security. For more information, see Configure Umbrella DNS Policy Using vManage.
24. Click **Next**.

    The **Policy Summary** page is displayed. For information on this page, see Create Unified Security Policy Summary.

Configure Lawful Intercept 2.0 Workflow

Table 119: Feature History

Feature Name	Release Information	Description
Lawful Intercept 2.0	Cisco vManage Release 20.9.1	This feature lets you configure a Lawful Intercept in Cisco SD-WAN Manager. Cisco SD-WAN Manager and Cisco SD-WAN Controller provides LEA with key information so that they can decrypt the Cisco Catalyst SD-WAN IPsec traffic captured by the MSP.
Lawful Intercept 2.0 Enhancements	Cisco vManage Release 20.10.1	This feature enhances the Cisco SD-WAN Manager GUI and the troubleshooting options available for the Lawful Intercept feature in Cisco Catalyst SD-WAN.
Lawful Intercept 2.0 Enhancements	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature extends Lawful Intercept to multitenancy mode, and provides support for Cisco SD-WAN Manager clusters. For more information on Cisco SD-WAN Manager clusters, see Cluster Management.

Note The Lawful Intercept feature can be configured only through Cisco SD-WAN Manager, and not through the CLI.

To configure Lawful Intercept in Cisco SD-WAN Manager, perform the following steps:

1. Create Lawful Intercept Administrator
2. Create Lawful Intercept API User
3. Create an Intercept

Configure Multiple IdPs

Table 120: Feature History

Feature Name	Release Information	Description
Single Sign-On Using Azure Active Directory (AD)	Cisco vManage Release 20.8.1	You can configure Azure AD as an external IdP using Cisco SD-WAN Manager and the Azure AD administration portal.
Configure Multiple IdPs for Single Sign-On Users of Cisco SD-WAN Manager	Cisco vManage Release 20.10.1	With this feature, you can configure up to three IdPs for providing different levels of access for single sign-on users of Cisco SD-WAN Manager.

Minimum supported release: Cisco vManage Release 20.10.1

The following workflow is for configuring multiple IdPs. For more information on enabling an IdP, see Enable an Identity Provider in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Identity Provider Settings** and choose **Edit**.
3. Click **Add New IDP Settings**.

Note After three IdPs are configured, the **Add New IDP Settings** option is no longer displayed.

4. Click the toggle button to switch between enabling and disabling IdP settings while retaining the existing configuration.
5. Click **IDP Name** and enter a unique name for your IdP.

   Examples:

   - **okta**
   - **idp1**
   - **provider**
   - **msp**

   You can configure a maximum of three IdPs.

Note You cannot map the same domain to multiple IdPs, but you can use the same IdP for multiple domains.

6. Click **Domain** and enter a unique domain name for your IdP, for example, okta.com.

   If the domain name already exists, Cisco SD-WAN Manager generates an error message.

Note You can also add a domain later to an existing IdP.

7. In the **Upload Identity Provider Metadata** section, upload the SAML metadata file you downloaded from your IdP.
8. Click **Save**.
9. After you configure a new IdP name, domain, and sign out of your current Cisco SD-WAN Manager session, you are redirected to a unified SAML login page.
10. In the unified SAML login page, if you require local authentication, remove the **login.html** portion of the URL. This redirects you to the local authentication page.

Note A user ID must be in an email address format, for example, **john@mystore.com**.

11. In the unified SAML login page, enter the SSO credentials for your IdP.

Note You are redirected to the unified SAML login page each time you access Cisco SD-WAN Manager after configuring a new IdP name and domain.

Configure NAT DIA IPv4 over an IPv6 Tunnel Using a CLI Add-On Template

Table 121: Feature History

Feature Name	Release Information	Description
Support for NAT DIA IPv4 over an IPv6 Tunnel	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can use this feature to route IPv4 traffic to the internet over an IPv6 tunnel. You can configure NAT DIA IPv4 over an IPv6 tunnel using the CLI or a CLI add-on template.

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Configure NAT DIA IPv4 over an IPv6 Tunnel Using a CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Choose a device from the device list.
5. In the **OTHER TEMPLATES** area, click **CLI Add-On Template**.
6. In the **CLI Add-On Template** area, enter the configuration.
7. Configure IPv4 over an IPv6 tunnel as shown in the following example configuration:

```
interface Tunnel1000
 no shutdown
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
```

```
 load-interval 30
 tunnel source GigabitEthernet1
 tunnel destination 2001:DB8:A1:10::10
 tunnel mode ipv6
 tunnel path-mtu-discovery
 tunnel route-via GigabitEthernet1 mandatory
!
ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel1000 overload
ip route 0.0.0.0 0.0.0.0 Tunnel1000 203.0.113.2
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

8. Click **Save**.

   The CLI add-on template that you created is displayed in the **CLI Configuration** table.

9. Attach the CLI add-on template to your device.

Configure NAT66 DIA

Table 122: Feature History

Feature Name	Release Information	Description
Support for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure NAT66 DIA using Cisco SD-WAN Manager, the CLI, or a device CLI template. NAT66 DIA allows you to direct local IPv6 internet traffic to exit directly to the internet from the service-side VPN (VPN 1) through the transport VPN (VPN 0).
Support for Multiple WAN Links for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can configure NAT66 to use multiple WAN links to direct local IPv6 traffic to exit directly to the internet.

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

Note In Cisco vManage Release 20.7.x release, **Feature Templates** is titled **Feature**.

3. Edit a **Cisco VPN Interface Ethernet** template by clicking **. . .** adjacent to it, and then choosing **Edit**.
4. Click **NAT** and choose **IPv6**.
5. In the **NAT** drop-down list, change the scope from **Default** to **Global**.

   Click **On** to enable NAT66.
6. In the **NAT Selection** field, choose **NAT66**.
7. Click **New Static NAT**.

8. In the **Source Prefix** field, specify the source IPv6 prefix.
9. In the **Translated Source Prefix** field, specify the translated source prefix.
10. In the **Source VPN ID** field, specify the source VPN ID.
11. Click **Update**.

Configure a NAT66 DIA Route

Enable an IPv6 route with NAT66 DIA in a **Cisco VPN** template.

Every service VPN, for example, VPN 1, routes packets into the transport VPN (VPN 0) for DIA traffic.

Configure a NAT66 DIA Route Using a Cisco VPN Template

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

Note In Cisco vManage Release 20.7.x release, **Feature Templates** is titled **Feature**.

3. Edit a **Cisco VPN** template by clicking **. . .** adjacent to it, and then choosing **Edit**.
4. Click **IPv6 Route**.
5. Click **New IPv6 Route**.
6. In the **Prefix** field, enter an IPv6 prefix for NAT66 translation.

   Global inside and outside prefixes should be unique per virtual routing and forwarding (VRF).

   IPv6-prefix delegation (PD) prefix length should be equal to or less than /56.

   A global outside prefix should be unique per VRF.

   The inside prefix length and an outside prefix length should be the same.

   Up to 250 VRFs are supported with a PD prefix of /56.
7. In the **Gateway** field, click **VPN**.
8. In the **Enable VPN** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable VPN.
9. In the **NAT** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable NAT66.
10. Click **Update**.

Configure On-Demand Tunnels Using Cisco SD-WAN Manager

Table 123: Feature History

Feature Name	Release Information	Description
Dynamic On-Demand Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can configure on-demand tunnels between any two Cisco Catalyst SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices.

Note

- See the Prerequisites for On-Demand Tunnels.
- Do not enable on-demand on the hub device.

On the spoke devices, enable on-demand at the system level on all VPN-0 transport interfaces. In the case of multi-homed sites, enable on-demand on all systems in the site.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Select a device.
5. From **Basic Information**, select **Cisco System**.
6. Click **Advanced**.
7. Enable **On-demand Tunnel**.
8. (optional) Configure the **On-demand Tunnel Idle Timeout** time. The default idle timeout value is 10 minutes. Range: 1 to 65535 minutes
9. Attach the System feature template to the device template for the spoke device.

Configure Per-VPN QoS

Table 124: Feature History

Feature Name	Release Information	Description
Per-VPN QoS	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	When a Cisco IOS XE Catalyst SD-WAN device receives traffic belonging to different VPNs from the branch network, you can configure a QoS policy to limit the bandwidth that can be used by the traffic belonging to each VPN or each group of VPNs.

Create Forwarding Classes

When you create a forwarding class, you map it to a queue. By associating traffic from different applications with different classes, you can ensure that the packets enter different queues. Using the QoS map, you can configure the outbound bandwidth, buffer and other properties for each queue to prioritize among the traffic streams served by these queues and achieve the desired QoS.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. From the list types on the left, click **Class Map**.
5. Click **New Class List**.
   a. Enter a unique name for the forwarding class.
   b. Choose a queue to which to map the forwarding class.
   c. Click **Save**.
6. Repeat Step 5 and the substeps to create more forwarding classes.

Create VPN Lists

A VPN list consists of one or more VPNs that need to be treated alike. To apply a specific QoS policy to traffic from a VPN or a group of similar VPNs, the QoS policy is linked to the corresponding VPN list.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. From the list types on the left, click **VPN**.

5. Click **New VPN List**.
   a. Enter a unique name for the VPN list.
   b. Enter the IDs of the VPNs to be included in the list.
   c. Click **Add**.
6. Repeat Step 5 and the substeps to create more VPN lists.

Create QoS Maps

Use QoS maps to distribute resources such as bandwidth and buffer among forwarding classes. Create as many QoS maps as required to apply different QoS policies to the different VPN lists.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. Click **Next**.
5. Click **Add QoS Map** and click **Create New**.
6. Enter a unique name for the QoS map.
7. Enter a description for the QoS map.
8. Click **Add Queue**.
   a. Choose a queue to add to the map.
   b. Choose the bandwidth percentage to allocate to the queue.
   c. Choose the buffer percentage to allocate to the queue.
   d. Packets exceeding the bandwidth or buffer percentage are dropped. Choose whether the packets are dropped randomly (**Random Early**) or from the end of the queue (**Tail**).
   e. Click **Save Queue**.
9. Repeat Step 8 and the substeps to add as more queues.
10. Click **Save Policy**.

Create VPN QoS Map

Use a VPN QoS Map to associate QoS policies with target VPN lists.

Note Before you proceed with the following steps, configure the required QoS Maps and VPN lists.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

2. Click **Localized Policy**.
3. Click **Add Policy** and click **Next**.
4. Create or import QoS maps and click **Next**.
5. Click **VPN QoS Map**.
6. Click **Add VPN Policy** and click **Create New**.
7. Enter a unique name and a description for the VPN QoS map.
8. For the default VPN, click the Edit icon.
   a. (Optional) Enter the maximum bandwidth for traffic belonging to the default VPN.
   b. Choose a QoS Map to apply a QoS policy to the default VPN.
   c. Click **Save VPN**.
9. Click **Add VPN**.
   a. Choose a VPN list.
   b. Enter the minimum bandwidth for traffic belonging to the VPNs.
   c. (Optional) Enter the maximum bandwidth for traffic belonging to the VPNs.
   d. Choose a QoS Map to apply a QoS policy to the VPNs.
   e. Click **Save VPN**.
10. Repeat Step 9 and the substeps to add more VPN lists.
11. Click **Save Policy**.
12. Apply the localized policy to the relevant device template.

Configure Extended Anti-Replay Window

Configure extended anti-replay window on both the source and remote Cisco IOS XE Catalyst SD-WAN devices.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. In the list of templates, locate the Cisco Security template for the Cisco IOS XE Catalyst SD-WAN device.
4. Click **...** for the template and choose **Edit**.
5. Choose **Basic Configuration**.
6. To enable **Extended Anti Replay**, click **On**.

7. (Optional) Enter **Extended Anti-Replay Window** duration.

   Default duration: 256 ms

   Range: 10 ms to 2048 ms

Note Choose an appropriate duration based on the configured queue limits and the traffic profile.

8. Click **Update**.

Attach VPN QoS Map to WAN Interface

To apply the QoS policy per VPN, attach the VPN QoS map to the Cisco VPN Interface Ethernet template for the WAN interface.

Note Before you proceed with the following steps, apply the localized policy in which the VPN-QoS Map is defined to the relevant device template.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. In the list of templates, locate the Cisco VPN Interface Ethernet template for the WAN interface.
4. Click **...** adjacent to the template and choose **Edit**.
5. Choose **ACL/QoS**.
6. For **Shaping Rate (kbps)**, choose the configuration type as **Global** and enter a shaping rate value.
7. For **VPN QoS Map**, choose the configuration type as **Global** and enter the name of the VPN QoS map.
8. Click **Update**.

Configure a PIM BSR

Table 125: Feature History

Feature Name	Release Information	Description
Dynamic Rendezvous Point (RP) Selection by a PIM BSR	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure automatic selection of an RP candidate using a PIM BSR in an IPv4 multicast overlay.

Prerequisites for Configuring a BSR Candidate

- Every Cisco Catalyst SD-WAN site must have its own RP.
- SPT-only mode must be enabled on all Cisco Catalyst SD-WAN sites.

Note For a BSR to work for any multicast stream that spans across Cisco Catalyst SD-WAN sites, SPT-only mode is mandatory. For a BSR within a local-site multicast stream within a Cisco Catalyst SD-WAN site, it is not necessary to enable SPT-only mode.

Workflow

For a PIM BSR to elect the RP, configure the following in Cisco SD-WAN Manager:

1. Multicast feature template with **SPT Only** set to **On** for the selected Cisco IOS XE Catalyst SD-WAN device.
2. PIM feature template with an interface.
3. RP candidate.
4. BSR candidate.

Configure Shortest-Path Tree (SPT-Only) Mode for a Multicast Feature Template

In Cisco SD-WAN Manager, configure **SPT Only** mode to ensure that the RPs can communicate with each other using the shortest-path tree.

Note When configuring a BSR, configuration of **SPT Only** mode is mandatory.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. From the **Select Devices** drop-down list, choose a Cisco IOS XE Catalyst SD-WAN device.
5. Under **Other Templates**, choose **Cisco Multicast**.
6. In the **Template Name** field, enter a name for the template.
7. In the **Description** field, enter a description of the template.

   The description can be up to 2048 characters and can contain only alphanumeric characters.
8. Under the **Basic Configuration** section for **SPT Only**, choose **On**.
9. To enable the **Local Replicator** on the device, choose **On** (otherwise keep it set to **Off**).
10. To configure a replicator, choose **Threshold**, and specify a value. (Optional, keep it set to the default value if you are not configuring a replicator).
11. Click **Save**.

Configure a PIM Feature Template and Add an Interface

Configure a PIM feature template and add an interface for an RP and the BSR candidate.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. From the **Select Devices** drop-down list, choose a Cisco IOS XE Catalyst SD-WAN device.
5. Under **Other Templates**, choose **Cisco PIM**.
6. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the **Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
8. Click **Interface**.

   For information on how to configure a PIM interface, see Configure PIM.
9. Click **New Interface**.
10. In the **Interface Name** field, specify an interface with a value.
11. In the **Query Interval (seconds)** field, the field auto-populates.

12. In the **Join/Prune Interval (seconds)** field, the field auto-populates.
13. Click **Add**.
14. Click **Save**.

Configure the RP Candidate

Configure the same Cisco IOS XE Catalyst SD-WAN device as the candidate RP for all multicast groups or selective groups.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Edit the PIM feature template that you created by clicking **...** and then clicking **Edit**.
4. Click **Basic Configuration**.
5. Click **RP Candidate**.
6. Click **New RP Candidate**.
7. From the **Interface** drop-down list, choose the interface that you used for configuring the PIM feature template.
8. (Optional) In the **Access List** field, if you have configured the access list with a value, add the same value.
9. (Optional) In the **Interval** field, if you have configured the interval with a value, add the same interval value.
10. In the **Priority** field, specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device.
11. Click **Add**.
12. Click **Update** to save your configuration changes.

Configure the BSR Candidate

1. Repeat Step 1 through Step 4 from the *Configure the RP Candidate* section.
2. Click **BSR Candidate**.
3. In the **BSR Candidate** field, chose the same interface from the drop-down list that you used for configuring the PIM feature template.
4. (Optional) In the **Hash Mask Length** field, specify the hash mask length.

   Valid values for hash mask length are from 0 – 32.
5. In the **Priority** field, specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device.

6. (Optional) In the **RP Candidate Access List** field, if you have configured the RP candidate access list with a value, add the same value.

   An RP candidate uses a standard access control list (ACL) where you can enter the name for the access list.

7. Click **Update** to save your configuration changes.

Configure Port Forwarding with NAT DIA

Table 126: Feature History

Feature Name	Release Information	Description
Support for Port Forwarding with NAT DIA	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, you can define one or more port-forwarding rules to send packets received on a particular port from an external network to reach devices on an internal network.

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

Create port-forwarding rules to allow access to a private network from the public domain.

Before You Begin

1. Configure and apply a data policy.
2. Configure a **Cisco VPN Interface Ethernet** template or edit an existing **Cisco VPN Interface Ethernet** template.
3. Configure interface overload mode. Interface overload mode is enabled by default.
4. Configure a NAT pool.

Configure Port Forwarding with NAT DIA

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. To edit a **Cisco VPN Interface Ethernet** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Under **NAT Pool**, click **New NAT Pool**.

6. Enter the required NAT pool parameters.

   For more information on the NAT pool parameters, see Configure a NAT Pool and a Loopback Interface.

7. Click **Add**.

8. To create a port-forwarding rule, click **Port Forward** > **New Port Forwarding Rule** and configure the parameters as described in the table.

Table 127: Port-Forwarding Parameters for NAT DIA

Parameter Name	Description
Protocol	Choose the **TCP** or **UDP** protocol to which to apply the port-forwarding rule. To match the same ports for both TCP and UDP traffic, configure two rules.
Source IP Address	Enter the source IP address to be translated.
Source Port	Enter a port number to define the source port to be translated. Range is 0 to 65535.
Translated Source IP Address	Specify the NAT IP address that will be advertised into OMP. Port forwarding is applied to traffic that is destined to this IP address from the overlay with the translated port match.
Translate Port	Enter the port number to apply port forwarding to. Range is 0 to 65535. Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, static translated source IP addresses must be within the configured dynamic NAT pool IP address range.
Static NAT Direction	Select the direction in which to perform network address translation.
Source VPN ID	Specify the service-side VPN from which the traffic is being sent.

9. Click **Update**.

Configure Redirect DNS in a Service-Side VPN

Table 128: Feature History

Feature Name	Release Information	Description
Redirect DNS in a Service-Side VPN	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can configure redirect DNS using Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

2. From the **Custom Options** drop-down list, choose **Traffic Policy** from the **Centralized Policy** menu.
3. Click **Traffic Data** to create a traffic data policy.
4. From the **Add Policy** drop-down list, choose **Create New**.
5. In the **Name** and **Description**, enter a name and a description for the data policy.
6. Click **Sequence Type**.

   The **Add Data Policy** dialog box is displayed.
7. Choose the type of data policy that you want to create—**Application Firewall**, **QoS**, **Service Chaining**, **Traffic Engineering**, or **Custom**.

   A policy sequence containing the selected type of data policy is added in the left pane.
8. Double-click the text string, and enter a name for the policy sequence.

   The name you type is displayed both in the **Sequence Type** list in the left pane and in the right pane.
9. Click **Sequence Rule**. The **Match/Action** dialog box is displayed, where **Match** is selected by default. The available policy match conditions are listed in the menu.
10. From the **Protocol** drop-down list, choose **IPv4** to apply the policy only to IPv4 address families.
11. To choose one or more **Match** conditions, click the fields and set the values as described.

Note Not all match conditions are available for all policy sequence types.

12. To select the actions to take on matching data traffic, click the **Actions** menu.
13. To drop matching traffic, click **Drop**.

    The available policy actions are listed on the right side.
14. To accept matching traffic, click **Accept**.

    The available policy actions are listed on the right side.
15. In the **Actions** menu, choose **Redirect DNS** to configure redirect DNS.
16. In the **Redirect DNS** condition field, enter the **IP Address** and click **Save Match and Actions**.
17. Click **Save Data Policy**.

Match Condition	Procedure
None (match all the packets)	Do not specify any match conditions.

Match Condition	Procedure
Applications / Application Family List / Custom Applications	**1.** In the **Match** conditions menu, click **Applications/Application Family List**. **2.** From the drop-down list, choose the application family. **3.** To create an application list: **a.** Click **New Application List**. **b.** Enter a name for the list. **c.** Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications. **d.** From the **Select Application** drop-down list, choose the corresponding applications or application families. **e.** Click **Save**.
DNS Application List	Add an application list to enable split DNS: **1.** In the **Match** conditions menu, click **DNS Application List**. **2.** From the drop-down list, choose the application family.
DNS	Add an application list to process split DNS: **1.** In the **Match** conditions menu, click **DNS**. **2.** From the drop-down list, choose **Request** to process DNS requests for the DNS applications.
Destination Data Prefix	**1.** In the **Match** conditions menu, click **Destination Data Prefix**. **2.** To match a list of destination prefixes, from the **Data Prefix** drop-down list, choose a list. **3.** To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field.
Destination Port	**1.** In the **Match** conditions menu, click **Destination Port**. **2.** In the **Destination Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with two numbers separated with a hyphen [-]).
DSCP	**1.** In the **Match** conditions menu, click **DSCP**. **2.** In the **DSCP** field, enter the DSCP value—a number from 0 through 63.
Packet Length	**1.** In the **Match** conditions menu, click **Packet Length**. **2.** In the **Packet Length** field, enter the length—a value from 0 through 65535.
PLP	**1.** In the **Match** conditions menu, click **PLP** to set the **Packet Loss Priority**. **2.** From the **PLP** drop-down list, choose **Low** or **High**.

Match Condition	Procedure
Protocol	**1.** In the **Match** conditions menu, click **Protocol**. **2.** In the **Protocol** field, enter the Internet Protocol number—a number from 0 through 255.
Source Data Prefix	**1.** In the **Match** conditions menu, click **Source Data Prefix**. **2.** To match a list of source prefixes, from the **Source Data Prefix List** drop-down list. choose a data prefix list. **3.** To match an individual source prefix, enter the prefix in the **Source** field.
Source Port	**1.** In the **Match** conditions menu, click **Source Port**. **2.** In the **Source** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Create Rules

Table 129: Feature History

Feature Name	Release Information	Description
Firewall FQDN Support	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This enhancement adds support to define a firewall policy using fully qualified domain names (FQDN), rather than only IP addresses. One advantage of using FQDNs is that they account for changes in the IP addresses assigned to the FQDN if this changes in the future.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.

Notes

- The FQDN is intended to be used for matching standalone servers in data centers or a private cloud. When matching public URLs, the recommended match action is 'drop'. If you use 'inspect' for public URLs, you must define all related sub-urls/redirect-urls under the FQDN pattern.

Limitations

- Maximum number of fully qualified domain name (FQDN) patterns supported for a rule under firewall policy: 64
- Maximum number of entries for FQDN to IP address mapping supported in the database: 5000

- If a firewall policy uses an FQDN in a rule, the policy must explicitly allow DNS packets, or resolution will fail.
- Firewall policy does not support mapping multiple FQDNs to a single IP address.
- Only two forms of FQDN are supported: full name or a name beginning with an asterisk (*) wildcard.

  Example: *.cisco.com
- If you choose the IP address type as IPv6 while creating a firewall rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list of Source Data Prefix(es). Additionally, Application Layer Gateway (ALG) is not supported for IPv6.

1. Start the Security Policy Configuration Wizard
2. In the **Name** field, enter a name for the policy.
3. In the **Description** field, enter a description for the policy.
4. Depending on your release of Cisco SD-WAN Manager, do one of the following:
   - Cisco vManage Release 20.4.1 and later releases:
     a. Click **Add Rule/Rule Set Rule**.
     b. Click **Add Rule**.
   - Cisco vManage Release 20.3.2 and earlier releases: click **Add Rule**.

   The zone-based firewall configuration wizard opens.
5. Choose the order for the rule.
6. Enter a name for the rule.
7. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type.
8. Choose an action for the rule:
   - **Inspect**
   - **Pass**
   - **Drop**
9. If you want matches for this rule to be logged, check the **Log** check box.
10. Configure one or more of the following fields.

Note For the following fields, you can also enter defined lists or define a list from within the window.

Table 130: Firewall Rules

Field	Description
Source Data Prefixes	IPv4 prefixes or IPv6 prefixes or prefix lists and/or domain names (FQDN) or list(s). Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Source Data Prefixes** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list of Source Data Prefix(es). Additionally, Application Layer Gateway (ALG) is not supported for IPv6.
Source Port(s)	Source port(s) and/or lists
Destination Data Prefix(es)	IPv4 prefixes or prefix list(s) and/or domain names (FQDN) or list(s) Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Destination Data Prefix(es)** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list. Additionally, ALG is not supported for IPv6.
Destination Ports	Destination ports and/or lists **Note** Destination ports or destination port lists cannot be used with protocols or protocol lists.
Protocol(s)	Protocols and/or list(s)
Application List(s)	Applications and/or lists **Note** If you chose an Application or Application Family List, you must choose at least one other match condition.

11. Click **Save** to save the rule.
12. (Optional) Repeat steps 4–10 to add more rules.
13. Click **Save Firewall Policy**.

Create Rule Sets

Table 131: Feature History

Feature Name	Release Information	Description
Support for Rule Sets	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can now configure sets of rules that are called rule sets that have the same intent. You can also re-use rule sets between security policies.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.

1. Start the Security Policy Configuration Wizard
2. Click **Add Rule/Rule Set Rule**. The zone-based firewall configuration wizard opens.
3. To add a rule set, click **Add Rule Set**.
4. Choose the order for the rule set.
5. Enter a name for the rule set.
6. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type.
7. Choose an action for the rule:
   - **Inspect**
   - **Pass**
   - **Drop**
8. If you want matches for this rule to be logged, check the **Log** check box.
9. Click + next to Rule Sets.
10. Choose from existing rule sets or click **+ New List** to create a new list.
    - To choose from an existing rule: click the existing rule(s) and click **Save**.
    - To create a new rule list **Cick + New List**.
      a. Configure a rule using one or more of the following fields.

Table 132: Firewall Rules

Field	Description
Source Data Prefix(es)	IPv4 prefixes or prefix lists and/or domain names (FQDN) or list(s) Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Source Data Prefixes** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list of Source Data Prefix(es). Additionally, Application Layer Gateway (ALG) is not supported for IPv6.
Source Port(s)	Source port(s) and/or list(s)
Destination Data Prefix(es)	IPv4 prefixes or prefix lists and/or domain names (FQDN) or list(s) Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Destination Data Prefix(es)** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list. Additionally, ALG is not supported for IPv6.
Destination Ports	Destination port(s) and/or list(s) **Note** Destination ports or destination port lists cannot be used with protocols or protocol lists.
Protocol(s)	Protocols and/or lists
Application List(s)	Applications and/or list(s) **Note** If you chose an Application or Application Family List, you must choose at least one other match condition.

b. Click **Save** to save the rule.

c. (Optional) Add more rules by repeating steps 7 and 8.

11. Click **Save** to save the rule set.

12. Click + next to Application List To Drop.

13. Choose existing lists or create your own.
14. Click **Save**.
15. Review the rule set and click **Save**.
16. (Optional) Create additional rule sets or reorder the rule sets and/or rules if required.
17. Click **Save Firewall Policy**.

You can also create rule sets from outside the Security Policy Wizard as follows:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Custom Options**.
3. Click **Lists**.
4. Click **Rule Sets**.
5. Click **New Rule Set**.
6. You can now choose from the various parameters such as source data prefix, port, protocol, and so on. When you create your rule, click **Save Rule** to save the rule and add it to your rule set.
7. Create any additional rules that you want to add to your rule set.
8. After creating all the rules that you want for your rule set, click **Save Rule Set**.

Configure HTTP/HTTPS Proxy Server

Table 133: Feature History

Feature Name	Release Information	Description
HTTP/HTTPS Proxy Server for Cisco SD-WAN Manager Communication with External Servers	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	Cisco SD-WAN Manager uses HTTP/HTTPS to access some web services and for some REST API calls. With this feature, you can channel the HTTP/HTTPS communication through an HTTP/HTTPS proxy server.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. For the **HTTP/HTTPS Proxy** setting, click **Edit**.
3. For the **Enable HTTP/HTTPS Proxy** setting, click **Enabled**.
4. Enter the **HTTP/HTTPS Proxy IP Address** and **Port** number.
5. Click **Save**.

Note Cisco SD-WAN Manager uses TCP port 7 echo request to validate reachability of the proxy server. Ensure that you configure your firewall and proxy server to allow the echo requests to make the destination host ports accessible.

Cisco SD-WAN Manager verifies that the HTTP/HTTPS proxy server is reachable and saves the server details in the configuration database. HTTP/HTTPS connections and REST API calls to external servers are directed through the proxy server.

If the HTTP/HTTPS proxy server is not reachable, Cisco SD-WAN Manager displays an error message on the GUI indicating the reason for failure.

Configure Implicit ACL on Loopback Interfaces

Table 134: Feature History

Feature Name	Release Information	Description
Implicit ACL on Loopback Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature lets you to enable implicit ACL on loopback TLOC interfaces so that ACL rules are applied to the traffic destined to it.

Similar to configuring physical WAN interfaces, you can configure implicit ACL on loopback interfaces using a feature template or using a CLI Add-on template in Cisco SD-WAN Manager.

For information about using a feature template to configure implicit ACL on loopback interfaces, see Configure VPN Ethernet Interface.

For information on using the CLI Add-On template, see Create a CLI Add-On Feature Template.

Configure Port Connectivity for Cloud OnRamp Colocation Cluster

Table 135: Feature History

Feature Name	Release Information	Description
Flexible Topologies	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1 Cisco NFVIS Release 4.2.1	You can configure the Stackwise Virtual Switch Link (SVL) and uplink ports of switches, and Cisco CSP data ports using the **Port Connectivity** configuration settings of Cloud OnRamp for Colocation cluster .
Support for SVL Port Configuration on 100G Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1 Cisco NFVIS Release 4.8.1	With this feature, you can configure SVL ports on 100-G Ethernet interfaces of Cisco Catalyst 9500-48Y4C switches, thus ensuring a high level of performance and throughput.

Prerequisites for Configuring SVL and Uplink Ports

- When configuring the SVL and uplink ports, ensure that the port numbers you configure on Cisco SD-WAN Manager match the physically cabled ports.
- Ensure that you assign serial numbers to both the switches. See Create and Activate Clusters.

Configure SVL and Uplink Ports

Note Before configuring the SVL and uplink ports using the **Cluster Topology** window, ensure that you create a Cloud OnRamp for Colocation cluster. See Create and Activate Clusters.

- On the **Cluster Topology** window, click **Add** next to **Port Connectivity**.

  In the **Port Connectivity** configuration window, both the configured switches appear. Hover over a switch port to view the port number and the port type.

Note For more information about SVL and uplink ports, see Wiring Requirements in the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide.

Change Default SVL and Uplink Ports

Before you change the default port number and port type, note the following information about Cisco Catalyst 9500-40X and Cisco Catalyst 9500-48Y4C switches:

- From Cisco vManage Release 20.8.1, you can configure two SVL ports and one Dual-Active Detection (DAD) port when creating a colocation cluster with two Cisco Catalyst 9500-40X switches or two Cisco Catalyst 9500-48Y4C switches.
- To ensure that SVL and DAD ports are configured correctly for Cisco Catalyst 9500-48Y4C switches, note the following information:
  - Configure the SVL ports on same-speed interfaces, that is, either 25-G interfaces or 100-G interfaces. Ensure that both switches have the same configuration.
  - Configure the DAD port only on 25-G interfaces on both switches.
  - In case of an existing cluster, you can change the SVL ports only if it is inactive.
  - A cluster created in releases earlier than Cisco vManage Release 20.8.1 automatically displays two SVL ports and one DAD port after the upgrade to Cisco vManage Release 20.8.1.
- In case of Cisco Catalyst 9500-40X switches, you must configure the SVL and DAD ports on 10-G interfaces on both switches.
- The following are the default SVL, DAD, and uplink ports of Cisco Catalyst 9500 switches:

  Cisco Catalyst 9500-40X
  - SVL ports: Te1/0/38-Te1/0/39, and Te2/0/38-Te2/0/39

    In Cisco vManage Release 20.7.1 and earlier releases, the default SVL ports are Te1/0/38-Te1/0/40 and Te2/0/38-Te2/0/40.
  - DAD ports: Te1/0/40 and Te2/0/40
  - Uplink ports: Te1/0/36, Te2/0/36 (input VLAN handoff), Te1/0/37, and Te2/0/37 (output VLAN handoff)

  Cisco Catalyst 9500-48Y4C
  - SVL ports: Hu1/0/49-Hu1/0/50 and Hu2/0/49-Hu2/0/50

    In Cisco vManage Release 20.7.1 and earlier releases, the default SVL ports are Twe1/0/46-Twe1/0/48 and Twe2/0/46-Twe2/0/48.
  - DAD ports: Twe1/0/48 and Twe2/0/48
  - Uplink ports: Twe1/0/44, Twe2/0/44 (input VLAN handoff), Twe1/0/45, and Twe2/0/45 (output VLAN handoff) for 25-G throughput.
- I, E, and S represent the ingress, egress, and SVL ports, respectively.

- Ensure that the physical cabling is the same as the default configuration, and click **Save**.

To change the default ports when the connectivity is different for SVL and uplink ports, perform the following:

1. If both the switches are using the same ports:
   a. Click a port on a switch that corresponds to a physically connected port.
   b. To add the port configuration to the other switch, check the **Apply change** check box.

   If both the switches aren't using the same ports:
   a. Click a port on **Switch1**.
   b. Choose a port type from the **Port Type** drop-down list.
   c. Click a port on **Switch2** and then choose the port type.
2. To add another port, repeat step 1.
3. Click **Save**.
4. To edit port connectivity information, in the **Cluster Topology** window, click **Edit** next to **Port Connectivity**.

Note You can modify the SVL and uplink ports of a cluster when the cluster hasn't been activated.

5. To reset the ports to default settings, click **Reset**.

The remaining ports (SR-IOV and OVS) on the Cisco CSP devices and the connections with switches are automatically discovered using Link Layer Discovery Protocol (LLDP) when you activate a cluster. You don't need to configure those ports.

Cisco Colo Manager discovers switch neighbor ports and identifies whether all Niantic and Fortville ports are connected. If any port isn't connected, CCM sends notifications to Cisco SD-WAN Manager that you can view in the task view window.

Configure Port-Scanning Detection Using a CLI Template

Table 136: Feature History

Feature Name	Release Information	Description
Configure Port-Scanning Detection Using a CLI Template	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can configure port-scanning detection and apply a severity level (low, medium, or high) using a CLI template.

Port scanning is a way of determining the open ports on a network, which receive and send data.

To configure port-scanning detection and include severity levels, use the following commands:

- **port-scan**

- **sense level**

Note The **port-scan** command can detect, but not block possible port-scan attacks.

For more information on using these commands, see the **port-scan** and **sense level** commands in the Cisco SD-WAN Command Reference Guide.

To detect port-scanning activity in your network, configure port-scanning detection on your device by copying and pasting in the configuration as a Cisco SD-WAN Manager CLI template. For more information on using CLI templates, see Create a CLI Add-On Feature Template in the Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x.

To generate port-scanning alerts, use Network Mapper (Nmap) commands. Nmap is an open-source tool for network scanning and discovery. For more information on Nmap command usage and installation, see https://nmap.org/book/man.html. Run the Nmap commands as an administrator:

1. After port-scanning detection is configured using a Cisco SD-WAN Manager CLI template, run the Linux Nmap commands from the device where port-scanning detection is configured.
2. After the Nmap commands are run, you can see the port-scanning alerts generated on the router by running the following Cisco IOS XE command:

```
Router# show utd engine standard logging events
```

3. To verify that the port-scanning configuration is applied on the router, use the following Cisco IOS XE **show** command:

```
Router# show utd engine standard config threat-inspection
```

```
Router# show utd engine standard config threat-inspection
UTD Engine Standard Configuration:

UTD threat-inspection profile table entries:
Threat profile: THREAT_INSP1
Mode: Intrusion Prevention
Policy: Security
Logging level: Infomational
Port Scan:
  Sense level: Medium
```

Configure Service-Side NAT Object Tracker

Table 137: Feature History

Feature Name	Release Information	Description
Service-Side NAT Object Tracker Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can use this feature to track LAN prefixes and LAN interfaces for service-side inside static NAT. You can configure the service-side NAT object tracker using Cisco SD-WAN Manager, a device CLI template, or a CLI add-on template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. To edit a **Cisco System** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **Tracker** and choose **New Object Tracker** to configure the service-side NAT object tracker parameters.

Table 138: Service-Side NAT Object Tracker Parameters

Field	Description
Tracker Type	Choose **Interface** or **Route** to configure object tracking for a LAN interface or a LAN prefix.
Object ID	Enter the object ID number. The object number identifies the tracked object and can be from 1 to 1000.
Interface	Choose a global or device-specific interface.

5. Click **Add**.
6. Click **Update**.
7. (Optional) To create a tracker group, choose **Tracker**, and click **Tracker Groups** > **New Object Tracker Groups** to configure the service-side NAT object tracker.

Note Ensure that you have created two trackers to create a tracker group.

Table 139: Service-Side NAT Object Tracker Group Parameters

Field	Description
Group Tracker ID	Enter the name of the tracker group.
Tracker ID	Enter the name of the object tracker that you want to group.
Criteria	Choose **AND** or **OR**. If you choose the **AND** operation, the transport interface status is reported as active if both the associated trackers of the tracker group report that the route is active. **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the route is active.

8. Click **Add**.

9. Click **Update**.

Configure Service-Side NAT Object Tracker Using a CLI Add-On Template

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Configure Service-Side NAT Object Tracker Using a CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Choose a device from the device list.
5. Click **CLI Add-On Template** under **OTHER TEMPLATES**.
6. In **CLI Add-On Template** area, enter the configuration as shown in the following example:

```
track 1 ip route 192.168.11.0 255.255.255.0 reachability
ip vrf 1
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
track 1
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload track 1
```

7. Click **Save**.

   The CLI add-on template that you created is displayed in the **CLI Configuration** table.
8. Attach the CLI add-on template to your device.

Configure Service-Side Static Network NAT

Table 140: Feature History

Feature Name	Release Information	Description
Service-Side Static Network NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can use this feature to configure a single static NAT pool for an entire subnet. You can configure service-side static network NAT using Cisco SD-WAN Manager or a device CLI template.

Before You Begin

- Configure and apply a data policy.

  For more information on creating and applying a centralized data policy for service-side NAT, see Create and Apply a Centralized Data Policy for Service-Side NAT.

- Configure a **Cisco VPN** template or edit an existing **Cisco VPN** template.
- Configure service-side static NAT.

Note You need to configure a NAT pool prior to configuring service-side static network NAT.

For more information on configuring service-side static NAT and a NAT pool, see Configure Service-Side Static NAT.

Configure Service-Side Static Network NAT

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Click **Static NAT**.
6. Under **Static NAT**, click **New Static NAT Subnet**.
7. Enter the required parameters.

Table 141: New Static NAT Subnet Parameters

Parameter Name	Description
Source IP Subnet	Enter the inside local address as the source IP subnet address.
Translated Source IP Subnet	Enter the outside global subnet address as the translated source IP subnet address. Maps a public IP address to a private source address.
Network Prefix Length	Enter the network prefix length.
Static NAT Direction	Select the direction for the network address translation. Choose **Inside** as the direction for performing network address translation.
Add Object /Group Tracker	(Optional) Enter the object ID number if you want to track an object. The object tracker functionality is supported for service-side static network NAT.

8. Click **Update**.

Configure SLA Class

Table 142: Feature History

Feature Name	Release Information	Description
Best of the Worst (BOW) Tunnel Selection	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure best tunnel path to pick the best path while configuring SLA class.

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Policies**. Centralized Policy is selected and displayed by default.
2. Click **Add Policy**.
3. In the create groups of interest page, from the left pane, click **SLA Class**, and then click **New SLA Class List**.
4. In the **SLA Class List Name** field, enter a name for SLA class list.
5. Define the SLA class parameters:
   a. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.
   b. In the **Latency** field, enter the maximum packet latency on the connection, a value from 1 through 1,000 milliseconds.
   c. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
   d. Choose the required app probe class from the **App Probe Class** drop-down list.
6. (Optional) Check the **Fallback Best Tunnel** check box to enable the best tunnel criteria.

   This optional field is available from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a to pick the best path or color from the available colors when a SLA is not met. When this option is selected, you can choose the required criteria from the drop-down. The criteria are a combination of one or more of loss, latency, and jitter values.
7. Select the **Criteria** from the drop-down. The available criteria are:
   - None
   - Latency
   - Loss
   - Jitter
   - Latency, Loss
   - Latency, Jitter
   - Loss, Latency

- Loss, Jitter
- Jitter, Latency
- Jitter, Loss
- Latency, Loss, Jitter
- Latency, Jitter, Loss
- Loss, Latency, Jitter
- Loss, Jitter, Latency
- Jitter, Latency, Loss
- Jitter, Loss, Latency

8. (Optional) Enter the **Loss Variance (%)**, **Latency Variance (ms)**, and the **Jitter Variance (ms)** for the selected criteria.

   For more information, see Configure Variance for Best Tunnel Path.

9. Click **Add**.

Configure SNMPv3 on Cisco IOS XE Catalyst SD-WAN Devices Using Cisco SD-WAN Manager

Table 143: Feature History

Feature Name	Release Information	Description
Support for SNMPv3 AES-128 and AES-256 bit Encryption Protocol	Cisco vManage Release 20.7.1 Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	You can now configure SNMPv3 users with SHA-1 protocol and AES-128 and AES-256 encryption on Cisco IOS XE Catalyst SD-WAN devices.

To configure SNMPv3, in **SNMP Version**, navigate to **Template** page and configure groups and trap information:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose the type of device for which you are creating the template.

5. Click **Additional Templates**. This takes you to the **Additional Templates** section.
6. From the **Cisco SNMP** drop-down list, choose **Create Template**.

   The SNMP template form containing fields for naming the template and for defining SNMP parameters is displayed.
7. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
9. In **SNMP Version** section, click **V3**. For SNMPv3, you can configure groups and trap information.
10. In the **View & Groups** section, click **View**, choose **New View**, and configure the following fields:

Table 144: View and Groups Parameters for Cisco IOS XE Catalyst SD-WAN Devices

Field Name	Description
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 255 characters. You must add a view name for all the views before adding a group.
Object Identifiers (OID)	Click **Add Object Identifiers** and configure the following parameters: • Object Identifier: Enter the OID of the object. For example, to view the internet part of the SNMP MIB, enter the OID 1.3.6.1. To view the private part of the Cisco Catalyst SD-WAN MIB, enter the OID 1.3.6.1.4.1.9. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. • Exclude OID: Click **Off** to include the OID in the view or click **On** to exclude the OID from the view. To remove an OID from the list, click **Delete** adjacent to the corresponding entry. To add an OID to the view list, click **Add**.

11. Click **Add**.

Click **Group**, choose **New Group**, and configure the following parameters.

Note It's mandatory to create an SNMP view before you proceed with SNMP group configuration.

Table 145: Group Parameters

Field Name	Description
Name	Enter the name for the group. The name can be from 1 through 32 characters and can include angle brackets (< >).

Field Name	Description
Security Level	Choose the security level from the drop-down for the SNMPv3 security model: SNMPv3 is a security model in which an authentication strategy for a user and the group in which the user resides are set up. A security level is the permitted level of security within a security model. • noAuthNoPriv: Uses a username match for authentication. • authNoPriv: Provides authentication based on the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) algorithms. • authPriv: Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.
View	Choose the view from the drop-down list to apply to the group. The view specifies the portion of the MIB tree that the group can access.

To add the SNMP group, click **Add**.

To configure SNMPv3 users, in the **User** section, click **New User**, and provide information in the following fields. Note that it's mandatory to create an SNMP group before you proceed with SNMP user configuration.

Table 146: SNMPv3 Users Parameters

Field Name	Description
User	Enter a unique name for the user. It can be 1 to 32 alphanumeric characters.
Authentication Protocol	Choose the authentication mechanism for the user: • SHA-1 message digest. • MD5 digest. **Note** Support for MD5 authentication protocol will be deprecated shortly.
Authentication Password	If you have the localized MD5 or SHA digest, you can specify the respective string as password. The digest is in the format *aa:bb:cc:dd* where *aa*, *bb*, *cc*, and *dd* are hexadecimal values. Also, the digest should be exactly 16 octets in length.
Privacy Protocol	Choose the privacy type for the SHA-1 authentication protocol user: AES-CFB-128: Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 128-bit key. AES-256-CFB-128: Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 256-bit key.
Privacy Password	Enter the privacy password either in cleartext or as an AES-encrypted key.
Group	Choose the group name from the drop-down list. Configured SNMPv3 group names are displayed in the drop-down list.

Note Starting from Cisco IOS XE Release 17.11.1a, SNMP v3 users with SHA-256 and AES-256 authentication must use 1161 as special port.

To add an SNMP user, click **Add**.

(Optional) To configure the Trap Target server, in the **Trap** section, click **New Trap Target**, and enter information in the following fields. Note that it's mandatory to create an SNMP user before you proceed with trap target server configuration.

Table 147: Trap Target Serve Parameters

Field Name	Description
VPN ID	Enter the number of the VPN to use to reach the trap server. Range: 0 to 65530.
IP Address	Enter the IP address of the SNMP server.
UDP Port	Enter the UDP port number for connecting to the SNMP server. Range: 1 to 65535.
User Name	Choose the name of the configured user from the drop-down list.
Source Interface	Enter the interface used to send traps to the remote SNMP server.

To add the Trap Target server, click **Add**.

To save the feature template, click **Save**.

Note The SNMP walk application is blocked if you switch the SNMPv3 configuration to SNMPv2 configuration in the device template and apply this change through a template push. This is because the **snmp mib community-map** command for SNMPv3 isn't removed during the configuration change. Hence, you can't switch from SNMPv3 to SNMPv2 directly, when the SNMPv3 configuration template is active. To switch to SNMPv2, you must first remove the SNMPv3 configuration from the device and then push the SNMPv2 template through a separate commit.

Configure Traffic Flow Monitoring on Cisco IOS XE Catalyst SD-WAN Devices

Cflowd traffic flow monitoring uses Flexible NetFlow (FNF) to export traffic data. Perform the following steps to configure Cflowd monitoring:

Table 148: Feature History

Feature Name	Release Information	Description
Flexible NetFlow Support for IPv6 and Cache Size Modification	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	Configure Cflowd traffic flow monitoring on Cisco IOS XE Catalyst SD-WAN devices.
Log Packets Dropped by Implicit ACL	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	To enable logging of dropped packets, check the **Implicit ACL Logging** check box and to configure how often the packet flows are logged, enter the value in the **Log Frequency** field.
Flexible NetFlow Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Configure Cflowd traffic flow monitoring to collect ToS, sampler ID, and remarked DSCP values in netflow records.
Flexible NetFlow for VPN0 Interface	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Configure this feature using the CLI template and also add-on CLI template.
Flexible NetFlow Export Spreading	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco Catalyst SD-WAN Control Components Release 20.9.x Cisco vManage Release 20.9.1	This feature enables export spreading to prevent export storms that occur when a burst of packets are sent to external collector. The export of the previous interval is spread during the current interval to prevent export storms. When NetFlow packets are sent over a low-bandwidth circuit, the export spreading functionality is enabled to avoid packet drops.
Flexible NetFlow Export of BFD Metrics	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	With this feature, you can export Bidirectional Forwarding Detection (BFD) metrics to an external collector for generating BFD metrics of loss, latency, and jitter. This feature provides enhanced monitoring and faster collection of network state data.
Real-Time Device Options for Monitoring Cflowd and SAIE Flows	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	With this feature, you can apply filters for monitoring specific Cflowd and SD-WAN Application Intelligence Engine (SAIE) applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. This feature was already available on Cisco vEdge devices and is being extended to Cisco IOS XE Catalyst SD-WAN devices in this release.

Configure Global Flow Visibility

Enable Cflowd visibility globally on all Cisco IOS XE Catalyst SD-WAN devices so that you can perform traffic flowing monitoring on traffic coming to the router from all VPNs in the LAN.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. Click **Next** to advance through the wizard pages until you reach **Policy Overview** and then the **Policy Settings** page.
5. Enter **Policy Name** and **Policy Description**.
6. Check the **Netflow** check box to enable flow visibility for IPv4 traffic.
7. Check the **Netflow IPv6** check box to enable flow visibility for IPv6 traffic.

Note Enable flow visibility for IPv4 and IPv6 traffic before configuring Cflowd traffic flows with SAIE visibility.

For more information on monitoring Cflowd and SAIE flows, see the Devices and Controllers chapter of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

8. Check **Implicit ACL Logging** to configure your Cisco IOS XE Catalyst SD-WAN device to log dropped packets in the traffic.

   With this configuration, you have visibility of the packets dropped by implicit access control lists (ACL) in case of a link failure in the system.

9. Enter **Log Frequency**.

   Log frequency determines how often packet flows are logged. Maximum value is 2147483647. It is rounded down to the nearest power of 2. For example, for 1000, the logging frequency is 512. Thus, every 512th packet in the flow is logged.

10. Enter **FNF IPv4 Max Cache Entries** to configure FNF cache size for IPv4 traffic.

    For example, enter 100 to configure FNF cache for IPv4/IPv6 traffic as shown in the following example.

11. Enter **FNF IPv6 Max Cache Entries** to configure FNF cache size for IPv6 traffic.

    For example, enter 100 to configure FNF cache for IPv4/IPv6 traffic as shown in the following example.

Note The minimum cache size value is 16. The maximum of total cache size (IPv4 cache + IPv6 cache) should not exceed the limit for each platform. If cache size is not defined and the platform is not in the list, then default maximum cache entries is 200k.

The maximum cache entries is the maximum concurrent flows that Cflowd can monitor. The maximum cache entries vary on different platforms. For more information, contact Cisco Support.

The following example shows the flow-visibility configuration for both IPv4 and IPv6:

```
policy
    flow-visibility
    implicit-acl-logging
    log-frequency 1000
    flow-visibility-ipv6
    ip visibility cache entries 100
    ipv6 visibility cache entries 100
```

While running `policy flow-visibility` or `app-visibility` to enable the FNF monitor, you may see the following warning message displaying a GLOBAL memory allocation failure. This log is triggered by enabling FNF monitoring (`policy flow-visibility` or `app-visibility`) with a large cache size.

```
Jul  4 01:45:00.255: %CPPEXMEM-3-NOMEM: F0/0: cpp_cp_svr: QFP: 0, GLOBAL memory allocation
 of 90120448 bytes by FNF failed
Jul  4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: CPR STILE
EXMEM GRAPH, Allocations: 877, Type: GLOBAL
Jul  4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: SBC, Bytes
Allocated: 53850112, Type: GLOBAL
```

The warning message does not necessarily indicate a flow monitor application failure. The warning message can indicate internal steps that FNF uses for applying memory from the External Memory Manager (EXMEM) infrastructure.

Use the **show platform hardware qfp active classification feature-manager exmem-usage** command to display the EXMEM memory usage for various clients.

```
Device# show platform hardware qfp active active classification feature-manager exmem-usage

EXMEM Usage Information

Total exmem used by CACE: 39668

Client       Id   Total VMR     Total Usage   Total%   Alloc     Free
-------------------------------------------------------------------------
acl          0      11           2456          6         88       84
qos          2     205          31512         79          7        5
fw           4       8            892          2          2        1
obj-group   39      82           4808         12          5        2
```

To ensure that the FNF monitor is enabled successfully, use the **show flow monitor** *monitor-name* command to check the status (`allocated` or `not allocated`) of a flow monitor.

```
Device# show flow monitor sdwan_flow_monitor
Flow Monitor sdwan_flow_monitor:
  Description:       monitor flows for vManage and external collectors
  Flow Record:       sdwan_flow_record-003
  Flow Exporter:     sdwan_flow_exporter_1
                     sdwan_flow_exporter_0
  Cache:
    Type:                normal (Platform cache)
    Status:              allocated
    Size:                250000 entries
    Inactive Timeout:    10 secs
    Active Timeout:      60 secs

    Trans end aging:   off

SUCCESS
   Status:            allocated
FAILURE
   Status:            not allocated
```

Configure Global Application Visibility

Enable Cflowd visibility globally on all Cisco IOS XE Catalyst SD-WAN devices so that you can perform traffic flowing monitoring on traffic coming to the router from all VPNs in the LAN.

The `app-visibility` enables `nbar` to see each application of the flows coming to the router from all VPNs in the LAN. If `app-visibility` or `app-visibility-ipv6` is defined, then `nbar` is enabled globally for both IPv4 and IPv6 flows.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. Click **Next** to advance through the wizard pages until you reach **Policy Overview** and then the **Policy Settings** page.
5. Enter **Policy Name** and **Policy Description**.
6. Check the **Application** check box to enable application visibility for IPv4 traffic.
7. Check the **Application IPv6** check box to enable application visibility for IPv6 traffic.

Note Enable application visibility for IPv4 and IPv6 traffic before configuring Cflowd traffic flows with SAIE visibility.

For more information on monitoring Cflowd and SAIE flows, see the Devices and Controllers chapter of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

8. Enter **FNF IPv4 Max Cache Entries** to configure FNF cache size for IPv4 traffic.

   For example, enter 100 to configure FNF cache size for IPv4 traffic as shown in the following example.
9. Enter **FNF IPv6 Max Cache Entries** to configure FNF cache size for IPv6 traffic.

   For example, enter 100 to configure FNF cache size for IPv6 traffic as shown in the following example.

The following example shows the application visibility configuration for both IPv4 and IPv6:

```
policy
 app-visibility


 app-visibility-ipv6
 ip visibility cache entries 100
 ipv6 visibility cache entries 100
!
```

Note The **policy app-visibility** command also enables global flow visibility by enabling **nbar** to get the application name.

Note If you configure Cflowd global `flow-visibility`, but you do not configure Cflowd `app-visibility`, the exported application to Cisco SD-WAN Manager returns a result of unknown. The same application exported to an external collector using the IPFIX analyzer may contain an incorrect application name.

If you want to retain the application name, define Cflowd `app-visibility` to avoid this issue.

Configure Cflowd Monitoring Policy

Table 149: Feature History

Feature Name	Release Information	Description
Flexible NetFlow Support for IPv6 and Cache Size Modification	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	Configure Cflowd traffic flow monitoring on Cisco IOS XE Catalyst SD-WAN devices.
Log Packets Dropped by Implicit ACL	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	To enable logging of dropped packets, check the **Implicit ACL Logging** check box and to configure how often the packet flows are logged, enter the value in the **Log Frequency** field.
Flexible NetFlow Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Configure Cflowd traffic flow monitoring to collect ToS, sampler ID, and remarked DSCP values in netflow records.
Flexible NetFlow for VPN0 Interface	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Configure this feature using the CLI template and also add-on CLI template.
Flexible NetFlow Export Spreading	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco Catalyst SD-WAN Control Components Release 20.9.x Cisco vManage Release 20.9.1	This feature enables export spreading to prevent export storms that occur when a burst of packets are sent to external collector. The export of the previous interval is spread during the current interval to prevent export storms. When NetFlow packets are sent over a low-bandwidth circuit, the export spreading functionality is enabled to avoid packet drops.
Flexible NetFlow Export of BFD Metrics	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	With this feature, you can export Bidirectional Forwarding Detection (BFD) metrics to an external collector for generating BFD metrics of loss, latency, and jitter. This feature provides enhanced monitoring and faster collection of network state data.

Feature Name	Release Information	Description
Real-Time Device Options for Monitoring Cflowd and SAIE Flows	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	With this feature, you can apply filters for monitoring specific Cflowd and SD-WAN Application Intelligence Engine (SAIE) applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. This feature was already available on Cisco vEdge devices and is being extended to Cisco IOS XE Catalyst SD-WAN devices in this release.

To configure a policy for Cflowd traffic flow monitoring, use the Cisco SD-WAN Manager policy configuration wizard. The wizard consists of four sequential pages that guide you through the process of creating and editing policy components:

1. **Create Applications or Groups of Interest**: Create lists that group related items together and that you call in the match or action components of a policy.
2. **Configure Topology**: Create the network structure to which the policy applies.
3. **Configure Traffic Rules**: Create the match and action conditions of a policy.
4. **Apply Policies to Sites and VPNs**: Associate a policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard pages, create policy components or blocks. In the last page, apply policy blocks to sites and VPNs in the overlay network. For the Cflowd policy to take effect, activate the policy.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options**.
3. Under **Centralized Policy**, click **Traffic Policy**.
4. Click **Cflowd**.
5. Click **Add Policy** and then click **Create New**.
6. Enter the **Name** and **Description** for the policy.
7. In the **Cflowd Template** section, enter **Active Flow Timeout**.
8. In the **Inactive Flow Timeout** field, enter the timeout range.
9. In the **Flow Refresh** field, enter the range.
10. In the **Sampling Interval** field, enter the sample duration.
11. In the **Protocol** drop-down list, choose an option from the drop-down list.

    Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the **Advanced Settings** field displays when you choose **IPv4** or **Both** from the options.
12. Under the **Advanced Settings**, do the following to collect additional IPv4 flow records:
    - Check the **TOS** check box.
    - Check the **Re-marked DSCP** check box.

13. Under the **Collector List**, click **New Collector**. You can configure up to four collectors.
    a. In the **VPN ID** field, enter the number of the VPN in which the collector is located.
    b. In the **IP Address** field, enter the IP address of the collector.
    c. In the **Port** field, enter the collector port number.
    d. In the **Transport Protocol** drop-down list, choose the transport type to use to reach the collector.
    e. In the **Source Interface** field, enter the name of the interface to use to send flows to the collector.
    f. In the **Export Spreading** field, click the **Enable** or **Disable** radio button.

       Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, the **Export Spreading** field is available to prevent export storms that occur due to the creation of a synchronized cache. The export of the previous interval is spread during the current interval to prevent export storms.
    g. In the **BFD Metrics Exporting** field, click the **Enable** or **Disable** radio button.

       Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **BFD Metrics Exporting** field is available for collecting BFD metrics of loss, jitter, and latency.
    h. In the **Exporting Interval** field, enter the interval in seconds for sending BFD metrics.

       Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **Exporting Interval** field is available for specifying the export interval for BFD metrics.

       Once you enable BFD metrics exporting, you can see the **Exporting Interval** field.

       The **Exporting Interval** field controls the intervals by which BFD metrics are sent.

       The default BFD export interval is 600 seconds.

Field	Description
Cflowd Policy Name	Enter a name for the Cflowd policy.
Description	Enter a description for the Cflowd policy.
Active Flow Timeout	Enter an active flow timeout value. The range is 30 to 3600 seconds.
Inactive Flow Timeout	Enter an inactive flow timeout value. The range is 1 to 3600 seconds.
Flow Refresh	Enter the interval for sending Cflowd records to an extremal collector. The range is 60 through 86400 seconds.
Sampling Interval	Enter the sample duration. The range is 1 through 65536 seconds.
Protocol	Choose the traffic protocol type from the drop-down list. The options are: **IPv4**, **IPv6**, or **Both**. The default protocol is **IPv4**.
TOS	Check the **TOS** check box. This indicates the type of field in the IPv4 header.

Field	Description
Re-marked DSCP	Check the **Re-marked DSCP** check box. This indicates the traffic output specified by the remarked data policy.
VPN ID	Enter the VPN ID. The range is 0 through 65536.
IP Address	Enter the IP address of the collector.
Port	Enter the port number of the collector. The range is from 1024 through 65535.
Transport Protocol	Choose the transport type from the drop-down list to reach the collector. The options are: **TCP** or **UDP**.
Source Interface	Choose the source interface from the drop-down list.
Export Spreading	Click the **Enable** or **Disable** radio button to configure export spreading. The default is **Disable**.
BFD Metrics Exporting	Click the **Enable** or **Disable** radio button to configure export of Bidirectional Forwarding Detection (BFD) metrics. The default is **Disable**.
Exporting Interval	Enter the export interval in seconds for sending the BFD metrics to an external collector. Enter an integer value. This field is displayed only if you enable BFD metrics export. The default BFD export interval is 600 seconds.

14. Click **Save Cflowd Policy**.

Configure Flexible Netflow on VPN0 Interface

You can enable FNF on a VPN0 interface using a CLI template or the CLI add-on template. The ezPM profile helps in creating a new profile to carry all the Netflow VPN0 monitor configuration. On selecting a profile and specifying a few parameters, ezPM provides the remaining provisioning information. A profile is a pre-defined set of traffic monitors that can be enabled or disabled for a context. You can configure Easy Performance Monitor (ezPM) and enable FNF as follows.

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile <sdwan-fnf> traffic-monitor
 <all> [ipv4/ipv6]
Device(config-perf-mon)# exporter destination <destination address> source <source interface>
 transport udp vrf <vrf-name> port <port-number> dscp <dscp>
```

The following example shows how to configure a performance monitor context using the sdwan-fnf profile. This configuration enables monitoring of traffic metrics. Here, 10.1.1.1 is the IP address of the third-party collector, GigabitEthernet5 is the source interface, and 4739 is the listening port of the third-party collector.

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile sdwan-fnf traffic-monitor
 all [ipv4/ipv6]
Device(config-perf-mon)# exporter destination <10.1.1.1> source <GigabitEthernet5> transport
 udp vrf <vrf1> port <4739> dscp <1>
```

Configure Traffic Rules

Table 150: Feature History

Feature Name	Release Information	Description
Policy Matching with ICMP Message	Cisco IOS XE Release 17.4.1 Cisco vManage Release 20.4.1	You can now define a new match condition that can be used to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.

When you first open the **Configure Traffic Rules** window, **Application-Aware Routing** is selected by default.

You can also view already created AAR routing policies listed in the page. It provides various information related to the policies such as the Name of the policy, Type, Mode, Description, Update By, and Last Updated details.

Note You can refer to the Mode column for the security status details of the policy. The status helps to differentiate whether the policy is used in unified security or not. The mode status is applicable only for security policies and not relevant to any centralized or localized policies.

For more information on configuring traffic rules for the Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) flow, see Cisco Catalyst SD-WAN Application Intelligence Engine Flow.

Note In Cisco vManage Release 20.7.1 and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

To configure traffic rules for a centralized data policy:

1. Click **Traffic Data**.
2. Click the **Add Policy** drop-down.
3. Click **Create New**. The **Add Data Policy** window displays.
4. Enter a name and a description for the data policy.
5. In the right pane, click **Sequence Type**. The **Add Data Policy** popup opens.
6. Select the type of data policy you want to create, **Application Firewall**, **QoS**, **Traffic Engineering**, or **Custom**.

Note If you want to configure multiple types of data policies for the same match condition, you need to configure a custom policy.

7. A policy sequence containing the text string **Application**, **Firewall**, **QoS**, **Traffic Engineering**, or **Custom** is added in the left pane.
8. Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.
9. In the right pane, click **Sequence Rule**. The **Match/Action** box opens, and **Match** is selected by default. The available policy match conditions are listed below the box.

Match Condition	Procedure
None (match all packets)	Do not specify any match conditions.
Applications /Application Family List	**a.** In the **Match** conditions, click **Applications/Application Family List**. **b.** In the drop-down, select the application family. **c.** To create an application list: **1.** Click **New Application List**. **2.** Enter a name for the list. **3.** Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications. **4.** In the **Select Application** drop-down, select the desired applications or application families. **5.** Click **Save**. This match condition is available for IPv6 traffic from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1.
Destination Data Prefix	**a.** In the **Match** conditions, click **Destination Data Prefix**. **b.** To match a list of destination prefixes, select the list from the drop-down. **c.** To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field.
Destination Port	**a.** In the **Match** conditions, click **Destination Port**. **b.** In the **Destination Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Match Condition	Procedure
DNS Application List	Add an application list to enable split DNS. **a.** In the **Match** conditions, click **DNS Application List**. **b.** In the drop-down, select the application family. This match condition is available for IPv6 traffic from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1.
DNS	Add an application list to process split DNS. **a.** In the **Match** conditions, click **DNS**. **b.** In the drop-down, select **Request** to process DNS requests for the DNS applications, and select **Response** to process DNS responses for the applications.
DSCP	**a.** In the **Match** conditions, click **DSCP**. **b.** In the **DSCP** field, type the DSCP value, a number from 0 through 63.
Packet Length	**a.** In the **Match** conditions, click **Packet Length**. **b.** In the **Packet Length** field, type the length, a value from 0 through 65535.
PLP	**a.** In the **Match** conditions, click **PLP** to set the **Packet Loss Priority**. **b.** In the **PLP** drop-down, select **Low** or **High**. To set the PLP to **High**, apply a policer that includes the **exceed remark** option.
Protocol	**a.** In the **Match** conditions, click **Protocol**. **b.** In the **Protocol** field, type the Internet Protocol number, a number from 0 through 255.
ICMP Message	To match ICMP messages, in the Protocol field, set the Internet Protocol Number to 1, or 58, or both. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.
Source Data Prefix	**a.** In the **Match** conditions, click **Source Data Prefix**. **b.** To match a list of source prefixes, select the list from the drop-down. **c.** To match an individual source prefix, enter the prefix in the **Source** field.
Source Port	**a.** In the **Match** conditions, click **Source Port**. **b.** In the **Source** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Match Condition	Procedure
TCP	**a.** In the **Match** conditions, click **TCP**. **b.** In the **TCP** field, **syn** is the only option available.

10. For QoS and Traffic Engineering data policies: From the **Protocol** drop-down list, select **IPv4** to apply the policy only to IPv4 address families, **IPv6** to apply the policy only to IPv6 address families, or **Both** to apply the policy to IPv4 and IPv6 address families.
11. To select one or more **Match** conditions, click its box and set the values as described.

Note Not all match conditions are available for all policy sequence types.

12. To select actions to take on matching data traffic, click the **Actions** box.
13. To drop matching traffic, click **Drop**. The available policy actions are listed in the right side.
14. To accept matching traffic, click **Accept**. The available policy actions are listed in the right side.
15. Set the policy action as described.

Note Not all actions are available for all match conditions.

Action Condition	Description	Procedure
Counter	Count matching data packets.	**a.** In the **Action** conditions, click **Counter**. **b.** In the **Counter Name** field, enter the name of the file in which to store packet counters.
DSCP	Assign a DSCP value to matching data packets.	**a.** In the **Action** conditions, click **DSCP**. **b.** In the **DSCP** field, type the DSCP value, a number from 0 through 63.
Forwarding Class	Assign a forwarding class to matching data packets.	**a.** In the **Match** conditions, click **Forwarding Class**. **b.** In the **Forwarding Class** field, type the class value, which can be up to 32 characters long.

Action Condition	Description	Procedure
Log	Minimum release: Cisco vManage Release 20.11.1 and Cisco IOS XE Release 17.11.1a Click **Log** to enable logging. When (DP, AAR or ACL) data policy packets are configured with log action, logs generated and logged to syslog. Due to the global **log-rate-limit**, not all logs are logged. A syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.	**a.** In the **Action** conditions, click **Log** to enable logging.
Policer	Apply a policer to matching data packets.	**a.** In the **Match** conditions, click **Policer**. **b.** In the **Policer** drop-down field, select the name of a policer.
Loss Correction	Apply loss correction to matching data packets. Forward Error Correction (FEC) recovers lost packets on a link by sending redundant data, enabling the receiver to correct errors without the need to request retransmission of data. FEC is supported only for IPSEC tunnels, it is not supported for GRE tunnels. • **FEC Adaptive** – Corresponding packets are subjected to FEC only if the tunnels that they go through have been deemed unreliable based on measured loss. If you choose **FEC Adaptive**, an additional field, **Loss Threshold**, displays that allows you to specify the packet loss threshold for automatically enabling FEC. Adaptive FEC starts to work at 2% packet loss; this value is configurable. You can specify a loss threshold of 1 to 5%. The default packet loss threshold is 2%. • **FEC Always** – Corresponding packets are always subjected to FEC. • **Packet Duplication** – Sends duplicate packets over a single tunnel. If more than one tunnel is available, duplicated packets will be sent over the tunnel with the best parameters.	**a.** In the **Match** conditions, click **Loss Correction**. **b.** In the **Loss Correction** field, select **FEC Adaptive**, **FEC Always**, or **Packet Duplication**.
Click **Save Match and Actions**.		

16. Create additional sequence rules as desired. Drag and drop to re-arrange them.
17. Click **Save Data Policy**.
18. Click **Next** to move to **Apply Policies to Sites and VPNs** in the wizard.

Match Parameters - Data Policy

A centralized data policy can match IP prefixes and fields in the IP headers, as well as applications. You can also enable split DNS.

Each sequence in a policy can contain one or more match conditions.

Table 151:

Match Condition	Description
Omit	Match all packets.
Applications/Application Family List	Applications or application families. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.
Destination Data Prefix	Group of destination prefixes, IP prefix and prefix length. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
Destination Region	Choose one of the following: • **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using a multi-hop path, through the core region. • **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions. • **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination. **Note** Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
DNS Application List	Enables split DNS, to resolve and process DNS requests and responses on an application-by-application basis. Name of an **app-list** list . This list specifies the applications whose DNS requests are processed. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.
DNS	Specify the direction in which to process DNS packets. To process DNS requests sent by the applications (for outbound DNS queries), specify **dns request**. To process DNS responses returned from DNS servers to the applications, specify **dns response**.
DSCP	Specifies the DSCP value.
Packet length	Specifies the packet length. The range is 0 through 65535; specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
Packet Loss Priority (PLP)	Specifies the packet loss priority. By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.

Match Condition	Description
Protocol	Specifies Internet protocol number. The range is 0 through 255.
ICMP Message	For Protocol IPv4 when you enter a Protocol value as 1, the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. Likewise, the **ICMP Message** field displays for Protocol IPv6 when you enter a Protocol value as 58. When you select Protocol as Both, the **ICMP Message or ICMPv6 Message** field displays. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.
Source Data Prefix	Specifies the group of source prefixes or an individual source prefix.
Source Port	Specifies the source port number. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
TCP Flag	Specifies the TCP flag, syn.
Traffic To	In a Multi-Region Fabric architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN. **Note** Minimum release: Cisco vManage Release 20.8.1

Table 152: ICMP Message Types/Codes and Corresponding Enumeration Values

Type	Code	Enumeration
0	0	echo-reply

3		unreachable
	0	net-unreachable
	1	host-unreachable
	2	protocol-unreachable
	3	port-unreachable
	4	packet-too-big
	5	source-route-failed
	6	network-unknown
	7	host-unknown
	8	host-isolated
	9	dod-net-prohibited
	10	dod-host-prohibited
	11	net-tos-unreachable
	12	host-tos-unreachable
	13	administratively-prohibited
	14	host-precedence-unreachable
	15	precedence-unreachable
5		redirect
	0	net-redirect
	1	host-redirect
	2	net-tos-redirect
	3	host-tos-redirect
8	0	echo
9	0	router-advertisement
10	0	router-solicitation
11		time-exceeded
	0	ttl-exceeded
	1	reassembly-timeout
12		parameter-problem
	0	general-parameter-problem
	1	option-missing
	2	no-room-for-option
13	0	timestamp-request

14	0	timestamp-reply
40	0	photuris
42	0	extended-echo
43		extended-echo-reply
	0	echo-reply-no-error
	1	malformed-query
	2	interface-error
	3	table-entry-error
	4	multiple-interface-match

Table 153: ICMPv6 Message Types/Codes and Corresponding Enumeration Values

Type	Code	Enumeration
1		unreachable
	0	no-route
	1	no-admin
	2	beyond-scope
	3	destination-unreachable
	4	port-unreachable
	5	source-policy
	6	reject-route
	7	source-route-header
2	0	packet-too-big
3		time-exceeded
	0	hop-limit
	1	reassembly-timeout
4		parameter-problem
	0	Header
	1	next-header
	2	parameter-option
128	0	echo-request
129	0	echo-reply
130	0	mld-query
131	0	mld-report

132	0	mld-reduction
133	0	router-solicitation
134	0	router-advertisement
135	0	nd-ns
136	0	nd-na
137	0	redirect
138		router-renumbering
	0	renum-command
	1	renum-result
	255	renum-seq-number
139		ni-query
	0	ni-query-v6-address
	1	ni-query-name
	2	ni-query-v4-address
140		ni-response
	0	ni-response-success
	1	ni-response-refuse
	2	ni-response-qtype-unknown
141	0	ind-solicitation
142	0	ind-advertisement
143		mldv2-report
144	0	dhaad-request
145	0	dhaad-reply
146	0	mpd-solicitation
147	0	mpd-advertisement
148	0	cp-solicitation
149	0	cp-advertisement
151	0	mr-advertisement
152	0	mr-solicitation
153	0	mr-termination
155	0	rpl-control

Match Parameters

Access List Parameters

Access lists can match IP prefixes and fields in the IP headers.

In the CLI, you configure the match parameters with the **policy access-list sequence match** command.

Each sequence in an access-list must contain one match condition.

Match class in ACL is not supported. You can use rewrite policy to configure DSCP values.

For access lists, you can match these parameters:

Match Condition	Description
Class	Name of a class defined with a **policy class-map** command.
Destination Data Prefix	Name of a data-prefix-list list.
Destination Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
DSCP	Specifies the DSCP value. The range is 0 through 63.
Protocol	Specifies the internet protocol number. The range is 0 through 255.
ICMP Message	When you select a Protocol value as 1 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. When you select a Next Header value as 58 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1. For **`icmp-msg`** and **`icmp6-msg`** message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table in the Centralized chapter.
Packet Length	Specifies the length of the packet. The range can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
Source Data Prefix	Specifies the name of a **data-prefix-list** list.
PLP	Specifies the Packet Loss Priority (PLP) (**high** | **low**). By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Source Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
TCP	**syn**

Route Policy Parameters

For route policies, you can match these parameters:

Match Condition	Description
Address	Specifies the name of a **Prefix-List** list.
AS Path List	Specifies one or more BGP AS path lists. You can write each AS as a single number or as a regular expression. To specify more than one AS number in a single path, include the list in quotation marks (" "). To configure multiple AS numbers in a single list, include multiple **AS Path** options, specifying one AS path in each option.
Community List	List of one of more BGP communities. In **Community List**, you can specify: • *aa*:*nn*: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.
Extended Community List	Specifies the list of one or more BGP extended communities. In **community**, you can specify: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.
BGP Local Preference	Specifies the BGP local preference number. The range is 0 through 4294967295.
Metric	Specifies the route metric value. The range is 0 through 4294967295.
Next Hop	Specifies the name of an IP prefix list.
OMP Tag	Specifies the OMP tag number. The range is 0 through 4294967295.
Origin	Specifies the BGP origin code. The optionss are: EGP (default), IGP, Incomplete.
OSPF Tag	Specifies the OSPF tag number. The range is 0 through 4294967295.
Peer	Specifies the peer IP address.

Structural Components of Policy Configuration for Application-Aware Routing

Here are the structural components required to configure application-aware routing policy. Each one is explained in more detail in the sections below.

```
policy
  lists
    app-list list-name
      (app application-name | app-family application-family)
    prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    vpn-list list-name
      vpn-id vpn-id
 log-frequency number
 sla-class sla-class-name
   jitter milliseconds
   latency milliseconds
   loss percentage
 app-route-policy policy-name
   vpn-list list-name
     sequence number
       match
         match-parameters
       action
         backup-sla-preferred-color colors
         count counter-name
         log
         sla-class sla-class-name [strict] [preferred-color colors]
     default-action
       sla-class sla-class-name
apply-policy site-list list-name
  app-route-policy policy-name
```

Lists

Application-aware routing policy uses the following types of lists to group related items. You configure these lists under the **policy lists** command hierarchy on Cisco Catalyst SD-WAN Controllers.

Table 154:

List Type	Description	Command
Applications and application families	List of one or more applications or application families running on the subnets connected to the Cisco IOS XE Catalyst SD-WANdevice. Each **app-list** can contain either applications or application families, but you cannot mix the two. To configure multiple applications or application families in a single list, include multiple **app** or **app-family** options, specifying one application or application family in each **app** or **app-family** option. • *application-name* is the name of an application. The Cisco IOS XE Catalyst SD-WAN device supports about 2300 different applications. • *application-family* is the name of an application family. It can one of the following: **antivirus**, **application-service**, **audio_video**, **authentication**, **behavioral**, **compression**, **database**, **encrypted**, **erp**, **file-server**, **file-transfer**, **forum**, **game**, **instant-messaging**, **mail**, **microsoft-office**, **middleware**, **network-management**, **network-service**, **peer-to-peer**, **printer**, **routing**, **security-service**, **standard**, **telephony**, **terminal**, **thin-client**, **tunneling**, **wap**, **web**, and **webmail**.	**app-list** *list-name* (**app** *application-name* | **app-family** *application-family*)
Data prefixes	List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.	**data-prefix-list** *list-name* **ip-prefix** *prefix/length*

List Type	Description	Command
Sites	List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple **site-id** options, specifying one site number in each option. You can specify a single site identifier (such as **site-id 1**) or a range of site identifiers (such as **site-id 1-10**).	**site-list** *list-name* **site-id** *site-id*
VPNs	List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. You can specify a single VPN identifier (such as **vpn-id 1**) or a range of VPN identifiers (such as **vpn-id 1-10**).	**vpn-list** *list-name* **vpn** *vpn-id*

In the Cisco Catalyst SD-WAN Controller configuration, you can create multiple iterations of each type of list. For example, it is common to create multiple site lists and multiple VPN lists so that you can apply data policy to different sites and different customer VPNs across the network.

When you create multiple iterations of a type of list (for example, when you create multiple VPN lists), you can include the same values or overlapping values in more than one of these list. You can do this either on purpose, to meet the design needs of your network, or you can do this accidentally, which might occur when you use ranges to specify values. (You can use ranges to specify data prefixes, site identifiers, and VPNs.) Here are two examples of lists that are configured with ranges and that contain overlapping values:

- **vpn-list list-1 vpn 1-10**

  vpn-list list-2 vpn 6-8

- **site-list list-1 site 1-10**

  site-list list-2 site 5-15

When you configure data policies that contain lists with overlapping values, or when you apply data policies, you must ensure that the lists included in the policies, or included when applying the policies, do not contain overlapping values. To do this, you must manually audit your configurations. The Cisco IOS XE Catalyst SD-WAN configuration software performs no validation on the contents of lists, on the data policies themselves, or on how the policies are applied to ensure that there are no overlapping values.

If you configure or apply data policies that contain lists with overlapping values to the same site, one policy is applied and the others are ignored. Which policy is applied is a function of the internal behavior of Cisco IOS XE Catalyst SD-WAN device when it processes the configuration. This decision is not under user control, so the outcome is not predictable.

SLA Classes

Table 155: Feature History

Feature	Release Information	Description
Support for six SLA Classes per Policy	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to configure up to six SLA classes per policy on Cisco IOS XE Catalyst SD-WAN devices. This allows additional options to be configured in an application-aware routing policy.
Support for SLA Classes	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature allows you to configure up to a maximum of eight SLA classes on Cisco Catalyst SD-WAN Controller. This allows for additional options to be configured in an application-aware routing policy.

An SLA (service-level agreement) determines the action taken in application-aware routing. An SLA class defines the maximum jitter, maximum latency, maximum packet loss, or a combination of these values for the Cisco IOS XE Catalyst SD-WAN device's data plane tunnels. (Each tunnel is defined by a local TLOC–remote TLOC pair.) You configure SLA classes under the **policy sla-class** command hierarchy onCisco Catalyst SD-WAN Controllers. In Cisco IOS XE Release 17.2 and onwards, you can configure a maximum of eight SLA classes. However, only 4 unique SLA classes can be defined in an application aware route policy. In older releases, you can configure a maximum of four SLA classes.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, you can configure up to six SLA classes per policy on the Cisco IOS XE Catalyst SD-WAN devices.

You can configure the following parameters in an SLA class:

Table 156:

Description	Command	Value or Range
Maximum acceptable packet jitter on the data plane tunnel	**jitter** *milliseconds*	1 through 1000 milliseconds
Maximum acceptable packet latency on the data plane tunnel.	**latency** *milliseconds*	1 through 1000 milliseconds
Maximum acceptable packet loss on the data plane tunnel.	**loss** *percentage*	0 through 100 percent

VPN Lists

Each application-aware policy instance is associated with a VPN list. You configure VPN lists with the **policy app-route-policy vpn-list** command. The VPN list you specify must be one that you created with a **policy lists vpn-list** command.

Sequences

Within each VPN list, an application-aware policy contains sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy. You configure sequences with the **policy app-aware-policy vpn-list sequence** command.

Each sequence in an application-aware policy can contain one **match** command and one **action** command.

Match Parameters

Application-aware routing policy can match IP prefixes and fields in the IP headers. You configure the match parameters with the **match** command under the **policy app-route-policy vpn-list sequence** command hierarchy on Cisco Catalyst SD-WAN Controllers.

You can match these parameters:

Table 157:

Description	Command	Value or Range
Match all packets	Omit **match** command	—
Applications or application families	**app-list** *list-name*	Name of an **app-list** list
Group of destination prefixes	**destination-data-prefix-list** *list-name*	Name of a **data-prefix-list** list
Individual destination prefix	**destination-ip** *prefix*/*length*	IP prefix and prefix length
Destination port number	**destination-port** *number*	0 through 65535. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
DSCP value	**dscp** *number*	0 through 63
Internet Protocol number	**protocol** *number*	0 through 255

Description	Command	Value or Range
For Protocol IPv4 when you enter a Protocol value as 1, the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. Likewise, the **ICMP Message** field displays for Protocol IPv6 when you you enter a Protocol value as 58. When you select Protocol as Both, the **ICMP Message or ICMPv6 Message** field displays. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.	**icmp-msg** *value* **icmp6-msg** *value*	For `icmp-msg` and `icmp6-msg` message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table.
Packet loss priority (PLP)	**plp**	(**high** | **low**) By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Group of source prefixes	**source-data-prefix-list** *list-name*	Name of a **data-prefix-list** list
Individual source prefix	**source-ip** *prefix/length*	IP prefix and prefix length
Source port number	**source-port** *number*	0 through 65535; enter a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])

Description	Command	Value or Range
Split DNS, to resolve and process DNS requests on an application-by-application basis	**dns-app-list** *list-name* **dns** (**request** | **response**)	Name of an **app-list** list. This list specifies the applications whose DNS requests are processed. To process DNS requests sent by the applications (for outbound DNS queries), specify **dns request**. To process DNS responses returned from DNS servers to the applications, specify **dns response**.

Action Parameters

When data traffic matches the match parameters, the specified action is applied to it. For application-aware routing policy, the action is to apply an SLA class. The SLA class defines the maximum packet latency or maximum packet loss, or both, that the application allows on the data plane tunnel used to transmit its data. TheCisco Catalyst SD-WAN software examines the recently measured performance characteristics of the data plane tunnels and directs the data traffic to the WAN connection that meets the specified SLA.

The following actions can be configured:

Table 158:

Description	Command	Value or Range
When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching, not a strict matching.	**backup-sla-preferred-color** *colors*	**3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, **silver**
Count matching data packets.	**action count** *counter-n ame*	Name of a counter.
SLA class to match. All matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.	**action sla-class** *sla-class-name*	SLA class name defined in **policy sla-class** command

Description	Command	Value or Range
Group of data plane tunnel colors to prefer when an SLA class match occurs. Traffic is load-balanced across all tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching.	**action sla-class** *sla-class-name* **preferred-color** *colors*	SLA class name defined in **policy sla-class** command and one of the supported tunnel colors.
Strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Note that for policy configured with this option, data traffic that matches the match conditions is dropped until the application-aware routing path is established.	**action sla-class** *sla-class-name* **strict** **action sla-class** *sla-class-name* **preferred-color** *color* **strict** **action sla-class** *sla-class-name* **preferred-color** *colors* **strict**	SLA class name defined in **policy sla-class** command

If more than one data plane tunnel satisfies an SLA class criteria, the Cisco IOS XE Catalyst SD-WAN device selects one of them by performing load-balancing across the equal paths.

Default Action

A policy's default action defines how to handle packets that match none of the match conditions. For application-aware routing policy, if you do not configure a default action, all data packets are accepted and transmitted based on normal routing decisions, with no consideration of SLA.

To modify this behavior, include the **default-action sla-class** *sla-class-name* command in the policy, specifying the name of an SLA class you defined in the **policy sla-class** command.

When you apply an SLA class in a policy's default action, you cannot specify the **strict** option.

If no data plane tunnel satisfies the SLA class in the default action, the Cisco IOS XE Catalyst SD-WAN device selects one of the available tunnels by performing load-balancing across equal paths.

Expected behavior when data flow matches both AAR and data policies:

1. When data policy local TLOC action is configured, the **App-route preferred-color** and **backup-preferred-color** actions are ignored.
2. The **sla-class** and **sla-strict** actions are retained from the application routing configuration.
3. The data policy TLOC takes precedence.

When there is a **local-tloc-list** action that has multiple options, choose the local-TLOC that meets SLA.

- If no **local-tloc** meets SLA, then choose equal-cost multi-path routing (ECMP) for the traffic over the **local-tloc-list**.
- If none of the **local-tloc** is up, then choose a TLOC that is up.

- If none of the **local-tloc** is up and the DP is configured in restrict mode, then drop the traffic.

Configure Type 6 Passwords Using CLI Add-On Template

You can configure type 6 passwords when using CLI add-on feature templates by doing the following:

1. Navigate to **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Under the Select Devices pane, select the devices for which you are creating the template.
5. Under the Select Template pane, scroll down to the Other Templates section.
6. Click **CLI Add-On Template**. For information on CLI add-on feature templates, see CLI Add-On Feature Templates.
7. Enter a Template Name and Description.
8. Type or paste the CLI that you want to run on your device.
9. Select the plaintext password in the CLI and click the **Encrypt Type 6** button.
10. Click **Save**.

Configure Underlay Measurement and Tracing Services

Table 159: Feature History

Feature Name	Release Information	Description
Underlay Measurement and Tracing Services	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	The underlay measurement and tracing services (UMTS) feature provides visibility into the exact paths that tunnels take between local and remote Cisco IOS XE Catalyst SD-WAN devices, through the underlay network (the physical devices that compose the network).

Configure UMTS Using Configuration Group

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

2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **System Profile**.
4. Click **Add Feature**.
5. From the **Type** drop-down list, choose **Performance Monitoring**.
6. In the **Feature Name** field, enter a name for the feature.
7. In the **Description** field, enter a description for the feature.
8. Click **Underlay Measurement Track Service**.
9. To trace the tunnel paths regularly, based on a time interval, do the following:
   a. From the **Monitoring** drop-down list, choose **Global**.
   b. Click the toggle button to enable the continuous monitoring option in UMTS.
   c. In the **Monitoring Interval (Minutes)** drop-down list, choose a time.

      This option enables you to monitor the exact path during a specific time period.
10. To trace tunnel paths when triggered by an event, do the following:
    a. Click the **Event Driven** drop-down list, and choose **Global**.
    b. Click the **Event Type** drop-down list, and choose one or more event types.
    c. Click **Save**.
11. Click the **Associated Devices** tab.
12. From the list of Cisco IOS XE Catalyst SD-WAN devices, choose one or more Cisco IOS XE Catalyst SD-WAN devices, and then click **Deploy**.
13. In the **Process Overview** window, click **Next**.

    The **Selected Devices to Deploy** window displays the Cisco IOS XE Catalyst SD-WAN devices selected previously.
14. Check or uncheck the check boxes adjacent to the Cisco IOS XE Catalyst SD-WAN devices and then click **Next**.
15. In the **Summary** window, click **Deploy** to deploy the configurations in the Cisco IOS XE Catalyst SD-WAN devices.

Note With the **Monitor** option enabled in Cisco SD-WAN Manager, time-series data for the exact path can be generated and displayed in Cisco SD-WAN Analytics.

For more information on using configuration groups, see Configuration Groups and Feature Profiles.

Configure Unified Communications

Table 160: Feature History

Feature Name	Release Information	Description
Integration with Cisco Unified Communications	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can configure items for UC voice services from the Feature tab and the Voice Policy page for a supported device.

Add a Voice Card Feature Template

A voice card feature template configures analog and PRI ISDN digital interfaces, which provide configuration settings for ports on voice cards in routers.

When you add a voice card feature template, for an analog interface, you configure the type of voice card you are configuring, port information for the card, and parameters for the service that you receive from your service provider. For a digital interface, you configure the type of voice card, the T1 or E1 controller, and related parameters.

When you add a module for a voice card, Cisco SD-WAN Manager assists you with the placement of the module by displaying available slots and sub-slots for the module. Cisco SD-WAN Manager determines the available slots and sub-slots based on the device model.

The following table describes options for configuring an analog interface.

Table 161: Analog Interface Configuration Options

Option	Description	Cisco IOS CLI Equivalent
Module	Select the type of voice module that is installed in the router.	—
Module Slot/Sub-slot	Enter the slot and sub-slot of the voice module.	**voice-card** *slot/subslot*
Use DSP	Enable this option if you want to use the built-in DSPs on the network interface module for TDM calls.	**no local-bypass**
Port Type	Select the type of ports on the voice module that you are configuring for this interface (**FXS** or **FXO**). You can select **All** to define the port type for all ports of the selected type, or **Port Range** to define the port type for a specified range of ports. Using Port Range, you can create analog interfaces as described later in this procedure to configure different ranges of ports.	—

Option	Description	Cisco IOS CLI Equivalent
Description	Enter a description of the selected port or ports. For example, fax machine or paging system.	**description** *string*
Secondary Dialtone	Available if you select FXO from the Port Type drop-down list. Set to **On** if you want the selected ports to generate a secondary dial tone when callers access an outside line.	**secondary dialtone**
Connection PLAR	Enter the Private Line Automatic Ringdown extension to which the selected ports forward inbound calls.	**connection plar** *digits*
OPX	Available if you select FXO from the Port Type drop-down list. Check this option if you want to enable Off-Premises Extension for the PLAR extension.	**connection plar opx** *digits*
Signal Type	Select the Signal Type that indicates an on-hook or off-hook condition for calls that the ports receive. Options are **Loopstart**, **Groundstart**, or **DID**. The DID option is available if you select FXS from the Port Type drop-down list.	**signal** {groundstart | loopstart} **signal did** {delay-dial | immediate | wink-start}
Caller-ID Enable	Available if you select a signal type of Loopstart or Groundstart. Set to **ON** if you want to enable caller ID information for inbound calls.	**caller-id enable**
DID Signal Mode	Available if you select a signal type of DID. Choose the mode for the DID signal type (**Delay Dial**, **Immediate**, or **Wink Start**). Default: Wink Start.	**signal did** {delay-dial | immediate | wink-start}
Shutdown	Set to **ON** if you want to shut down ports that are not being used. Default: Off.	**shutdown**

The following table describes options for configuring a digital interface.

Table 162: Digital Interface Configuration Options

Option	Description	Cisco IOS CLI Equivalent
Digital Interface Tab Provides options for configuring parameters for a T1/E1 voice module and the clock source for the module ports. Before you configure these options, ensure that you have the appropriate DSP module installed for each T1/E1 voice module.		
Module	Select the type of T1/E1 voice module that is installed in the router.	—
Interface Type	Select the type of interface on the voice module: • **T1 PRI**—Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding • **E1 PRI**—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps	**card type** {**t1** | **e1**} *slot sub-slot*
Slot/Sub-slot	Enter the slot and sub-slot of the voice module.	**voice-card** *slot*/*sub-slot*
Use DSP	Enable this option if you want to use the built-in DSPs on the network interface module for TDM calls.	**no local-bypass**

Option	Description	Cisco IOS CLI Equivalent
Interface	Perform these actions to configure the number of T1/E1 ports to be provisioned on the module, and the clock source for each port: **1.** Click **Add**. The Port and Clock Selector window displays. **2.** Check the check box that corresponds to each port that you want to configure. The number of ports that you can configure depends on the Module type that you select. **3.** For each port, select the clock source: • **Line**—Sets the line clock as the primary clock source. With this option, the port clocks its transmitted data from a clock that is recovered from the line receive data stream. • **Primary Clock**—Sets the port to be a primary clock source. • **Secondary Clock**—Sets the port to be a secondary clock source. • **Network**—Sets the backplane clock or the system oscillator clock as the module clock source. We recommend that you set one port to be the primary clock and set another port going to the same network as a secondary clock source to act as a backup. **4.** Click **Add**.	**controller** {**t1** | **e1**} *slot*/*sub-slot*/*number* **clock source** {**network** | **line** | **line primary** | **line secondary**}
Network Participation	This check box displays after you add an interface. Check this check box to configure the T1/E1 module to participate in the backplane clock. Uncheck this check box to remove the clock synchronization with the backplane clock for the module. By defult, this check box is checked.	**network-clock synchronization participate** *slot*/*sub-slot*

Option	Description	Cisco IOS CLI Equivalent
Shutdown	Perform these actions to disable or enable the controller, serial interface, or voice port that is associated with the interface port. 1. Click **Shutdown Selected**. The Shutdown window displays. 2. For each port, select the item or items that you want to enable (**Controller**, **Serial**, or **Voice Port**. If you do not select an item, it is enabled. 3. Click **Add**.	**controller e1/t1** *slot*/*sub-slot*/*port* **shutdown** **interface serial** *slot*/*sub-slot*/**port:** {**15** | **23**} **shutdown** **voice-port** *slot*/*sub-slot*/**port:** {**15** | **23**} **shutdown**
Time Slots	Select the number of time slots of the interface type. Valid ranges: • For T1 PRI—Time slots 1 through 24. The 24th time slot is the D channel. • For E1 PRI— Time slots 1 through 31. The 16th time slot is the D channel.	**controller e1/t1** *slot*/*sub-slot*/*port* **pri-group timeslots** *timeslot-range* [**voice-dsp**]
Framing	Select the frame type for the interface type. For a T1 PRI interface type, options are: • **esf**—Extended super frame (default) • **sf**—Super frame For an E1 PRI interface type, options are: • **crc4**—CRC4 framing type (default) • **no-crc4**—No CRC4 framing type	**controller t1** *slot*/*sub-slot*/*port* **framing** [**esf** | **sf**] **controller e1** *slot*/*sub-slot*/*port* **framing** [**crc4** | **no-crc4**] [**australia**]
Australia	This check box displays when you select E1 PRI for the interface type. Check this check box to use the **australia** framing type.	**controller e1** *slot*/*sub-slot*/*port* **framing** [**crc4** | **no-crc4**] **australia**

Option	Description	Cisco IOS CLI Equivalent
Line Code	Select the line code type for the interface type. For a T1 PRI interface type, options are: • **ami**—Use Alternate Mark Inversion as the line code type • **b8zs**—Use binary 8-zero substitution as the line code type (default) For an E1 PRI interface type, options are: • **ami**—Use Alternate Mark Inversion as the line code type • **hdb3**—Use high-density binary 3 as the line code type (default)	**controller t1** *slot*/*sub-slot*/*port* **linecode** [**ami** | **b8zs**] **controller e1** *slot*/*sub-slot*/*port* **linecode** [**ami** | **hdb3**]
Line Termination	This check box appears only for an Interface type of E1 PRI. Select the line termination type for the E1 controller: • **75-ohm**—75 ohm unbalanced termination • **120-ohm**—120 ohm balanced termination (default)	**controller e1** *slot*/*sub-slot*/*port* **line-termination** {**75-ohm** | **120-ohm**}
Cable Length Type	This check box appears only for an Interface type of T1 PRI. Select the cable length type for the T1 PRI interface type: • **long**—Long cable length • **short**—Short cable length	**controller t1** *slot*/*sub-slot*/*port* **cablelength** {**short** | **long**}
Cable Length	This check box appears only for an interface type of T1 PRI. Select the cable length for the T1 PRI interface type. Use this option to fine-tune the pulse of a signal at the receiver for a T1 cable. The default value is **0db**.	**controller t1** *slot*/*sub-slot*/*port* **cablelength** {**[short** [**110ft** | **220ft** | **330ft** | **440ft** | **550ft** | **660ft**]] [**long** [**-15db** | **-22.5db** | **-7.5db** | **0db**]]}

Option	Description	Cisco IOS CLI Equivalent
Network Side	Enable this option to have the device use the standard PRI network-side interface. By default, this option is disabled (set to **No**).	**interface serial** *slot*/*sub-slot*/**port:** {**15**| **23**} **isdn protocol-emulate** [**network**| **user**]
Switch Type	Select the ISDN switch type for this interface: • **primary-qsig**—Supports QSIG signaling according tot the Q.931 protocol. Network side functionality is assigned with the isdn protocol-emulate command. • **primary-net5**—NET5 ISDN PRI switch types for Asia, Australia, and New Zealand. ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system. • **primary-ntt**—Japanese NTT ISDN PRI switches. • **primary-4ess**—Lucent (AT&T) 4ESS switch type for the United States. • **primary-5ess**—Lucent (AT&T) 5ESS switch type for the United States. • **primary-dms100**—Nortel DMS-100 switch type for the United States. • **primary-ni**—National ISDN switch type.	**interface serial** *slot*/*sub-slot*/**port:** {**15**| **23**} **isdn switch-type** [**primary-4ess** | **primary-5ess** |**primary-dms100** | **primary-net5** | **primary-ni** | **primary-ntt** | **primary-qsig**]

Option	Description	Cisco IOS CLI Equivalent
ISDN Timer	Perform these actions to configure the ISDN timers for the interface: **1.** Click **Add**. The ISDN Timer window displays. **2.** Configure the following timers as needed. The values are in milliseconds. • **T200**. Valid range: integers 400 through 400000. Default: 1000. • **T203**. Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations. • **T301**. Valid range: integers 180000 through 86400000. The default value is based on the switch type and network side configurations. • **T303**. Valid range: integers 400 through 86400000. The default value is based on the switch type and network side configurations. • **T306**. Valid range: integers 400 through 86400000. Default: 30000. • **T309**. Valid range: integers 0 through 86400000. The default value is based on the switch type and network side configurations. • **T310**. Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations. • **T321**. Valid range: Integers 0 through 86400000. The default value is based on the switch type and network side configurations. **3.** Click **Add**.	**interface serial** *slot*/*sub-slot*/**port:**{**15**| **23**} **isdn timer T200** *value* **isdn timer T203** *value* **isdn timer T301** *value* **isdn timer T303** *value* **isdn timer T306** *value* **isdn timer T309** *value* **isdn timer T310** *value* **isdn timer T321** *value*
Delay Connect Timer	Select the duration, in milliseconds, to delay connect a PRI ISDN hairpin call. Valid range: integers 0 through 200. Default: 20.	**voice-port** *slot*/*sub-slot*/**port:**{**15**| **23**} **timing delay-connect** *value*

Option	Description	Cisco IOS CLI Equivalent
Clock Tab Use this tab to configure priority order for the primary and secondary clock sources that you selected for each module. This tab is vailable after you configure a PRI ISDN digital interface and click **Add**.		
Clock Priority Sorting	Configure the priority of up to six clock sources. The drop-down list displays the interface ports for which a primary or secondary clock source is defined and that is configured for network participation. Check a check box to select the port for inclusion in the priority list, and use the **Up arrow** next to a port to change its priority. The list displays the ports in order of priority, with the port with the highest priority at the top of the list. After you configure the priority, this field displays the selected ports in priority order. We recommend that all ports in the priority list be of the same type, either E1-PRI or T1-PRI.	**network-clock input-source** priority **controller** [**t1**| **e1**] *slot*/*sub-slot*/*port*
Automatically Sync	Select **Add** to enable network synchronization between all modules and the router. Default: **On**.	network-clock synchronization automatic
Wait to restore clock	Enter the amount of time, in milliseconds, that the router waits before including a primary clock source in the clock selection process. Valid range: 0 through 86400. Default: 300.	network-clock wait-to-restore *milliseconds*

To add a voice card feature template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select the supported device to which you want to add voice services.
4. Select **Voice Card** from the **Unified Communications** templates.

5. In **Template Name**, enter a name for the template.

   This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.

7. To configure an analog interface, click **New Analog Interface** and configure interface options as described in the "Analog Configuration Options" table.

   From Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, click **Analog Interface** in the Interface area to access **New Analog Interface**.

   You can add as many analog interfaces as needed, based on the number of interfaces that your module supports.

   After you configure each analog interface, click **Add**.

   If any analog interfaces are already configured, they appear in the interfaces table on this page. To edit an existing interface, click **…** and click its pencil icon to edit the options in the window that pops up as described in the "Analog Configuration Options" table, and click **Save Changes**. To delete an interface, click **…** and click the trash can icon.

8. To configure a PRI ISDN digital interface, in the **Interface** area, click **Digital Interface**, click **New Digital Interface**, and configure interface options as described in the "Digital Interface Configuration Options" table.

   After you configure each PRI ISDN digital interface, click **Add**.

   Based on the number of interfaces that your module supports, you can add as many PRI ISDN digital interfaces as needed.

   If any digital interfaces are already configured, they appear in the interfaces table on this page. To edit an existing interface, click **...** and click its pencil icon to edit the options in the window that pops up as described in the "Digital Interface Configuration Options" table, and click **Save Changes**. To delete an interface, click **…**, and click its trash can icon.

   After you save the interface configuration, you cannot change the module type, interface type, slot or sub-slot, or time slots.

   If you want to change time slots, you must delete the interface and create a new one.

   If you want to change the module type, interface type, and slot or sub-slot, detach the template from the device, unmap the voice policies that are associated with the interfaces, and delete all interfaces that are associated with the module and slot or sub-slot. Next, push the template to the device, reload the device, and create new required interfaces. Finally, push the new template to the device, and reattach the template to the device.

9. Click **Save**.

10. (Optional) If you want to configure more analog or PRI ISDN digital interfaces for this template, then:

    a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

    b. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

c. Click **...** for the template you wish to configure, and click **Edit**.

d. Repeat Step 7 or Step 8 and Step 9.

Add a Call Routing Feature Template

A call routing feature template configures parameters for TDM-SIP trunking, including trusted IP addresses for preventing toll fraud, and a dial plan. A dial plan, made up of dial peers, defines how a router routes traffic to and from voice ports to the PSTN or to another branch.

The following table describes global options for configuring call routing.

Table 163: Global Call Routing Options

Option	Description	Cisco IOS CLI Equivalent
Trusted IPv4 Prefix List	Enter the IPv4 addresses with which the router can communicate through SIP. Enter each IPv4 address in CIDR format. For example, 10.1.2.3/32. Separate each address with a comma (,). The router does not communicate with other IPv4 addresses, which prevents fraudulent calls being placed through the router. A Trusted IPv4 Prefix is required for TDM to IP calls.	**voice service voip** **ip address trusted list** **ipv4** *ipv4-address*/*ipv4-network-mask*
Trusted IPv6 Prefix List	Enter the IPv6 addresses with which the router can communicate through SIP. Separate each IPv6 address with a comma (,). The router does not communicate with other IPv6 addresses, which prevents fraudulent calls being placed through the router. A Trusted IPv6 Prefix is required for TDM to IP calls.	**voice service voip** **ip address trusted list** **ipv6** *ipv6-prefix*//*prefix-length*
Source Interface	Enter the name of the source interface from which the router initiates SIP control and media traffic. This information defines how the return/response to this traffic should be sent.	**voice service voip** **sip** **bind control source-interface** *interface-id* **bind media source-interface** *interface-id*

The following table describes options for configuring dial peers.

Table 164: Dial Peer Options

Option	Description	Cisco IOS CLI Equivalent
Voice Dial Peer Tag	Enter a number to be used to reference the dial peer.	**dial-peer voice** *number* {**pots** | **voip**}
Dial Peer Type	Select the type of dial peer that you are creating (**POTS** or **SIP**).	**dial-peer voice** *number* {**pots** | **voip**}
Direction	Select the direction for traffic on this dial peer (**Incoming** or **Outgoing**).	Incoming: dial-peer voice *number* {pots | voip} **incoming called-number** *string* Outgoing: dial-peer voice *number* {pots | voip} **destination-pattern** *string*
Description	Enter a description of this dial peer.	**description**
Numbering Pattern	Enter a string that the router uses to match incoming calls to the dial peer. Enter the string as an E.164 format regular expression in the form [0-9,A-F#*.?+%()-]*T?.	Incoming: dial-peer voice *number* {pots | voip} **incoming called-number***string* Outgoing: dial-peer voice *number* {pots | voip} **destination-pattern** *string*
Forward Digits Type	Available if you select the POTS dial peer type and the Outgoing direction. Select how the dial peer transmits digits in outgoing numbers: • **All**—The dial peer transmits all digits • **None**—The dial peer does not transmit digits that do not match the destination pattern • **Some**—The dial peer transmits the specified number of right-most digits Default: None.	All: dial-peer voice *number* pots **forward-digits all** None: dial-peer voice *number* pots **forward-digits 0** Some: dial-peer voice *number* pots **forward-digits** *number*

Option	Description	Cisco IOS CLI Equivalent
Forward Digits	Available if you select **Some** for Forward Digits Type. Enter the number of right-most digits in the outgoing number to transmit. For example, if you set this value to 7 and the outgoing number is 1112223333, the dial peer transmits 2223333.	dial-peer voice *number* pots **forward-digits** *number*
Prefix	Available if you select the POTS dial peer type and the Outgoing direction. Enter digits to be prepended to the dial string for outgoing calls.	dial-peer voice *number* pots **prefix** *string*
Transport Protocol	Available if you select SIP for the Dial Peer Type. Choose the transport protocol (**TCP** or **UDP**) for SIP control signaling.	dial-peer voice *number* voip **session transport** {**tcp** | **udp**}
Preference	Available if you select POTS or SIP for the Dial Peer Type. Select an integer from 0 to 10, where the lower the number, the higher the preference. If dial peers have the same match criteria, the system uses the one with the highest preference value. Default: 0 (highest preference).	dial-peer voice *number* voip **preference** *value* dial-peer voice *number* pots **preference** *value*
Voice Port	Available if you select the POTS dial peer type. Enter the voice port that the router uses to match calls to the dial peer. For an analog port, enter the port you want. For a digital **T1** PRI ISDN port, enter a port with the suffix:**23**. For a digital E1 PRI ISDN port, enter a port with the suffix :**15**. For an outgoing dial peer, the router sends calls that match the dial peer to this port. For an incoming dial peer, this port serves as an extra match criterion. The dial peers are matched only if a call comes in on this port.	dial-peer voice *number* pots For an analog port: **port** *slot*/*subslot*/*port* For a digital port: **port** *slot*/*subslot*/*port***:15** **port** *slot*/*subslot*/*port***:23**

Option	Description	Cisco IOS CLI Equivalent
Destination Address	Available if you select the SIP dial peer type and the Outgoing direction. Enter the network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched. Enter the address in one of these formats: • dns:*hostname.domain* • *sip-server* ipv4:*destination-addres* ipv6:*destination-address*	**session target** {**ipv4:***destination-address* | **ipv6:***destination-address*| **sip-server** | **dns:***hostname.domain*}

To add a call routing feature template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select the supported device to which you want to add call routing features.
4. Click **Call Routing** from the **Unified Communications** templates.
5. In **Template Name**, enter a name for the template.

   This field can contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.
7. In **Global**, configure options as described in the "Global Call Routing Options" table.
8. In **Dial Plan**, perform one of these actions:
   - To configure a dial peer directly, configure options as described in the "Dial Peer Options" table.
   - To create or edit a dial peer CSV file, click **Download Dial Peer List** to download the system provided file named Dial-Peers.csv. The first time you download this file, it contains field names but no records. Update this file as needed by using an application such as Microsoft Excel. For detailed information about this file, see Dial Peer CSV File.
   - To import configuration information from a dial peer CSV file that you have created, click **Upload Dial Peer List**.

   You can add as many dial peers as needed. Click **Add** after you configure each dial peer.

If any dial peers already are configured, they appear in the dial peers table on this page. To edit a configured dial peer, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the table, and click **Save Changes**. To delete a dial peer, click **…**, and click its trash can icon.

9. Click **Save**.

Add an SRST Feature Template

An SRST feature template configures parameters for Cisco Unified Survivable Remote Site Telephony (SRST) for SIP. With Cisco Unified SRST, if the WAN goes down or is degraded, SIP IP phones in a branch site can register to the local gateway so that they continue to function for emergency services without requiring WAN resources that are no longer available.

The following table describes global options for configuring Cisco Unified SRST.

Table 165: Global Cisco Unified SRST Options

Option	Description	Cisco IOS CLI Equivalent
System Message	Enter a message that displays on endpoints when Cisco Unified SRST mode is in effect.	**voice register global** **system message** *string*
Max Phones	Enter the number of phones that the system can register to the local gateway when in Cisco Unified SRST mode. The available values and the maximum values that you can enter in this field depend on the device that you are configuring. Hover your mouse pointer over the Information icon next to this field to see maximum values for supported devices.	**voice register global** **max-pool** *max-voice-register-pools*
Max Directory Numbers	Enter the number of DNs that the gateway supports when in Cisco Unified SRST mode. The available values and the maximum values that you can enter in this field depend on the device that you are configuring. Hover your mouse pointer over the Information icon next to the Max phones to support field to see maximum values for supported devices.	**voice register global** **max-dn** *max-directory-numbers*
Music on Hold	Select **Yes** to play music on hold on endpoints when a caller is on hold when in Cisco Unified SRST mode. Otherwise, select **No**.	—

Option	Description	Cisco IOS CLI Equivalent
Music on Hold file	Enter the path and file name of the audio file for music on hold. The file must be in the system flash and must be in .au or .wav format. In addition, the file format must contain 8-bit 8-kHz data, for example, CCITT a-law or u-law data format.	**call-manager-fallback** **moh** *filename*

The following table describes options for configuring Cisco Unified SRST phone profiles.

Table 166: SRST Phone Profile Options

Option	Description	Cisco IOS CLI Equivalent
Voice Register Pool Tag	Enter the unique sequence number of the IP phone to be configured. The maximum value is defined by the Max phones to support option in the Global tab of the SRST feature template.	**voice register pool** *pool-tag*
Device Network IPv6 Prefix	Enter the IPv6 prefix of the network that contains the IP phone to support. For example, a.b.c.d/24.	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]
Device Network IPv4 Prefix	Enter the IPv4 prefix of the network that contains the IP phone to support.	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]

To add an SRST feature template:

1. From the Cisco SD-WAN Manager menu, Choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select the supported device to which you want to add Cisco Unified SRST features.
4. Click **SRST** from the Unified Communications templates.
5. In **Template Name**, enter a name for the template.

   This field can contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.
7. In **Global Settings**, configure options as described in the "Global SRST Options" table.

8. From **Phone Profile**, click **New Phone Profile** to create a phone profile, and configure options as described in the "SRST Phone Profile Options" table.

   A phone profile provides pool tag and device network information for a SIP phone.

   You can add as many phone profiles as needed. Click **Add** after you configure each phone profile.

   If any phone profiles already are configured, they appear in the phone profiles table on this page. To edit a configured phone profile, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the table, and click **Save Changes**. To delete a phone profile, click **…**, and click its trash can icon.

9. Click **Save**.

Add a DSPFarm Feature Template

A DSP farm is a pool of DSP resources on a router. Cisco Catalyst SD-WAN uses DSP farm resources that are available to Cisco Unified Communications Manager for Cisco Unified Communications Manager controlled transcoding, conferencing (non-secure only), and media termination point (MTP) services. Cisco Unified Communications Manager dynamically invokes these resources as needed in a call path.

A DSPFarm feature template is used to set up and provision a DSP farm. The template supports dedicated DSP modules only. T1/E1 modules are not supported.

When you add a DSPFarm feature template, you configure options for the following items:

- Media resource modules—DSP modules and their placement on a router. You determine and build DSP farm profiles based on media resource modules.
- DSP farm profiles—Each profile defines parameters for provisioning a specific DSP farm service type. A profile includes options for provisioning a group of DSP resources that is used for transcoding, conferencing (only non-secure conferencing is supported), or MTP services. A profile is registered to a Cisco Unified Communications Manager so that the Cisco Unified Communications Manager can invoke the resources for a service as needed.
- SCCP config—Configures a local interface that is used to communicate with up to four Cisco Unified Communications Manager servers, and configures related information that is required to register the DSP farm profiles to Cisco Unified Communications Manager. Also configures one or more Cisco Unified Communications Manager groups, each of which includes up to four Cisco Unified Communications Manager servers that control the DSP farm services that, in turn, are associated with the servers.

When you add a media resource module, Cisco SD-WAN Manager assists you with the placement of the module by displaying available slots and sub-slots for the module. Cisco SD-WAN Manager determines the available slots and sub-slots based on the device model.

The following table describes options for configuring media resources.

Table 167: Media Resource Options

Option	Description	Cisco IOS CLI Equivalent
Module	Select the router resource module to carry DSP resources that are used by DSPFarm profiles.	—

Option	Description	Cisco IOS CLI Equivalent
Slot/sub-slot ID	Select the slot and sub-slot in which the resource module that you selected resides.	**voice-card** *slot*/*subslot* **dsp service dspfarm**

The following table describes options for configuring DSP farm services.

Table 168: DSP Farm Service Options

Option	Description	Cisco IOS CLI Equivalent
Profile Type	Select the type of DSP farm service that this profile is for. Options are **Transcoder**, **Conference**, and **MTP**	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**}
Profile ID	A system-generated unique identifier for the profile.	—
Universal	Available if you select Transcoder for the Profile Type When this check box is unchecked, transcoding is allowed only between the G.711 codec and other codecs. When this check box is checked, transcoding is allowed between codecs of any type.	**dspfarm profile** *profile-identifier* **transcode** [**universal**]

Option	Description	Cisco IOS CLI Equivalent
List Codec		**codec** *codec-name*

Option	Description	Cisco IOS CLI Equivalent

	Select the codecs that are available for the DSP farm service that this profile defines.
	The following codecs are supported. For MTP profile types, you can select one option, or you can select **pass-through** and one other option. If you want to change a codec, unselect the current codec before selecting a new one.
	• For the Transcoder profile type:
	  • g711alaw
	  • g711ulaw
	  • g729abr8
	  • g729ar8
	  • g729br8
	  • g729r8
	  • g722-64
	  • ilbc
	  • iSAC
	  • pass-through
	• For the Conference profile type:
	  • g711alaw
	  • g711ulaw
	  • g722r-64
	  • g729abr8
	  • g729ar8
	  • g729br8
	  • g729r8
	• For the MTP profile type for software MTP only:
	  • g711ulaw
	  • g711alaw	

Option	Description	Cisco IOS CLI Equivalent
	• g722-64 • g729abr8 • g729ar8 • g729br8 • g729r8 • ilbc • iSAC • pass-through • For the MTP profile type for hardware MTP only, or for hardware and software MTP: • g711ulaw • g711alaw • pass-through	
Conference Maximum Participants	Available if you select Conference for the Profile Type. Select the maximum number of parties that can participate in a conference bridge (**8**, **16**, or **32**).	**maximum conference-participants** *number*
Maximum Sessions	Available if you select Transcoder or Conference for the Profile Type. Enter the maximum number of sessions that this profile can support. This value depends on the maximum number sessions that can be configured with the DSP resources that are available on the router. These resources are based on the type of modules in the router. To determine these resources, you can use a DSP calculator.	**maximum sessions** *number*

Option	Description	Cisco IOS CLI Equivalent
MTP Type	Available if you select MTP for the Profile Type. Select the way in which the router performs minor MTP translations such as G.711alaw to G.711ulaw, and DTMF conversions. Options are: • **Hardware**—MTP translations and conversions are performed by the hardware DSP resources • **Software**—MTP translations and conversions are performed by the router CPU	**maximum session** {**hardware** | **software**}
MTP Maximum Hardware Sessions	Available if you select Hardware for the MTP type. Select the maximum number of hardware sessions that can be used for MTP translations and conversions. Maximum value: 4000	**maximum session hardware** *number*
MTP Maximum Software Sessions	Available if you select Software for the MTP type. Select the maximum number of CPU sessions that can be used for MTP translations and conversions. Maximum value: 6000	**maximum session software** *number*
Application	Select the type of application to which the DSP farm services that are provisioned on the device are associated.	**associate application sccp**
Shutdown	Enable this option to take this profile out of service.	**shutdown**

The following table describes options for configuring SCCP.

Table 169: SCCP Options

Option	Description	Cisco IOS CLI Equivalent
CUCM Tab Configure up to 12 Cisco Unified Communications Manager servers to which the profiles that you defined in the Profile tab register.		
Local Interface	Enter the local interface that DSP services that are associated with the SCCP application use to register with Cisco Unified Communications Manager. Enter the interface in this format: ***interface-type/interface-number/port*** where: • *interface-type*—Type of interface that the services use to register with Cisco Unified Communications Manager. The type can be a GigabitEthernet interface or a port channel interface. • *interface-number*—Interface number that the services use to register with Cisco Unified Communications Manager. • *port*—(Optional) Port on which the interface communicates with Cisco Unified Communications Manager. If you do not specify a port, the default value 2000 is used. For example: **GigabitEthernet0/0/0**.	**sccp local** *interface-type interface-number* [**port** *port-number*]

Option	Description	Cisco IOS CLI Equivalent
Server List - *x*	Designate a Cisco Unified Communications Manager server to which the profiles that you defined in the Profile tab register. In the first field, enter the IP address or DNS name of the Cisco Unified Communications Manager server. In the second field, enter a numerical identifier for the Cisco Unified Communications Manager server. Click the Plus Sign icon (+) to configure up to 11 additional servers. To remove a server, click its corresponding Minus Sign icon. (–).	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* **version 7.0+**
CUCM Groups Tab This tab is available when at least one Cisco Unified Communications Manager server is configured in the Cisco Unified Communications Manager tab. Configure a Cisco Unified Communications Manager group, which includes up to 4 Cisco Unified Communications Manager servers that control the DSP farm services that, in turn, are associated with the servers. If any Cisco Unified Communications Manager groups are already configured, they appear in the table in this tab. To edit a configured Cisco Unified Communications Manager group, click its pencil icon in the Action column, edit the options in the window that pops up as described in the following rows, and click **Save Changes**. To delete a Cisco Unified Communications Manager group, click its trash can icon in the Action column.		
Add New CUCM Group	Click to add a new Cisco Unified Communications Manager group.	**sccp ccm group** *group-id*

Option	Description	Cisco IOS CLI Equivalent
Server Groups Priority Order	Select the priority in which the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group are used. To do so: 1. Click this field to display a list of the Cisco Unified Communications Manager servers that you configured on the Cisco Unified Communications Manager tab. 2. Select the server that you want to be the primary server. This server has the highest priority. 3. Click the field again and select the server that you want to be the redundant server with the next highest priority. Repeat this step to select other redundant servers. The servers appear in this field in priority order. To remove a server from the group, click its X icon. To change the priority order of servers, remove the servers and add them back in the desired order.	**associate ccm** *cisco-unified-communications-manager-id* **priority** *priority*

Option	Description	Cisco IOS CLI Equivalent
CUCM Media Resource Name Profile to be Associated	In the Cisco Unified Communications Manager Media Resource Name field, enter a unique name that is used to register a DSP farm profile to the Cisco Unified Communications Manager servers. The name must contain from 6 to 15 characters. Characters can be letter, numbers, slashes (/), hyphens (-), and underscores (_). Space characters are not allowed. In the corresponding Profile to be Associated field, select a DSP farm profile to be registered to this Cisco Unified Communications Manager group using the name that you entered. To select a profile, click this field to display a list of the profile IDs that were configured on the Profile tab, and click the ID of the profile that you want. To add another Cisco Unified Communications Manager media resource name and profile, click the plus sign (+). You can add up to 4 Cisco Unified Communications Manager media resources and profiles. To remove a Cisco Unified Communications Manager media resource name and profile, click its corresponding minus sign (–).	**associate ccm** *profile-identifier* **register** *device-name*

Option	Description	Cisco IOS CLI Equivalent
CUCM Switchback	Select the switchback method that the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group use to switch back after a failover: • **graceful**—Switchback occurs after all active sessions terminate gracefully. • **guard**—Switchback occurs either when active sessions are terminated gracefully or when the guard timer expires, whichever happens first. • **immediate**—Performs the Cisco Unified Communications Manager switchback to the higher priority Cisco Unified Communications Manager immediately when the timer expires, whether there is an active connection or not. Default: **graceful**.	**switchback method** {**graceful** | **guard** [*timeout-guard-value*] | **immediate**}
CUCM Switchover	Select the switchover method that Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager use group when failing over: • **graceful**—Switchback occurs after all active sessions terminate gracefully. • **immediate**—Switchover occurs immediately, whether there is an active connection or not. Default: **graceful**.	**switchover method** {**graceful** | **immediate**}

To add a DSPFarm feature template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select the supported device to which you want to add a DSP farm.
4. Click **DSPFarm** from the **Unified Communications** templates.
5. In **Template Name**, enter a name for the template.

   This field can contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.
7. From **Media Resources Modules**, click **Add Media Resources**, and configure options as described in the "Media Resource Options" table.

   A media resource module is a DSP module that is used by DSP Farm profiles.

   You can add as many media resources interfaces as needed.

   Click **Add** after you configure each media resource. After you configure a media resource, you cannot modify or delete it because other configuration items are based on the module and its placement. If you need to change a media resource configuration, you must remove the DSPFarm feature template and create a new one.

   If any media resources are already configured, they appear in the table in this tab. To edit a configured media resource, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the "Media Resource Options" table, and click **Save Changes**. To delete a media resource, click **…**, and click its trash can icon.
8. From **Profile**, click **Add New Profile** to add a profile for a DSP farm service on a router, and configure options for the profile as described in the "DSP Farm Service Options" table.

   Click **Add** after you configure a profile. You can add up to 10 DSP farm profiles for each feature template.

   Before you create a profile, you must know the maximum number of sessions that can be configured with the DSP resources that are available on the router. These resources are based on the type of modules in the router. To determine these resources, you can use a DSP calculator.

   After you add a profile, you can modify the List Codec, Maximum Sessions, Maximum Conference Participants, and Shutdown options. You cannot change the profile type. If you want to change the profile type, you must delete the profile and create a new one.

   If any profiles are already configured, they appear in the table in this tab. To edit a configured profile, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the "DSP Farm Service Options" table, and click **Save Changes**. To delete a profile, click **…**, and click its trash can icon.
9. In **SCCP Config**, configure options as described in the "SCCP Options" table.
10. Click **Save**.

Add a Voice Policy

A voice policy defines how the system augments and manipulates calls for various endpoint types. Endpoints include voice ports, POTS dial peers, SIP dial peers, and Cisco Unified SRST phone profiles. A voice policy includes subpolicies for each endpoint that you want to configure.

To add a voice policy:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.
2. Click **Add Voice Policy**.
3. In **Voice Policy Name**, enter a name for the policy.
4. Configure the following as required:
   - **Voice Ports**–See Configure Voice Ports for a Voice Policy, on page 477
   - **POTS Dial Peers**–See Configure POTS Dial Peers for a Voice Policy, on page 493
   - **SIP Dial Peers**–See Configure SIP Dial Peers for a Voice Policy, on page 502
   - **SRST Phones**–See Configure SRST Phones for a Voice Policy, on page 515
5. Click **Save Policy**.

Configure Voice Ports for a Voice Policy

When you configure voice ports for a voice policy, you configure options that define how the system augments and manipulates calls for the voice port endpoint type.

You can configure the following call functionality policy options, depending on the type of voice card you are using:

- **Trunk Group**— Use these options to configure voice ports as a member of a trunk group for the card. You can configure one trunk group for voice card. The following table describes these options.

Table 170: Trunk Group Options for Voice Ports

Option	Description	Cisco IOS CLI Equivalent
Add New Trunk Group	Click to add a trunk group for the selected card. You can add one trunk group for a voice port.	—
Copy from Existing	Click to copy an existing trunk group to a new trunk group. In the box that appears, change the name if desired, select a trunk group, and click **Copy**.	—
Name	Name of the trunk group. The name can contain up to 32 characters.	**trunk group** *name*

Option	Description	Cisco IOS CLI Equivalent
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle** [**both** | **even** | **odd**] **hunt-scheme least-used** [**both** | **even** | **odd**] **hunt-scheme longest-idle** [**both** | **even** | **odd**] **hunt-scheme round-robin** [**both** | **even** | **odd**] **hunt-scheme sequential** [**both** | **even** | **odd**] **hunt-scheme random**

Option	Description	Cisco IOS CLI Equivalent
	Select the hunt scheme in the trunk group for outgoing calls: • **least-idle both**—Searches for an idle channel with the shortest idle time • **least-idle even**—Searches for an idle even-numbered channel with the shortest idle time • **least-idle odd**—Searches for an idle odd-numbered channel with the shortest idle time • **least-used both**—Searches for a trunk group member that has the highest number of available channels (applies only to PRI ISDN cards) • **least-used even**—Searches for a trunk group member that has the highest number of available even-numbered channels (applies only to PRI ISDN cards) • **least-used odd**—Searches for a trunk group member that has the highest number of available odd-numbered channels (applies only to PRI ISDN cards) • **longest-idle both**—Searches for an idle odd-numbered channel with the longest idle time • **longest-idle even**—Searches for an idle channel that has the highest number of available even-numbered channels • **longest-idle odd**—Searches for an idle channel that has the highest number of available odd-numbered channels • **round-robin both**—Searches trunk group members in turn for an idle channel, starting with the trunk group member that follows the last used member • **round-robin even**—Searches trunk group member in turn for an idle even-numbered channel, starting with	

Option	Description	Cisco IOS CLI Equivalent
	the trunk group member that follows the last used member • **round-robin odd**—Searches trunk group member in turn for an idle odd-numbered channel, starting with the trunk group member that follows the last used member • **sequential-both**—Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-even**—Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-odd**—Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **random**—Searches for a trunk group member at random and selects a channel from the member at random Default: **least-used both**	
Max Calls	Enter the maximum number of calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of calls. If the maximum number of calls is reached, the trunk group becomes unavailable for more calls. • In field—Enter the maximum number of incoming calls that are allowed for this trunk group • Out field— Enter the maximum number of outgoing calls that are allowed for this trunk group Valid range for both fields: integers 0 through 1000.	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]

Option	Description	Cisco IOS CLI Equivalent
Max-Retry	Select the maximum number of outgoing call attempts that the trunk group makes if an outgoing call fails. If you do not enter a value and a call fails, the system does not attempt to make the call again. Valid range: integers 1 through 5.	**trunk group** *name* **max-retry** *attempts*
Save Trunk Group	Click to save the Trunk Group that you configured.	—

- **Translation Profile**—Use these options to configure translation rules for calling and called numbers. The following table describes these options.

Table 171: Translation Profile Options for Calling and Called Numbers

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected card. You can create up to two translation profiles for this endpoint.	**voice translation-profile** *name*
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	—
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence* /*match-pattern*/ / *replace-pattern*/ Reject Rule: **rule** *precedence* **reject** /*match-pattern*/

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation Rules CSV File. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the Action drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string.	

Option	Description	Cisco IOS CLI Equivalent
	To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. **8.** Click **Save**. **9.** Add more translation rules as needed. **10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file. **11.** Click **Finish** at the bottom of the pane.	

- **Station ID**—Use these options to configure the name and number for caller ID display. The following table describes these options.

Table 172: Station ID Options

Option	Description	Cisco IOS CLI Equivalent
Station Name	Enter the name of the station. The station name can contain up to 50 letters, numbers, and spaces, dashes (-), and underscores (_).	**station-id name** *name*
Station Number	Enter the phone number of the station in E.164 format. The station number can contain up to 15 numeric characters.	**station-id number** *number*

- **Line Params**—Use these options to configure line parameters on the card for voice quality. The following table describes these options.

Table 173: Line Params Options

Option	Description	Cisco IOS CLI Equivalent
Gain	Enter the gain, in dB, for voice input. Valid range: –6 through 14. Default: 0	**input gain** *decibels*

Option	Description	Cisco IOS CLI Equivalent
Attenuation	Enter the amount of attenuation, in dB, for transmitted voice output. Valid range: –6 through 14. Default: 3.	**output attenuation** *decibels*
Echo Canceller	Select **Enable** to apply echo cancellation to voice traffic. By default, this option is enabled.	**echo-cancel** *enable*
Voice Activity Detection (VAD)	Select **Enable** to apply VAD to voice traffic. By default, this option is enabled.	**vad**
Compand Type	Select the companding standard to be used to convert between analog and digital signals in PCM systems (**U-law** or **A-law**). Default: U-Law.	**compand-type** {**u-law** | **a-law**}
Impedance	This field does not apply to PRI ISDN cards. Select the terminating impedance for calls. Default: 600r.	**impedance** {**600c** | **600r 900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}
Call Progress Tone	Select the locale for call progress tones.	**cptone** *locale*

- **Tuning Params**—Use these options to configure parameters for signaling between voice ports and another instrument. The following table describes these options.

Table 174: Tuning Params Options

Option	Description	Cisco IOS CLI Equivalent
Tuning Params Options for FXO Cards		
Pre Dial Delay	Enter the delay, in seconds, of the delay on the FXO interface between the beginning of the off-hook state and the initiation of DTMF signaling. Valid range: 0 through 10. Default: 1.	**pre-dial-delay** *seconds*

Option	Description	Cisco IOS CLI Equivalent
Supervisory Disconnect	Select the type of tone that indicates that a call has been released and that a connection should be disconnected: • **Anytone**—Any tone indicates a supervisory disconnect • **Signal**—A disconnect signal indicates a supervisory disconnect • **Dualtone**—A dual-tone indicates a supervisory disconnect Default: Signal.	Anytone: supervisory disconnect **anytone** Signal: supervisory disconnect Dualtone: supervisory disconnect **dualtone** {**mid-call** | **pre-connect**}
Dial Type	Select the dialing method for outgoing calls: • **pulse**—Pulse dialer • **dtmf**—Dual-tone multifrequency dialer • **mf**—Multifrequency dialer Default: dtmf.	**dial-type** {**dtmf** | **pulse** | **mf**}
Timing Sup-Disconnect	Enter the minimum time, in milliseconds, that is required to ensure that an on-hook indication is intentional and not an electrical transient on the line before a supervisory disconnect occurs (based on power denial signaled by the PSTN or PBX). Valid range: 50 through 1500. Default: 350.	**timing sup-disconnect** *milliseconds*

Option	Description	Cisco IOS CLI Equivalent
Battery Reversal	Battery reversal reverses the battery polarity on a PBX when a call connects, then changes the battery polarity back to normal when the far-end disconnects. Select **Answer** to configure the port to support answer supervision by detection of battery reversal. Select **Detection Delay** to configure the delay time after which the card acknowledges a battery-reversal signal, then enter the delay time in milliseconds. Valid range: 0 through 800. Default: 0 (no delay). If an FXO port or its peer FXS port does not support battery reversal, do not configure battery reversal options to avoid unpredictable behavior.	**battery-reversal** [**answer**] **battery-reversal-detection-delay** *milliseconds*
Timing Hookflash out	Enter the duration, in milliseconds, of hookflash indications that the gateway generates on the FXO interface. Valid range: 50 through 1550. Default: 400.	**timing hookflash-out** *milliseconds*
Timing Guard out	Enter the number of milliseconds after a call disconnects before another outgoing call is allowed. Valid range: 300 through 3000. Default: 2000.	**timing guard-out** *milliseconds*
Tuning Params Options for FXS Cards		
Timing Hookflash In	Enter the minimum and maximum duration, in milliseconds, of an on-hook condition to be interpreted as a hookflash by the FXS card. Valid range for minimum duration: 0 through 400. Default minimum value: 50. Valid range for maximum duration: 50 through 1500. Default maximum value: 1000.	**timing hookflash-in** *maximum-milliseconds minimum-milliseconds*
Pulse Digit Detection	To enable pulse digit detection at the beginning of a call, select **Yes**. Default: Yes.	**pulse-digit-detection**

Option	Description	Cisco IOS CLI Equivalent
Loop Length	Select the length for signaling on FXS ports (**Long** or **Short**). Default: Short.	**loop-length** [**long** | **short**]
Ring	• **Frequency**—Select the frequency, in Hz, of the alternating current that, when applied, rings a connected device. Default: 25. • **DC Offset**—Applies only if Loop Length is set to Long. Select the voltage threshold below which a ring does not sound on devices. Valid values: 10-volts, 20-volts, 24-volts, 30-volts, and 35-volts.	**ring frequency** *number* **ring dc-offset** *number*
Ringer Equivalence Number (REN)	Select the REN for calls that this card processes. This number specifies the loading effect of a telephone ringer on a line. Valid range: 1 through 5. Default: 1.	**ren** *number*

- **Supervisory Disconnect**—Use these options to configure parameters for supervisory disconnect events. The following table describes these options.

Table 175: Supervisory Disconnect Options

Option	Description	Cisco IOS CLI Equivalent
Add New Supervisory Disconnect	Click to add a supervisory disconnect event.	—
Mode	Choose the mode for the supervisory disconnect event: • **Custom CPTone**—Provides options for configuring cptone detection parameters for a supervisory disconnect event • **Dual Tone Detection Params**—Provides options for configuring dual-tone detection parameters for a supervisory disconnect event	**voice class custom-cptone** *cptone-name* **voice class dualtone-detect-params** *tag*

Option	Description	Cisco IOS CLI Equivalent
Supervisory Name	Applies to Custom CPTone mode. Enter a name for the supervisory disconnect event. The name can contain up to 32 characters. Valid characters are letters, numbers, dashes (-), and underscores (_).	**voice class custom-cptone** *cptone-name*
Dualtone	Applies to Custom CPTone mode. Select the type of dual-tone that causes a disconnect. Options are: • Busy • Disconnect • Number Unobtainable • Out of Service • Reorder • Ringback	**dualtone** {**ringback** |**busy** | **reorder** | **out-of-service** | **number-unobtainable** | **disconnect**}
Cadence	Applies to Custom CPTone mode. Enter the cadence interval, in milliseconds, of the dual-tones that cause a disconnect. Enter the cadence as an on/off value pair, separated with a space. You can enter up to 4 on/off value pairs, separated with a space.	**cadence** *cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time* [*cycle-3-on-time cycle-3-off-time* [*cycle-4-on-time cycle-4-off-time*]]]
Dualtone Frequency	Applies to Custom CPTone mode. Enter the frequency, in Hz, of each tone in the dual-tone. Valid range for each tone is 300 through 3600.	**frequency** *frequency-1* [*frequency-2*]
Supervisory Number	Applies to Custom Dual Tone Detection Params mode. Enter a unique number to identify dual-tone detection parameters. Valid range: 1 through 10000.	**voice class dualtone-detect-params** *tag-number*
Cadence-Variation	Applies to Custom Dual Tone Detection Params mode. Enter the maximum time, in milliseconds, by which the tone onset can vary from the onset time and still be detected. The system multiplies the value that you enter by 10. Valid range: 0 through 200 in units of 10. Default: 10.	**cadence-variation** *time*

Option	Description	Cisco IOS CLI Equivalent
Frequency	Applies to Custom Dual Tone Detection Params mode. • Max Delay—Enter the maximum delay, in milliseconds, before a supervisory disconnect is performed after the dual-tone is detected. The system multiplies the value that you enter by 10. Valid range: 0 through 100 in units of 10. Default: 10. • Max Deviation—Enter the maximum deviation, in Hz, by which each tone can deviate from configured frequencies and be detected. Valid range: 10 through 125. Default: 10. • Max Power—Enter the power of the dual-tone, in dBm0, above which a supervisory disconnect is no detected. Valid range: 0 through 20. Default: 10. • Min Power— Enter the power of the dual-tone, in dBm0, below which a supervisory disconnect is not detected. Valid range: 10 through 35. Default: 30. • Power Twist—Enter difference, in dBm0, between the minimum power and the maximum power of the dual-tone above which a supervisory disconnect is not detected. Valid range: 0 through 15. Default: 6.	**freq-max-delay** *time* **freq-max-deviation** *hertz* **freq-max-power** *dBm0* **freq-min-power** *dBm0* **freq-power-twist** *dBm0*
Save	Click to save the supervisory disconnect information that you configured.	—

- **DID Timers**—Use these options to configure timers for DID calls. The following table describes these options.

Table 176: DID Timers Options

Option	Description	Cisco IOS CLI Equivalent
Wait Before Wink	Enter the amount of time, in milliseconds, that the card waits after receiving a call before sending a wink signal to notify the remote side that it can send DNIS information. Valid range: 100 through 6500. Default: 550.	**timing wait-wink** *milliseconds*
Wink Duration	Enter the maximum amount of time, in milliseconds, of the wink signal for the card. Valid range: 50 through 3000. Default: 200.	**timing wait-duration** *milliseconds*
Clear Wait	Enter the minimum amount of time, in milliseconds, between an inactive seizure signal and the call being cleared for the card. Valid range: 200 through 2000. Default: 400.	**timing clear-wait** *milliseconds*
Dial Pulse Min Delay	Enter the amount of time, in milliseconds, between wink-like pulses for the card. Valid range: 0 or 140 through 5000. Default: 140.	**timing dial-pulse min-delay** *milliseconds*
Answer Winkwidth	Enter the minimum delay time, in milliseconds, between the start of an incoming seizure and the wink signal. Valid range: 110 through 290. Default: 210.	**timing answer-winkwidth** *milliseconds*

To configure voice ports for a voice policy, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.
2. Click **Add Voice Policy**, and choose **Voice Ports** in the left pane.
3. From the **Add Voice Ports Policy Profile** drop-down list, select **Create New**.

   Alternatively, you can select **Copy from Existing** to copy an existing voice policy to a new voice policy. In the box that appears, select the name of the policy profile to copy, enter a new name for the profile if desired, and click **Copy**.
4. Select **FXO**, **FXS**, **PRI ISDN**, or **FXS DID** to specify the type of voice port that the policy is for.
5. Select the types of call functionality policy options that you want to configure from the list of options that displays, and click **Next**. These option types include the following:

- **Trunk Group**—Available for FXO, FXS, FXS DID, and PRI ISDN cards.

  Use these options to configure voice ports as a member of a trunk group for the card.

- **Translation Profile**—Available for FXO, FXS, PRI ISDN, and FXS DID cards.

  Use these options to configure translation rules for calling and called numbers.

- **Station ID**—Available for FXO, FXS, and FXS DID cards.

  Use these options to configure the name and number for caller ID display.

- **Line Params**—Available for FXO, FXS, PRI ISDN, and FXS DID cards.

  Use these options to configure line parameters on the card for voice quality.

- **Tuning Params**—Available for FXO and FXS cards.

  Use these options to configure parameters for signaling between voice ports and another instrument.

- **Supervisory Disconnect**—Available for FXO cards.

  Use these options to configure parameters for supervisory disconnect events. These events provide an indication that a call has disconnected.

- **DID Timers**—Available for FXS DID cards.

  Use these options to configure timers for DID calls.

6. In the page that displays, configure as needed the options on the tabs as needed.

The tabs that are available depend on the voice port and call functionality policy option types that you selected.

- **Trunk Group** options—For a description of these options, see the "Trunk Group Options for Voice Ports" table.

  If any trunk groups are already configured for other voice cards, they appear in the trunk groups table on this page. To edit a configured trunk group, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the "Trunk Group Options for Voice Ports" table, and click **Save Changes**. To delete a trunk group, click **…**, and click its trash can icon.

  After you click **Save Trunk Group** when saving trunk group options, configure the priority for a trunk group by double-click the Priority field for a trunk group in the Trunk Group table, entering a priority number, and pressing **Enter** or clicking outside of the Priority field. Valid priority numbers are integers 1 through 64. The number you enter is the priority of the POTS dial peer in the trunk group for incoming and outgoing calls.

- Translation Profile options—For a description of these options, see the "Translation Profile Options for Calling and Called Numbers" table.

  After you click **Finish** when configuring translation profile options, perform these actions:

  a. Add another translation profile if needed. You can create up to two translation profiles for this endpoint.

  b. Click **Save Translation Profile**.

  c. For each translation profile that you create, double-click the dash (-) that displays in **Direction** column in the table of translation rules and select **Incoming** or **Outgoing** from the drop-down list that displays. The Incoming selection applies the corresponding translation rule to traffic

that is incoming to this endpoint. The Outgoing selection applies the corresponding translation rule to traffic that is outgoing from this endpoint.

- **Station ID** options—For a description of these options, see the "Station ID Options" table.
- **Line Params** options—For a description of these options, see the "Line Params Options" table.
- **Tuning Params** options—For a description of these options, see the "Tuning Params Options" table.
- **Supervisory Disconnect** options—For a description of these options, see the "Supervisory Disconnect Options" table.

  You can configure as many supervisory disconnect events as needed.
- **DID Timers** options—For a description of these options, see the "DID Timers Options" table

7. Click **Next**
8. In **Policy Profile Name**, enter a name for this child policy.
9. In **Policy Profile Description**, enter a description for this child policy.
10. Click **Save**.

Configure POTS Dial Peers for a Voice Policy

When you configure POTS Dial Peers for a voice policy, you configure options that define how the system augments and manipulates calls for the POTS dial peer endpoint type.

You can configure the following options:

- **Trunk Groups**—The following table describes these options.

Table 177: Trunk Group Options for POTS Dial Peers

Option	Description	Cisco IOS CLI Equivalent
Add New Trunk Group	Click to add a trunk group for the selected card. You can add one trunk group for a voice port.	—

Option	Description	Cisco IOS CLI Equivalent
Copy from Existing	Click to copy an existing trunk group to a new trunk group. In the box that appears, change the name if desired, select a trunk group, and click **Copy**. A trunk group name whose name is preceded with "{Master}" is already associated with this voice policy. When you copy a this type of trunk group, the system reuses the existing trunk group without creating another instance of the trunk group definition. In this case, you cannot change the name.	—
Name	Name of the trunk group. The name can contain up to 32 characters.	**trunk group** *name*

Option	Description	Cisco IOS CLI Equivalent
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle** [**both** | **even** | **odd**] **hunt-scheme least-used** [**both** | **even** | **odd**] **hunt-scheme longest-idle** [**both** | **even** | **odd**] **hunt-scheme round-robin** [**both** | **even** | **odd**] **hunt-scheme sequential** [**both** | **even** | **odd**] **hunt-scheme random**

Option	Description	Cisco IOS CLI Equivalent
	Select the hunt scheme in the trunk group for outgoing calls: • **least-idle both**—Searches for an idle channel with the shortest idle time • **least-idle even**—Searches for an idle even-numbered channel with the shortest idle time • **least-idle odd**—Searches for an idle odd-numbered channel with the shortest idle time • **least-used both**—Searches for a trunk group member that has the highest number of available channels (applies to only PRI ISDN cards) • **least-used even**—Searches for a trunk group member that has the highest number of available even-numbered channels (applies only to PRI ISDN cards) • **least-used odd**—Searches for a trunk group member that has the highest number of available odd-numbered channels (applies only to PRI ISDN cards) • **longest-idle both**—Searches for an idle odd-numbered channel with the longest idle time • **longest-idle even**—Searches for an idle channel that has the highest number of available even-numbered channels • **longest-idle odd**—Searches for an idle channel that has the highest number of available odd-numbered channels • **round-robin both**—Searches trunk group members in turn for an idle channel, starting with the trunk group member that follows the last used member • **round-robin even**—Searches trunk group member in turn for an idle even-numbered channel, starting with	

Option	Description	Cisco IOS CLI Equivalent
	the trunk group member that follows the last used member • **round-robin odd**—Searches trunk group member in turn for an idle odd-numbered channel, starting with the trunk group member that follows the last used member • **sequential-both**—Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-even**—Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-odd**—Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **random**—Searches for a trunk group member at random and selects a channel from the member at random Default: **least-used both**	
Max Calls	Enter the maximum number of calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of calls. If the maximum number of calls is reached, the trunk group becomes unavailable for more calls. • **In field**—Enter the maximum number of incoming calls that are allowed for this trunk group. • **Out field**— Enter the maximum number of outgoing calls that are allowed for this trunk group. Valid range for both fields: integers 0 through 1000.	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]

Option	Description	Cisco IOS CLI Equivalent
Max-Retry	Select the maximum number of outgoing call attempts that the trunk group makes if an outgoing call fails. If you do not enter a value and a call fails, the system does not attempt to make the call again. Valid range: integers 1 through 5.	**trunk group** *name* **max-retry** *attempts*

- **Translation Profiles**—The following table describes these options.

Table 178: Translation Profile Options for POTS Dial Peers

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected POTS dial peer. You can create up to two translation profiles for this endpoint.	—
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	—
Name	Name of the translation profile. The name can contain up to 32 characters.	**voice translation-profile** *name*
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence /match-pattern/ / replace-pattern/* Reject Rule: **rule** *precedence* **reject** */match-pattern/*

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation Rules CSV File. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the **Action** drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string.	

Option	Description	Cisco IOS CLI Equivalent
	To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. **8.** Click **Save**. **9.** Add more translation rules as needed. **10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file. **11.** Click **Finish** at the bottom of the pane.	

To configure POTS dial peers for a voice policy:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**
2. Click **Add Voice Policy**, and choose **POTS Dial Peer** in the left pane.
3. From the **Add POTS Dial Peer Policy Profile** drop-down list, select **Create New**.

   Alternatively, you can select **Copy from Existing** to copy an existing POTS dial peer policy to a new one. In the box that appears, select the name of the policy profile to copy, enter a new name for the profile if desired, and click **Copy**.
4. Select the types of POTS dial peers that you that you want to configure from the list of options that displays, and click **next**.

   Options are **Trunk Group** (beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a) and **Translation Profile**.
5. To configure trunk groups, perform the following actions.

   If any trunk groups are already configured, they appear in the trunk groups table on this page. To edit a configured trunk group, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the "Trunk Groups for POTS Dial Peers Options" table, and click **Save Changes**. To delete a trunk group, click **…**, and click its trash can icon.

   a. Configure trunk group options as described in the "Trunk Groups Options for POTS Dial Peers " table.

   b. Add another trunk group if needed.

      You can create up to 64 trunk groups for this endpoint.

   c. Click **Save Trunk Group**.

d. Configure the priority for a trunk group by double-click the Priority field for a trunk group in the Trunk Group table, entering a priority number, and pressing **Enter** or clicking outside of the Priority field. Valid priority numbers are integers 1 through 64. Repeat this process for the other trunk groups in the table. The number you enter is the priority of the POTS dial peer in the trunk group for incoming and outgoing calls.

6. To configure translation profiles, perform these actions:

a. Configure translation profile options as described in the "Translation Profile Options for POTS Dial Peers" table.

b. Add another translation profile if needed.

You can create up to two translation profiles for this endpoint.

c. Click **Save Translation Profile**.

d. For each translation profile that you create, double-click the dash (-) that displays in **Direction** column in the table of translation rules and select **Incoming** or **Outgoing** from the drop-down list that displays.

The Incoming selection applies the corresponding translation rule to traffic that is incoming to this endpoint. The Outgoing selection applies the corresponding translation rule to traffic that is outgoing from this endpoint.

7. Click **Next**.

8. In **Policy Profile Name**, enter a name for this child policy.

9. In **Policy Profile Description**, enter a description for this child policy.

10. Click **Save**.

Configure SIP Dial Peers for a Voice Policy

When you configure SIP Dial Peers for a voice policy, you configure options that define how the system augments and manipulates calls for the SIP dial peer endpoint type.

You can configure the following options, depending on the policy type for which you are configuring SIP dial peers:

- **Translation Profiles**—Use these options to configure translation rules for called and calling numbers on SIP dial peers. The following table describes these options.

Table 179: Translation Profile Options for Calling Numbers on SIP Dial Peers

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected SIP dial peer. You can create up to two translation profiles for this endpoint.	**voice translation-profile** *name*

Option	Description	Cisco IOS CLI Equivalent
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	—
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence* /*match-pattern*/ / *replace-pattern*/ Reject Rule: **rule** *precedence* **reject** /*match-pattern*/

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation Rules CSV File. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the Action drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string.	

Option	Description	Cisco IOS CLI Equivalent
	To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. **8.** Click **Save**. **9.** Add more translation rules as needed. **10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file. **11.** Click **Finish** at the bottom of the pane.	

- **Media Profiles**—Use these options to configure codecs to be available for the SIP trunk communication with remote dial peers and DTMF relay options to use for SIP calls. The following table describes these options.

Table 180: Media Profile Options

Option	Description	Cisco IOS CLI Equivalent
Add New Media Profile	Click to add a translation profile for the dial peer.	—
Copy from Existing	Click to copy an existing media profile to a new media profile. In the box that appears, enter a media profile number for the profile, and click **Copy**.	—
Media Profile Number	Enter a number for this SIP media profile. Valid range: Integers 1 through 10000.	**voice class codec** *tag-number*
Codec	Move from the Source list to the Target list the codecs that you want to be made available for the SIP trunk to use when communicating with the remote dial peer. Codecs in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them.	**voice class codec** *tag-number* **codec preference** *value codec-type*

Option	Description	Cisco IOS CLI Equivalent
DTMF	Move from the Source list to the Target list the DTMF relay options that you want the system to use for SIP calls. Items in the Target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them. If you want to include the **Inband** option in the Target list, it can be the only option in that list. If you want to include other options in the Target list, move the Inband option to the Source list before saving the media profile.	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Save	Click to save the configuration settings that you made.	—

- **Modem Pass-through**—Use these options to configure the modem pass-through feature for a SIP dial peer endpoint. The following table describes these options.

Table 181: Modem Pass-Through Options

Option	Description	Cisco IOS CLI Equivalent
Add New Modem Pass-through	Click to add a modem pass-through for this SIP dial peer endpoint.	—
Copy from Existing	Click to copy an existing modem pass-through to a new modem pass-through profile. In the box that appears, select an existing modem pass-through, enter new name if desired, and click **Copy**.	—
Name	Name of the modem pass-through. This name is used when you copy an existing modem pass-through profile to a new one.	—

Option	Description	Cisco IOS CLI Equivalent
Protocol	Select the protocol for the modem pass-through: • **None**—Modem pass-through is disabled on the device • **NSE G.711ulaw**—Uses named signaling events (NSEs) to communicate G.711ulaw codec switchover between gateways • **NSE G.711alaw**—Uses named signaling events (NSEs) to communicate G.711alaw codec switchover between gateways	None: **no modem passthrough** NSE G.711 ulaw: **modem passthrough nse codec g711ulaw** NSE G.711 alaw: **modem passthrough nse codec g711alaw**
Save Modem Pass-Through	Click to save the configuration settings that you made.	—

- **Fax Protocol**—Use these options to configure the fax protocol capability for a SIP dial peer endpoint. The following table describes these options.

Table 182: Fax Protocol Options

Option	Description	Cisco IOS CLI Equivalent
Add New Fax Protocol	Click to add a fax protocol for the dial peer.	—
Copy from Existing	Click to copy an existing fax protocol to a new fax protocol. In the box that appears, select an existing fax protocol, enter new name if desired, and click **Copy**.	—
Name	Name of the fax protocol. This name is used when you copy an existing fax profile to a new fax profile.	—

Option	Description	Cisco IOS CLI Equivalent

Primary	Select from a set of fax protocol options. Each option is a bundled set of related fax commands.
	For a detailed description of each bundle, see the “Primary Fax Protocol Command Bundles” table
	The descriptions of the bundles include the following components:
	• **nse**—Uses NSEs to switch to T.38 fax relay mode
	• **force**—Unconditionally uses Cisco Network Services Engines (NSE) to switch to T.38 fax relay
	• **version**—Specifies a version for configuring fax speed:
	  • **0**—Configures version 0, which uses T.38 version 0 (1998–G3 faxing)
	  • **3**—Configures version 3, which uses T.38 version 3 (2004–V.34 or SG3 faxing)
	• **none**—No fax pass-through or T.38 fax relay is attempted
	• **Pass-through**—The fax stream uses one of the following high-bandwidth codecs:
	  • **g711ulaw**—Uses the G.711 ulaw codec
	  • **g711alaw**—Uses the G.711 alaw codec
		fax protocol { **none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**]| **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}

Fallback	Available when the primary protocol bundle name that you selected in the Primary field begins with “T.38” or with “Fax Pass-through.” Select the fallback mode for fax transmissions. This fallback mode is used if the primary fax protocol cannot be negotiated between device endpoints. For a detailed description of each option, see the "Fallback Protocol Options” table.	**fax protocol** {none | pass-through {g711ulaw | g711alaw} [**fallback none**] | t38 [nse [force]] [version {0 | 3}] [ls-redundancy value [hs-redundancy value]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}

Option	Description	Cisco IOS CLI Equivalent
Low Speed	Available when the primary protocol bundle name that you selected in the Primary field begins with "T.38." Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range: varies from 0 (no redundancy) to 5. Default: 0.	**ls-redundancy** *value*
High Speed	Available when the primary protocol bundle name that you selected in the Primary field begins with "T.38." Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range: varies from 0 (no redundancy) to 2. Default: 0	**hs-redundancy** *value*
Save Fax Protocol	Click to save the configuration settings that you made.	—

The following table describes the bundled sets of fax commands that are available for the Primary option when you configure the fax protocol capability for a SIP dial peer endpoint.

For low speed (ls) redundancy, the range varies from 0 (no redundancy) to 5. For high speed (HS redundancy, the range varies from 0 (no redundancy) to 2.

Table 183: Primary Fax Protocol Command Bundles

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 3	Primary fax protocol is T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3** **ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0	Primary fax protocol is T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0** **ls-redundancy** *value* **hs-redundancy** *value*

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 3 NSE	Primary fax protocol is NSE based T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3 nse ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 3 NSE force	Primary fax protocol is NSE force option of T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3 nse force ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0 NSE	Primary fax protocol is NSE option of T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 0 NSE force	Primary fax protocol is NSE force option of T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 0 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE force No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 0 Rate 14.4 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 NSE Rate 14.4 No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 NSE force Rate 14.4 No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 Rate 9.6 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax Relay Version 0 NSE Rate 9.6 No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax Relay Version 0 NSE force Rate 9.6 No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 0 Rate 14.4	Primary fax protocol is T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 NSE Rate 14.4	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 NSE force Rate 14.4	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 Rate 9.6	Primary fax protocol is T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax Relay Version 0 NSE Rate 9.6	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax Relay Version 0 NSE force Rate 9.6	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
None	Fax protocol is disabled.	**fax protocol none**
Fax Pass-through G711ulaw	Primary fax protocol is fax pass-through with pass-through codec set to g711ulaw.	**fax protocol pass-through g711ulaw**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
Fax Pass-through G711ulaw No ECM	Primary fax protocol is fax pass-through with pass-through codec set to g711ulaw and ECM disabled.	**fax protocol pass-through g711ulaw** **fax-relay ecm disable**
Fax Pass-through G711alaw	Primary fax protocol is fax pass-through with pass-through codec set to g711alaw.	**fax protocol pass-through g711alaw**
Fax Pass-through G711alaw No ECM	Primary fax protocol is fax pass-through with pass-through codec set to g711alaw and ECM disabled.	**fax protocol pass-through g711alaw** **fax-relay ecm disable**

The following table describes the selections that are available for the Fallback option when you configure the fax protocol capability for a SIP dial peer endpoint.

Table 184: Fallback Protocol Options

Fallback Fax Protocol Options	Description	Cisco IOS CLI Equivalent
None	Fallback Fax Protocol is None. All special fax handling is disabled.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback none** **fax protocol pass-through** {**g711ulaw** | **g711alaw** } **fallback none**
Fax Pass-through G711ulaw	Fallback Fax Protocol is Fax Pass-through with pass-through codec set to g711ulaw.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711ulaw**
Fax Pass-through G711alaw	Fallback Fax Protocol is Fax Pass-through with pass-through codec set to g711alaw.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711alaw**

To configure SIP dial peers for a voice policy:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.
2. Click **SIP Dial Peer**.
3. From the **Add SIP Dial Peer Policy Profile** drop-down list, choose **Create New**.

   Alternatively, you can select **Copy from Existing** to copy an existing SIP dial peer policy to a new one. In the box that appears, select the name of the policy profile to copy, enter a new name for the profile if desired, and click **Copy**.
4. Select the policy types that you want to create and click **Next**:

- **Translation Profile**—Lets you configure translation rules for calling and called numbers.
- **Media Profile**—Lets you configure codecs to be available for the SIPtrunk communication with remote dial peers and DTMF relay options to use for SIP calls.
- **Modem Pass-through**—Lets you configure the modem pass-through feature for a SIP dial peer endpoint.
- **Fax Protocol**—Lets you lets you configure the fax protocol capability for a SIP dial peer endpoint. This capability is advertised and used when negotiating capabilities with the remote dial peer.

5. In the page that displays, configure options in the tabs that the following tables describe as needed.

   The tabs that are available depend on the policy types that you selected.

   - **Translation Profile** options—For a description of these options, see the "Translation Profile Options for Calling Numbers on SIP Dial Peers" table.

     After you click **Finish** when configuring a translation profile, perform these actions:

     a. Add another translation profile if needed. You can create up to two translation profiles for this endpoint.

     b. Click **Save Translation Profile**.

     c. For each translation profile that you create, double-click the dash (-) that displays in **Direction** column in the table of translation rules and select **Incoming** or **Outgoing** from the drop-down list that displays. The Incoming selection applies the corresponding translation rule to traffic that is incoming to this endpoint. The Outgoing selection applies the corresponding translation rule to traffic that is outgoing from this endpoint.

   - **Media Profile** options—For a description of these options, see the "Media Profile Options" table.
   - **Modem Pass-through** options—For a description of these options, see the "Modem Pass-Through Options" table.
   - **Fax Protocol** options—For a description of these options, see the "Fax Protocol Options" table.

6. Click **Next**.
7. In **Policy Profile Name**, enter a name for this child policy.
8. In **Policy Profile Description**, enter a description for this child policy.
9. Click **Save**.

Configure SRST Phones for a Voice Policy

When you configure SRST Phones for a voice policy, you configure options that define how the system augments and manipulates calls for the Cisco Unified SRST phone endpoint type.

The following table describes options for configuring SRST phones for a voice policy.

Table 185: SRST Phones Configuration Options

Option	Description	Cisco IOS CLI Equivalent
Medial Profile Number	Enter a number for this Cisco Unified SRST media profile. Valid range: Integers 1 through 10000.	**voice class codec** *tag-number*
Codec	Move from the Source list to the Target list the codecs that you want to be available for phones when they are in Cisco Unified SRST mode and communicating with other phones that are in the same site and registered to the same gateway. Codecs in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them.	**voice class codec** *tag-number* **codec preference** *value codec-type*
DTMF field	Move from the source list to the target list the DTMF relay options that you want the system to use when in Cisco Unified SRST mode. Items in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them. If you want to include the **Inband** option in the Target list, it can be the only option in that list. If you want to include other options in the Target list, move the Inband option to the Source list before saving the media profile.	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Save	Click to save the configuration settings that you made.	—

To configure SRST phones for a voice policy, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**
2. Click **Add Voice Policy**, and choose **SRST Phone**.
3. From the **Add SRST Phone Policy Profile** drop-down list, select **Create New**.

   Alternatively, you can select **Copy from Existing** to copy an existing policy to a new one. In the box that appears, select the name of the policy profile to copy, enter a new name for the profile if desired, and click **Copy**.
4. Click **Media Profile**, and click **Next**.
5. Click **Add New Media Profile**.

6. In the page that displays, configure options as described in the "SRST Phones Configuration Options" table.
7. Click **Next**.
8. In **Policy Profile Name**, enter a name for this child policy.
9. In **Policy Profile Description**, enter a description for this child policy.
10. Click **Save**.

Provision a Device Template for Unified Communications

When you provision a device template for Unified Communications, you select UC-specific feature templates and set up the voice policy to include with the device template.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of supported device to which you want to attach the UC-specific feature templates and map the voice policy.
5. Click **Unified Communications**.
6. To select UC-specific feature templates to include with the device template, perform these actions:
   a. From the **Voice Card** drop-down list, select the voice card feature template that you want to attach to the device.
   b. From the **Call Routing** drop-down list, select the call routing feature template that you want to attach to the device.
   c. From the **SRST** drop-down list, select the SRST feature template that you want to attach to the device.
   d. From the **DSPFarm** drop-down list, select the DSPFarm template that you want to attach to the device.
7. To set up the voice policy to include with the device template, perform these actions:
   a. From the **Voice Policy** drop-down list, select the voice policy that you want to map to endpoints.
   b. Click **Mapping**.
   c. From the list of endpoint types in the left pane of the screen that displays, select the type of endpoint that contains the subpolicies that you want to map to specific endpoints.
   d. From the list of subpolicies that displays, click **…**, and click **Mapping** for the subpolicy that you want to map to specific endpoints.
   e. In the list of endpoints that displays, select each endpoint to which you want to map the subpolicy.
   f. Click **Map**.

g. Click **Save**.

8. To create the device template, click **Create**.

When you map subpolicies to endpoints, the system generates the CLI commands that the following table shows.

Table 186: Generated CLI Commands for Subpolicies to Endpoints Mapping

Endpoint	Subpolicy	Cisco IOS CLI Application Mapping	Remarks
Voice Port FXO Voice Port FXS Voice Port FXS DID Voice Port PRI ISDN POTS Dial Peer SIP Dial Peer	Translation profile	**translation-profile incoming** *profile-name* **translation-profile outgoing** *profile-name*	A translation profile policy is applied to a dial peer or a voice profile.
SRST Phone SIP Dial Peer	Media profile	voice register pool *number* **voice-class codec** *number* **dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}	A media profile policy includes voice class codec and DTMF relay configurations. This policy is applied to an incoming SIP dial peer, an outgoing SIP dial peer, or an SRST phone profile.
Voice Port FXO	Supervisory disconnect	voice port *number* **supervisory custom-cptone** *cptone-name* **supervisory dualtone-detect=params** *tag*	A supervisory disconnect policiy such as custom-cptone or dualtone-detect-params is applied to FXO voice interfaces.

Endpoint	Subpolicy	Cisco IOS CLI Application Mapping	Remarks
Voice Port FXO Voice Port FXS Voice Port FXS DID Voice Port PRI ISDN POTS Dial Peer	Trunk group	**trunk-group name** [*preference-num*] **voice-port** *number trunk-group name* [*preference-num*] **interface serial** *slot*/*sub-slot*/**port:**{**15** | **23**} **dial-peer voice** *tag* **pots** **trunkgroup name** *preference-num*	If more than one interface is assigned to the same trunk group, the *preference-num* value determines the order in which the trunk group uses the interfaces. A preference-num value of 1 is the highest preference, so an interface with that value is used first. A value of 64 is the lowest preference so an interface with that value is used last.
SIP Dial Peer	Modem pass-through	None: **no modem passthrough** G.711 ulaw: **modem passthrough nse codec g711ulaw** G.711 alaw: **modem passthrough nse codec g711alaw**	—
SIP Dial Peer	Fax protocol	**fax protocol** {**none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**] | **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}	—

Monitoring UC Operations

After you enable UC voice services for supported routers, you can monitor the real-time statuses of lines, calls, interfaces, and related items that a device processes.

To monitor UC operations:

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

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. In the table of devices, select the device for which you want to monitor UC operations.
3. From **Security Monitoring**, click **Real Time**.
4. In **Device Options**, select one of these options:
    - **Voice Calls**—Displays information for active voice calls. See the "Voice Call Monitoring Information" table.
    - **Voice VOIP Calls**—Displays information for active VOIP calls. See the "Voice VoIP Calls Monitoring Information" table.
    - **Voice Phone Info**—Displays information about Cisco Unified SRST registrations. See the "Voice Phone Info Monitoring Information" table.
    - **Voice Controller T1 E1 Current 15 mins Stats**—Displays configuration and status information for the T1/E1 voice module that is installed in the device, compiled over the past 15 minutes. See the "Voice Controller T1 E1 Current 15 Mins Stats Monitoring Information" table.
    - **Voice Controller T1 E1 Total Stats**—Displays configuration and status information for the T1/E1 voice module that is installed in the device, compiled since the module last started. See the "Voice Controller T1 E1 Total Stats" table.
    - **Voice ISDN Status**—Displays information about Layer 1 and Layer 2 status for the ISDN controller, and information about active calls. "See the Voice ISDN Status Information table".
    - **Voice DSPFarm SCCP CUCM Groups**—Displays detailed information about Cisco Unified Communications Manager groups that are configured for DSP farm services on a device. See the "Voice DSPFarm SCCP CUCM Groups" table.
    - **Voice DSPFarm Profile**—Displays detailed information about DSP farm service profiles and media resources that are configured on the device. See the "Voice DSPFarm Profile Monitoring Information" table.
    - **Voice DSP Farm SCCP Connections**—Displays detailed information about SCCP connections between the device and Cisco Unified Communications Manager. See the "Voice DSPFarm SCCP Connections" table.
    - **Voice DSPFarm Active**—Displays operational and status information about DSP farm resources that are active on the device. See the "Voice DSPFarm Active" table.

    You also can monitor operations that include UC operations by selecting the following options:
    - **Interface Detail**—Displays status and statistical information for interfaces that are configured for the router.
    - **Interface Statistics**—Displays statistical information for interfaces that are configured for the router
    - **Interface T1/E1**—Displays information for the T1/E1 voice module that is installed in the device

The following table describes the information that you see when you monitor voice calls.

Table 187: Voice Calls Monitoring Information

Field	Description
Call ID	System assigned identifier of a telephony call leg
Voice Port	Voice port used for the call
Codec	Negotiated codec used for the call
VAD	Indicates whether VAD is enabled or disabled for the call
DSP Cannel	DSP channel used for the call
DSP Type	Type of DSP used for the call
Aborted Packets	Number of packets aborted during the call
TX Packets	Number of packets transmitted during the call
RX Packets	Number of packets received during the call
Last Updated	Date and time when the information on this page was last updated

The following table describes the information that you see when you monitor voice VoIP calls.

Table 188: Voice VoIP Calls Monitoring Information

Field	Description
Call ID	System assigned identifier of an RTP connection for a call leg
Codec	Negotiated codec used for the call
Destination Address	IP address of the destination of the call
Destination Port	RTP port of the destination of the call
TX Packets	Number of packets transmitted during the call
RX Packets	Number of packets received during the call
Duration (ms)	Duration of the call, in milliseconds
Last Updated	Date and time when the information on this page was last updated

The following table describes the information that you see when you monitor voice phone information.

Table 189: Voice Phone Info Monitoring Information

Field	Description
Pool Tag	Tag number that is assigned to the Cisco Unified SRST phone pool on the device

Field	Description
ID Network	Identifier of the network subnet that the device uses to register phones that fallback from Cisco Unified Communications Manager to this device
Registration State	Indicates whether phones that are in Cisco Unified SRST mode are registered to this device
Dialpeer Tag	System assigned tag used by the dial peer that is assigned to the directory number of phones that are in Cisco Unified SRST mode and are registered to this device
Address	IP address of the device interface that is used for SIP SRST call control when phones fail over
Directory Number	Directory number of each phone that is in Cisco Unified SRST mode
Last Updated	Date and time when the information on this page was last updated

The following table describes the information that you see when you monitor voice controller T1/E1 information for the past 15 minutes.

Table 190: Voice Controller T1 E1 Current 15 Mins Stats Monitoring Information

Field	Description
Interface-slot-num	Slot number of the controller.
Insterface-subslot-num	Subslot number of the controller.
Interface-port-num	Port number of the controller.
Status	Status of the controller.
Type	Type of the controller.
Clock Source	Clock source used for the controller.
Line Code Violations	Number line code violations that have occurred.
Path Code Violations	Number path code violations that have occurred.
Slip Seconds	Number of slip seconds that have occurred. A slip can occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Frame Loss Seconds	Number of seconds in which out of frame (OOF) errors have occurred.
Line Err. seconds	Number of seconds in which Line Errored Seconds (LES) have occurred. A LES is a second in which one or more Line Code Violation errors are detected.

Field	Description
Degraded Minutes	Number of Degraded Minutes that have occurred. A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Seconds	Number of Errored Seconds that have occurred.
Bursty Errored Seconds	Number of Bursty Error Seconds that have occurred. A Bursty Error Second is a second with less than 320 and more than 1 path coding violation errors, no severely errored frame defects, and no detected incoming AIS defects.
Severely Errored Seconds	Number of Severely Errored Seconds that have occurred.
Unavailable Seconds	Number of Unavailable Seconds that have occurred. This value is calculated by counting the number of seconds that the interface is unavailable.
Last Updated	Date and time when the information on this page was last updated.

The following table describes the information that you see when you monitor voice controller T1/E1 information over the period since a device last started.

Table 191: Voice Controller T1 E1 Total Stats

Field	Description
Interface-slot-num	Slot number of the controller.
Insterface-subslot-num	Subslot number of the controller.
Interface-port-num	Port number of the controller.
Status	Status of the controller.
Type	Type of the controller.
Clock Source	Clock source used for the controller.
Line Code Violations	Number line code violations that have occurred.
Path Code Violations	Number path code violations that have occurred.
Slip Seconds	Number of slip seconds that have occurred. A slip can occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Frame Loss Seconds	Number of seconds in which out of frame (OOF) errors have occurred
Line Err. seconds	Number of seconds in which Line Errored Seconds (LES) have occurred. A LES is a second in which one or more Line Code Violation errors are detected.

Field	Description
Degraded Minutes	Number of Degraded Minutes that have occurred. A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Seconds	Number of Errored Seconds that have occurred.
Bursty Errored Seconds	Number of Bursty Error Seconds that have occurred. A Bursty Error Second is a second with less than 320 and more than 1 path coding violation errors, no severely errored frame defects, and no detected incoming AIS defects.
Severely Errored Seconds	Number of Severely Errored Seconds that have occurred.
Unavailable Seconds	Number of Unavailable Seconds that have occurred. This value is calculated by counting the number of seconds that the interface is unavailable.
Last Updated	Date and time when the information on this page was last updated.

The following table describes the information that you see when you monitor voice ISDN status.

Table 192: Voice ISDN Status Information

Field	Description
Key ID	Identifier of the table row
Interface	Name of the PRI ISDN digital interface
Switch Type	Switch type used for the PRI ISDN digital interface
Layer 1 Status	Layer 1 status of the PRI ISDN digital interface
Layer 2 Status	Layer 2 status of the PRI ISDN digital interface
Active Calls	Number of active calls on the PRI ISDN digital interface
Last Updated	Date and time when the information on this page was last updated

The following table describes the information that you see when you monitor Cisco Unified Communications Manager groups that are configured for DSP farm services on a device.

Table 193: Voice DSPFarm SCCP CUCM Groups Monitoring Information

Field	Description
CUCM Group ID	Identifier of the Cisco Unified Communications Manager group
Description	Description of the Cisco Unified Communications Manager group
Switchover Method	Method that the primary Cisco Unified Communications Manager server in this Cisco Unified Communications Manager group uses for failover

Field	Description
Switchback Method	Method that the secondary Cisco Unified Communications Manager server in this Cisco Unified Communications Manager group uses to switch back after a failover
CUCM ID	Identifier of each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
CUCM Priority	Priority in which the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group are used
Profile ID	Identifier of the DSP farm profile that is registered to each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
Reg. Name	Name of the DSP farm profile that is registered to each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
Last Updated	Date and time when the information on this page was last updated

The following table describes the information that you see when you monitor DSP farm service profiles and media resources that are configured on a device.

Table 194: Voice DSPFarm Profile Monitoring Information

Field	Description
Profile ID	Identifier of the DSP farm profile.
Service ID	Type of DSP farm service that is configured for this DSP farm profile.
Service Mode	Service mode for this DSP farm profile.
Resource ID	Resource identifier for the DSP resource group in this DSP farm profile.
Admin	Status of this DSP farm profile. If this field displays DOWN, ensure that the Shutdown option is not enabled in the Profile tab of the DSPFarm feature template that defines this DSP farm.
Operation	Status of the registration of the profile with Cisco Unified Communications Manager: • ACTIVE IN PROGRESS—Profile is in the process of registering with Cisco Unified Communications Manager • DOWN—Profile is unable to register with Cisco Unified Communications Manager • ACTIVE— Profile is registered with Cisco Unified Communications Manager

Field	Description
App. Type	Type of application with which the DSP farm services that are provisioned on the device are associated.
App. Status	Status of the association of this profile with Cisco Unified Communications Manager: • app-assoc-done—Profile is associated with Cisco Unified Communications Manager • app-assoc-not-done—Profile is not associated with Cisco Unified Communications Manager
Resource Provider	Information about the mediaresource family that relates to the profile.
Provider Status	Status of the media resources that relate to the profile.
Last Updated	Date and time when the information on this page was last updated.

The following table describes the information that you see when you monitor SCCP connections between a device and Cisco Unified Communications Manager.

Table 195: Voice DSPFarm SCCP Connections

Field	Description
Connection ID	Identifier of an SCCP connection for an active call that uses this DSP farm service
Session ID	Identifier of an SCCP session for an active call that uses this DSP farm service
Session Type	Type of DSP farm service for this SCCP connection
Mode	Mode for direction of traffic for this SCCP connection
Codec	Codec provisioned for this SCCP connection
Remote IP	IP address of the remote endpoint for this SCCP connection
Remote Port	Port number of the remote endpoint for this SCCP connection
Source Port	Port number of the local endpoint for this SCCP connection
Last Updated	Date and time when the information on this page was last updated

The following table describes the information that you see when you monitor DSP farm resources that are active on a device.

Table 196: Voice DSPFarm Active Monitoring Information

Field	Description
DSP	Identifier of the DSP for an active call that uses this DSP farm service

Field	Description
Status	Status of the DSP for an active call that uses this DSP farm service
Resource ID	Resource Identifier that is associated with the DSP that this connection uses
Bridge ID	Bridge Identifier that is associated with the DSP that this connection uses
Transmit Packets	Number of packets that this connection has transmitted
Received Packets	Number of packets that this connection has received
Last Updated	Date and time when the information on this page was last updated

Configure the Unified Threat Defense Resource Profiles Using Cisco SD-WAN Manager

Table 197: Feature History

Feature Name	Release Information	Description
Configure Unified Threat Defense Resource Profiles	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure Unified Threat Defense Resource Profiles using Cisco SD-WAN Manager.

You can configure the Unified Threat Defense resource profiles using Cisco Catalyst SD-WAN Manager by doing the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device(s).
4. Click **Security App Hosting**.
5. Enter a template name and description.
6. Choose whether to enable or disable NAT. NAT is enabled by default.

   To use Unified Threat Defense features that connect to the internet, you must enable NAT. For example, URL Filtering and Advanced Malware Protection connect to the internet to perform Cloud lookups. To use these features, enable NAT.
7. To download the URL database on the device, choose **Yes**.

8. To deploy more instances of Snort, choose one of the following resource profiles:
   - **Low**: This is the default profile.
   - **Medium**.
   - **High**.

   When you specify a larger resource profile, the device deploys more Snort instances to increase throughput. The larger resource profiles also use more resources on the device. The number of Snort instances deployed by the device differs by platform and software release.
9. Click **Save**.
10. Add this template to the device template.
11. Attach the device template to the device.

Configure Unified Logging for Security Connection Events

Table 198: Feature History

Feature Name	Release Information	Description
Unified Logging for Security Connection Events	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature supports Unified Logging which is used to capture information about connection events across different security features at different stages during policy enablement and execution.

To configure Unified Logging for security connection events, perform the following steps:

1. Configure Localized Policy Using Cisco SD-WAN Manager.
2. Select the policy application check boxes for **Netflow** and **Application**. For information, see Configure Policy Settings.
3. Enable logging for a unified security policy. You can enable logging either at a rule level or at global level Configure Firewall and Unified Security Policy.

Note You can also use the CLI Add-on template for configure Unified Logging for security connection events. For more information, see Create a CLI Add-On Feature Template.

Configure Unified Security Policy

Table 199: Feature History

Feature Name	Release Information	Description
Unified Security Policy	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature lets you to configure a single unified security policy in which you specify both the firewall action and the UTD action in the same rule in the policy.
Resource Limitations and Device-global Configuration Options	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enables you to define resource limitation options such as idle timeout and session limits, and device-global options in the policy summary page to fine-tune a firewall policy behaviour after a firewall policy is implemented in Cisco Catalyst SD-WAN.
Security Logging Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature allows you to export UTD logs to an external syslog server and specify the source interface from which the UTD syslog originates.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.

Perform the following tasks to create a unified security policy:

- Create an Object Group
- Create an Advanced Inspection Profile
- Configure Firewall and Unified Security Policy
- Add a Zone Pair
- Apply a Security Policy to a Device

Configure Wireless Management on Cisco ISR 1000 Series Routers

Table 200: Feature History

Feature Name	Release Information	Description
Wireless Management on Cisco ISR 1000 Series Routers (supporting WiFi 5 WLAN module)	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to configure wireless LAN settings on WiFi 5-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager. With Cisco SD-WAN Manager, you can automate the wireless LAN controller configuration and provide wireless connectivity without the need for another external controller to configure and manage the wireless settings on the routers. This feature lets you to configure wireless LAN settings on Cisco 1000 Series Integrated Services Routers .
Wireless Management on Cisco ISR 1000 Series Routers (supporting WiFi 6 WLAN module)	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature lets you to configure wireless LAN settings on WiFi 6-capable Cisco 1000 Series Integrated Services Routers.

To configure and manage wireless settings on Cisco ISR 1000 Series Routers:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

4. In the left pane, from **Select Devices**, choose a Cisco ISR 1000 Series Router for which you are creating a template.
5. Under **OTHER TEMPLATES**, click **ISR1K Wireless** to select it as the feature template.
6. In the **Template Name** field, enter a name for the feature template.

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the **Description** field, enter a description for the feature template.

   This field is mandatory, and it can contain all characters and spaces.

8. Enter the Wi-Fi SSID details for setting up a wireless LAN:

Parameter Name	Description
Wireless Network Name (SSID)	Enter a name for the wireless SSID. It can be a string from 4 to 32 characters. The SSID must be unique.
VLAN (Range 1-4094)	Enter a VLAN ID for the wireless LAN traffic.
Security Type	Choose a security type: • **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server. • **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase. • **Open**: Choose this option to allow access to the wireless network without authentication.
RADIUS Server IP	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the IP address of the RADIUS server.
Authentication Port	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the authentication port number of the RADIUS server.
Shared Secret	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the shared secret key of the RADIUS server.
Passphrase	(Optional) This field is available if you choose the **WPA2 Personal** option as the security type. Set a pass phrase. This pass phrase provides users with access to the wireless network.
Admin State	Choose an admin state.

Parameter Name	Description
Radio Type	Choose one of the following radio types: • **2.4GHz** • **5GHz** • **Both**
Broadcast SSID	Choose **On** to broadcast the SSID. Choose **Off** if you do not want the SSID to be visible to all the wireless clients.
QoS Profile	Choose a QoS profile.

9. Enter the **General** details for the wireless LAN:

Parameter Name	Description
Country	Choose the country where the ISR is installed.
Username	Specify the username of Cisco Mobility Express. If you are using a C1131 Cisco IOS XE Catalyst SD-WAN device specify the username for the EWC.
Password	Specify the password for Cisco Mobility Express or the EWC.

10. Enter the **Advanced** details for the wireless LAN:

Parameter Name	Description
Controller IP Address	**Note** For Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and Cisco vManage Release 20.6.1 and earlier releases, this field is displayed as **ME IP Address.** Specify the Management IP address of Cisco Mobility Express or EWC.
Subnet Mask	Specify the subnet mask for the Management IP address.
Default Gateway	Specify the default gateway address of Cisco Mobility Express or EWC.
2.4GHz Shutdown	Click **Yes** to shut down the 2.4 GHz radio type. Click **No** to not shut down this radio type.
5GHz Shutdown	Click **Yes** to shut down the 5 GHz radio type. Click **No** to not shut down this radio type.

11. Click **Save** to save your wireless configuration.

Configure a Router as an NTP Primary

Table 201: Feature History

Feature Name	Release Information	Description
Configuring a Router as an NTP Primary	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can configure a router as an NTP primary router from the NTP template tab.

You can configure one or more supported routers as an NTP primary router in a Cisco Catalyst SD-WAN deployment. A router that is configured in this way acts as the NTP server to which other nodes in the deployment synchronize their clocks.

Configuring a router as an NTP primary router is useful if you do not have an NTP server in your deployment.

To configure a router as an NTP primary router, you create a template that includes configured parameters for the NTP primary router. To do so, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Perform either of these actions:
   - To create a new template, under **Feature Templates**, click **Add Template**, choose the type of device to be the NTP primary router, and then choose the **NTP** template in the group of **Basic Information** templates.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

   - To update an existing template, click **...**, and click **Edit**.

3. Configure options for the template as desired, and in the Master tab, perform these actions:
   a. For the Master option, choose **Global** from the drop-down list, and then choose **On**.
   b. (Optional) In the **Stratum** field, enter the stratum value for the NTP primary router.

      The stratum value defines the hierarchical distance of the router from its reference clock.

      Valid values: Integers 1 through 15. If you do not enter a value, the system uses the router internal clock default stratum value, which is 8.
   c. (Optional) In the **Source** field, enter the name of the exit interface for NTP communication.

      If configured, the system sends NTP traffic to this interface.

      For example, enter **GigabitEthernet1** or **Loopback0**.
4. Click **Save** (for a new template) or **Update** (for an existing template).

CLI equivalent:

```
ntp master [stratum-number]
ntp source source-interface
```

Configure Service Chaining

Here is the workflow for configuring service chaining for a device managed by Cisco Catalyst SD-WAN:

1. Service devices are accessed through a specific VRF. In the VPN template that corresponds to the VRF for a service device, configure service chaining, specifying the service type and device addresses. By default, the tracking feature adds each service device status update to the service log. You can disable this in the VPN template.
2. Attach the VPN template to the device template for the device managed by Cisco Catalyst SD-WAN.
3. Apply the device template to the device.

Configure Service Chaining Using Cisco SD-WAN Manager

To configure service chaining for a device.

1. In Cisco SD-WAN Manager, create a VPN template.
2. Click**Service**.
3. In the **Service** section, click **New Service** and configure the following:
   - **Service Type**: Select the type of service that the service device is providing.
   - **IP Address**: IP Address is the only working option.
   - **IPv4 Address**: Enter between one and four addresses for the device.
   - **Tracking**: Determines whether the periodic health updates of the service device are recorded in the system log. Default: On

Note Maximum number of services: 8

4. Click **Add**. The service appears in the table of configured services.

Configure Sessions in Cisco SD-WAN Manager

Table 202: Feature History

Feature History	Release Information	Description
Configure Sessions in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature lets you see all the HTTP sessions that are open within Cisco SD-WAN Manager. It gives you details about the username, source IP address, domain of the user, and other information. A user with User Management Write access, or a netadmin user can trigger a log out of any suspicious user's session.

Set a Client Session Timeout in Cisco SD-WAN Manager

You can set a client session timeout in Cisco SD-WAN Manager. When a timeout is set, such as no keyboard or keystroke activity, the client is automatically logged out of the system.

Note You can edit Client Session Timeout in a multitenant environment only if you have a Provider access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Client Session Timeout**.
3. Click **Edit**.
4. Click **Enabled**.
5. Specify the timeout value, in minutes.
6. Click **Save**.

Set a Session Lifetime in Cisco SD-WAN Manager

You can specify how long to keep your session active by setting the session lifetime, in minutes. A session lifetime indicates the amount of time for which a session can be active. If you keep a session active without letting the session expire, you will be logged out of the session in 24 hours, which is the default session timeout value.

The default session lifetime is 1440 minutes or 24 hours.

Note You can edit Session Lifetime in a multitenant environment only if you have a Provider access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Session Life Time**.
3. Click **Edit**.
4. In the **SessionLifeTime** field, specify the session timeout value, in minutes, from the drop-down list.
5. Click **Save**.

Set the Server Session Timeout in Cisco SD-WAN Manager

You can configure the server session timeout in Cisco SD-WAN Manager. The server session timeout indicates how long the server should keep a session running before it expires due to inactivity. The default server session timeout is 30 minutes.

Note Server Session Timeout is not available in a multitenant environment even if you have a Provider access or a Tenant access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Server Session Timeout**.
3. Click **Edit**.
4. In the **Timeout(minutes)** field, specify the timeout value, in minutes.
5. Click **Save**.

Enable Maximum Sessions Per User

You can enable the maximum number of concurrent HTTP sessions allowed per username. If you enter 2 as the value, you can only open two concurrent HTTP sessions. If you try to open a third HTTP session with the same username, the third session is granted access, and the oldest session is logged out.

Note Maximum Session Per User is not available in a multitenant environment even if you have a Provider access or a Tenant access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Max Sessions Per User**.
3. Click **Edit**.
4. Click **Enabled**.

   By default, **Max Sessions Per User**, is set to **Disabled**.
5. In the **Max Sessions Per User** field, specify a value for the maximum number of user sessions.
6. Click **Save**.

Configure Security Dashboard

Security

The following dashlets and options are available on the **Monitor** > **Security** page in Cisco SD-WAN Manager:

Note In Cisco vManage Release 20.6.x and earlier releases, these options and dashlets are part of the **Dashboard** > **Security** page.

- **Actions**
- **Top Threats** (Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases)
- **Firewall Rule Counter**

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases, **Firewall Enforcement** has been renamed to **Firewall Rule Counter**

- **URL Filtering**
- **Advanced Malware Protection**
- **Intrusion Prevention** (Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases)
- **SecurityEvents** (Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases)
- **SecureInternet Gateway Tunnels** (Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases)

Actions

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1.

The **Actions** drop-down list in the security dashboard has the following options:

Table 203: Actions

Option	Description
Edit Security Dashboard	Choose this option to edit the security dashboard. You can perform the following actions: • Re-arrange: Drag and move the dashlets within the security dashboard. • Delete: Click **Delete** to delete a dashlet.

Option	Description
Show SecureX Ribbon	Click **Show SecureX Ribbon** to view the **SecureX** ribbon in the security dashboard. You can use the **SecureX** ribbon to access the **SecureX** portal from the the security dashboard. For more information, see View SecureX Ribbon.
Reset to Default View	This option is displayed if you have edited the security dashboard page. Click this option to revert to the default view of the security dashboard.

Configure SGT Inline Tagging Using Cisco SD-WAN Manager

Table 204: Feature History

Feature Name	Release Information	Description
Support for SGT Propagation with Cisco TrustSec Integration	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can configure the Cisco TrustSec Security Group Tag (SGT) propagation feature, Inline Tagging, from the **TrustSec** tab using the Cisco VPN template for one of the supported interfaces.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
4. Choose one of the available Cisco VPN Interface templates, for example, **Cisco VPN Interface Ethernet** .
5. Enter a name and a description for the feature template.
6. To enable SGT propagation, use the following options:
   - For Transport interface (VPN 0):
     a. Click **Tunnel**.
     b. In the **CTS SGT Propagation** field, click **On** to enable SGT propagation for inline tagging. By default, this option is disabled.
   - For service-side interface (VPN x):
     a. Click **TrustSec**.

b. From the **Enable SGT Propagation** drop-down list, choose **Global**, and then click **On**. Additional propagation options are displayed.

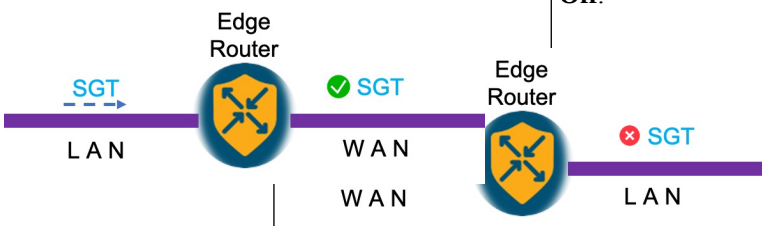
c. To propagate SGT in Cisco Catalyst SD-WAN, set **Propagate** to **On**.

The following table displays the SGT propagation options, and the LAN to WAN and WAN to LAN behavior based on the option you choose for SGT propagation. The options are displayed in the following table and available to you only if you set the **Enable SGT Propagation** to **On**.

Table 205: SGT Propagation options

SGT Propagation Options	LAN to WAN	WAN to LAN	Notes
Propagate = On **Security Group Tag** = <SGT Value> **Trusted** = On	SGT is propagated from LAN to WAN.	SGT is propagated from WAN to LAN.	This is the most common configuration. Usually, the SGT value is 2
Propagate = On **Security Group Tag** = <SGT Value> **Trusted** = Off	SGT is propagated from LAN to WAN with a configured SGT value.	SGT is propagated from WAN to LAN. No effect to the incoming SGT.	Overrides the incoming SGT from LAN to WAN because **Trusted** is set to **Off**
Propagate = Off **Security Group Tag** = <SGT Value> **Trusted** = On	SGT is propagated from LAN to WAN. No effect to the incoming SGT.	SGT is not propagated from WAN to LAN.	

SGT Propagation Options	LAN to WAN	WAN to LAN	Notes
Propagate = Off **Security Group Tag** = <SGT Value> **Trusted** = Off	SGT is propagated from LAN to WAN with a configured SGT value.	SGT is not added to the LAN packets. SGT is not propagated to	Overrides the incoming SGT from LAN to WAN because **Trusted** is set to **Off**.
Propagate = On	SGT propagated from LAN to WAN with SGT value	SGT is propagated from WAN to LAN with SGT value 0.	This can be configured only on a physical interface if there are existing sub interfaces.



Note

- Enterprise Network Compute System (ENCS) LAN and WAN ports allow propagation of SGT tags on its physical ports. The LAN interfaces must be connected to the LAN side and the WAN interfaces must be connected to the WAN side of the network. You must deploy Cisco Catalyst 8000V router or Integrated Services Virtual router to process the tagging.

7. Click **Save**.
8. Configure the routing protocols using the Cisco SD-WAN Manager templates. You can choose to use any of the routing protocols. .
9. Attach the feature template to the device template.

Configure SGT Propagation Using SXP and SGT Enforcement

Table 206: Feature History

Feature Name	Release Information	Description
SGT Propagation Using SXP and SGACL Enforcement	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can now configure SGT propagation using SXP and SGT enforcement on Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager.

Configure SXP for Dynamic IP-SGT Binding Using Cisco SD-WAN Manager

You can configure an SXP connection for downloading the IP-SGT binding from Cisco ISE to a Cisco IOS XE Catalyst SD-WAN device.

To configure an SXP connection in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section, choose **TrustSec**.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Enter the details for setting up an SXP connection:

Parameter Name	Description
Device SGT	Enter a value to configure the SGT for packets sent from a device. Range: 2 to 65519.
Credentials ID	Enter a TrustSec ID for the device. This ID must be the same as that in ISE and must not exceed 32 characters.
Credentials Password	Enter a TrustSec password for the device.

Parameter Name	Description
Enable Enforcement	Click **On** to enable at a global level. Click **Off** to disable SGT enforcement. **Note** You can enable this configuration either at a global level here, or at an interface level in step 8 of Configuring SGT Enforcement at an interface level in Cisco SD-WAN Manager, but not both.

8. Configure SXP for dynamic IP/SGT.

Parameter Name	Description
Enable SXP	Click **On** to enable an SXP connection on the device. When you enable SXP, you must enter a Node ID and a Node ID type. **Note** When you change a Node ID, you must first disable SXP and then push the template to the device. Then, you change the Node ID, and then push the template to the device again.
Source IP	Enter an IP address to set up a source IP address for SXP.
Password	Enter a default password for SXP.
Key Chain Name	Enter a name to configure the key chain for SXP.
Log Binding Changes	Click **On** to enable logging for IP-to-SGT binding changes.
Reconciliation Period (seconds)	Enter a time (in seconds) to configure the SXP reconciliation period. After a peer terminates an SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the SXP reconciliation period timer starts. While the SXP reconciliation period timer is active, the Cisco TrustSec software retains the SGT mapping entries learned from the previous connection and removes the invalid entries. The default value is 120 seconds (2 minutes). Setting the SXP reconciliation period to 0 seconds disables the timer and causes all the entries from the previous connection to be removed.
Retry Period (seconds)	Enter a time (in seconds) to configure the retry period for SXP reconnection.
Speaker Hold Time (seconds)	Enter time (in seconds) to configure the global hold-time period for a speaker device.
Minimum Listener Hold Time (seconds)	Enter a time (in seconds) to configure the minimum allowed hold-time period for a listener device.
Maximum Listener Hold Time (seconds)	Enter a time (in seconds) to configure the maximum allowed hold-time period for a listener device.
Node ID Type	Choose a node ID type.
Node ID	Enter a node ID. A node ID is used to identify the individual devices within the network.

9. Click **New Connection** to add a new SXP peer connection details.

Parameter Name	Description
Peer IP	Configure a peer IPv4 address for SXP.
Source IP	Configure a source IPv4 address for SXP.
Preshared Key	Choose a preshared key type.
Mode	Choose a connection mode. **Local** refers to the local device, and **Peer** refers to a peer device.
Mode Type	Choose a role for the device.
Minimum Hold Time	Enter time (in seconds) to configure the minimum hold time for the SXP connection.
Maximum Hold Time	Enter time (in seconds) to configure the maximum hold time for the SXP connection.
VPN ID	Enter a VPN or VRF ID for the SXP connection.

Note **Maximum Hold Time** and **Minimum Hold Time** can be configured only when you choose **Mode** as **Local** and **Mode Type** as **Listener**, or when **Mode** is **Peer** and **Mode Type** is **Speaker**.

Only **Minimum Hold Time** is configurable when **Mode** is **Local** and **Mode Type** is **Speaker** or when **Mode** is **Peer** and **Mode Type** is **Listener**.

Hold time cannot be configured if you choose **Mode Type** as **Both** (that is **Listener** and **Speaker**).

10. Click **Save** to save your configuration for an SXP connection.

Configure Static IP-SGT Binding Using Cisco SD-WAN Manager

To configure static IP-SGT, use the CLI add-on template in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section, choose **CLI Add-On Template** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.

7. In the **CLI Configuration** area, enter the following configuration:

```
cts role-based sgt-map vrf instance_name {ipv4_netaddress|ipv4_netaddress/prefix} sgt
sgt-number
cts role-based sgt-map vrf instance_name host {ipv4_hostaddress} sgt sgt-number
```

8. Click **Save** to save this configuration. This configuration can now be pushed to a Cisco IOS XE Catalyst SD-WAN device for propagation of the SGT over a Cisco Catalyst SD-WAN network.

Configure TCP-AO Support for SXP

Cisco TrustSec SXP peers exchange IP-SGT bindings over a TCP connection. TCP Authentication Option (TCP-AO) is used to guard against spoofed TCP segments in Cisco TrustSec SXP sessions between the peers. TCP-AO is resistant to collision attacks and provides algorithmic agility and support for key management.

To enable TCP-AO for an SXP connection, a TCP-AO key chain must be specified for the connection.

To establish an SXP peer connection with TCP-AO:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **BASIC INFORMATION** section, choose **Cisco Security** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Configure TCP-AO key chain and keys.

Parameter Name	Description
Keychain Name	Specify a TCP-AO key chain name. The key chain name can have a maximum of 256 characters.
Key ID	Specify a key identifier. Range: 0 to 2147483647.
Send ID	Specify the send identifier for the key. Range: 0 to 255.
Receiver ID	Specify the receive identifier for the key. Range: 0 to 255.

Parameter Name	Description
Include TCP Options	This field indicates whether TCP options other than TCP-AO must be used to calculate Message Authentication Codes (MACs). A MAC is computed for a TCP segment using a configured MAC algorithm, relevant traffic keys, and the TCP segment data prefixed with a pseudoheader. When options are included, the content of all options is included in the MAC with TCP-AO's **MAC field** is filled with zeroed. When the options are not included, all options other than TCP-AO are excluded from all MAC calculations.
Accept AO Mismatch	This field indicates whether the receiver must accept the segments for which the MAC in the incoming TCP-AO does not match the MAC that is generated on the receiver.
Crypto Algorithm	Specify the algorithm to be used to compute MACs for TCP segments. You can choosese one of these: • `aes-128-cmac` • `hmac-sha-1` • `hmac-sha-256`
Key String	Specify the master key for deriving the traffic keys. The master keys must be identical on both the peers. If the master keys do not match, authentication fails and segments may be rejected by the receiver. Range: 0 to 80 characters.
Send Lifetime Local	Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be used in TCP-AO authentication is valid. Specify the start time in the local time zone. By default, the start time corresponds to UTC time. The end time can be specified in three ways—infinite (no expiry), duration (1 to 2147483646 sec), exact time – (either UTC or local).
Accept Lifetime Local	Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be accepted for TCP-AO authentication is valid. Specify the start time in the local time zone. By default, the start time corresponds to UTC time. The end time can be specified in three ways—infinite (no expiry), duration (1 to 2147483646 sec), exact time – (either UTC or local).

Note When you configure a key chain for an SXP connection, at least one key in the key chain must be configured with the current time. All keys in the key chain cannot be configured completely with a future time.

Download SGACL Policies to Cisco IOS XE Catalyst SD-WAN devices

When configured in Cisco ISE, SGACL policies can be downloaded dynamically from Cisco ISE to a Cisco IOS XE Catalyst SD-WAN device using a RADIUS server.

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

2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **Basic Information**, choose **Cisco AAA** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Click **Radius** to configure a connection to a RADIUS server. The followin fields are displayed:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server.
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Range: 0 to 65535.
Accounting Port	Enter the UDP port that will be used to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 to 65535.
Timeout	Specify how long to wait to receive a reply from the RADIUS server before retransmitting a request. Range: 1 through 1000.
Retransmit Count	Specify how many times to search through the list of RADIUS servers while attempting to locate a server. Range: 1 through 1000.
Key Type	Click **PAC** as key type.
Key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can enter the key as a text string from—1 to 31 characters long,—and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.

8. Click **Radius Group** to add a new RADIUS group. The following fields are displayed:

Parameter Name	Description
Group Name	Displays the RADIUS group name. This field is automatically populated based on the VPN ID that you configure.
VPN ID	Enter a VPN ID.
Source Interface	Set the interface that will be used to reach the RADIUS server.
Radius Server	Choose an IP address for the RADIUS server.

9. Click **Radius COA** to configure the settings to accept change of authorization (CoA) requests from a RADIUS or other authentication server, and to act on requests to a connection to the RADIUS server.

   Updated policies are downloaded to the Cisco IOS XE Catalyst SD-WAN device when SGACL policies are modified on ISE and a CoA is pushed to the Cisco IOS XE Catalyst SD-WAN device.

   On clicking **Radius COA**, the following fields are displayed:

Parameter Name	Description
Client	Displays the RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests.
Domain Stripping	Configure domain stripping at the server group level. The stripping keyword compares the incoming username with the names oriented to the left of the @ domain delimiter.
Port	Specify the RADIUS Dynamic Author port. *Range:* 0 to 65535

10. Click **TrustSec** to configure more details for authorization. The following details are displayed:

Parameter Name	Description
CTS Authorization List	Specify a name of a list for authentication, authorization, and accounting (AAA) servers.
Radius group	Choose a RADIUS server.

11. Click **Save**.

Configure Static SGACL Policies in Cisco SD-WAN Manager

To configure static SGACL policies, use the CLI Add-On template in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section,, choose **CLI Add-On Template** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of any characters and spaces.
7. In the CLI configuration area, enter the following configuration:

```
interface gigabitethernet 1/1/3
cts role-based enforcement
cts role-based sgt-map sgt 2
```

```
interface gigabitethernet 1/1/4
no cts role-based enforcement[no] cts role-based permissions {[ default | from |
[source-sgt] | to | [dest-sgt]]}
[no] cts role-based permissions {[ default | from | [source-sgt] | to | [dest-sgt]]}
```

8. Click **Save**.

   This configuration can now be pushed to the Cisco IOS XE Catalyst SD-WAN device for enforcement of SGACL policies.

Configure SGT Enforcement at the Interface Level in Cisco SD-WAN Manager

To enforce SGT using SGACL policies at the interface level in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **Basic Information**, choose **Cisco VPN Interface Ethernet** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.
7. Click **TrustSec**.
8. In the **Enable Enforcement** field, click **On** to enable SGT enforcement on a particular interface.

Note You can enable this configuration either at an interface level in this step, or a global level using the **Enable Enforcement** field in Configuring SXP for Dynamic IP/SGT using vManage, but not both.

9. In the **Enter a SGT value** field, enter a value that can be used as a tag for enforcement .
10. Click **Save**.

Single Sign-On Using Azure Active Directory (AD)

Table 207: Feature History

Feature Name	Release Information	Description
Single Sign-On Using Azure AD	Cisco vManage Release 20.8.1	Single Sign-On (SSO) with security assertion mark-up language (SAML) gives faster, easier, and trusted access to cloud applications without storing passwords or requiring you to log in to each application individually.

Configure SNMP with Encrypted Strings Using CLI Templates

Table 208: Feature History

Feature Name	Release Information	Description
Configure SNMP with Encrypted Strings Using CLI Templates	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure SNMP with encrypted strings using CLI templates.

Use the CLI template feature or CLI add-on feature template to configure SNMP and also encrypt supported variables on Cisco IOS XE Catalyst SD-WAN devices. For more information on the encryption, see Type 6 Passwords on Cisco IOS XE SD-WAN Routers

Note If you encrypt plaintext strings using the CLI add on feature template, the strings are not encrypted in MIBs.

You cannot modify an existing SNMP community to convert it to encrypted strings. To encrypt the strings, you must delete and recreate the SNMP communities.

1. Navigate to **Configuration** > **Templates**
2. Use one of the following templates to add the CLI:
   - CLI add-on feature templates
     a. Click **Feature Templates**, and then click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

   b. Under the Select Devices pane, select the Cisco IOS XE Catalyst SD-WAN device devices for which you are creating the template.
   c. Under the Select Template pane, scroll down to the Other Templates section.

d. Click **CLI Add-On Template**.

- CLI templates

a. In **Device Templates**, click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

b. From the **Create Template** drop-down, select **CLI Template**.

c. Under the Select Devices pane, select the Cisco IOS XE Catalyst SD-WAN device devices for which you are creating the template.

3. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
5. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.
6. To encrypt plaintext values such as passwords or the SNMP community string, select the text and click **Encrypt Type6**.
7. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format `{{variable-name}}`. For example: `{{hostname}}`.
8. Click **Save**. The new feature template is displayed the Feature Template table.
9. To use the CLI add-on feature template, edit the device template as follows:
   a. In the **Templates** page, click **Device**.
   b. Select the device template for which you want to add the CLI add-on feature template.
   c. Click **...** and choose **Edit**.
   d. Scroll to the **Additional Templates** section.
   e. In the CLI Add-On Template field, select the CLI add-on feature template that you previously created.
   f. Click **Update**.

Configure TACACS Authentication for Cloud OnRamp Colocation Cluster

Table 209: Feature History

Feature Name	Release Information	Description
TACACS Authentication	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can configure the TACACS authentication for users using the **TACACS** configuration settings of Cloud OnRamp for Colocation cluster.

The TACACS authentication determines the valid users who can access the Cisco CSP and Cisco Catalyst 9500 devices after a cluster is active.

Points to consider

- By default, the admin users with Role-based access control (RBAC) are authorized to access the Cisco CSP and Cisco Catalyst 9500 devices.
- Do not configure the same user with different passwords when configuring using TACACS and RBAC. If same user with a different password is configured on TACACS and RBAC, the RBAC user and password authentication is used.

To authenticate users:

Note Before configuring the TACACS authentication for users using the **Cluster Topology** window, ensure that you create a Cloud OnRamp for Colocation cluster. See Create and Activate Clusters.

1. To add TACACS server configuration, on the **Cluster Topology** window, click **Other Settings** > **Add** next to **TACACS**.

   To edit TACACS server configuration, in the **Cluster Topology** window, click **Other Settings** > **Edit** next to **TACACS**.

   In the **TACACS** configuration window, enter information about the following:

   - Template Name—The TACACS template name can contain 128 alphanumeric characters.
   - (Optional) Description—The description can contain 2048 alphanumeric characters.

2. To add a new TACACS server, click **+ New TACACS SERVER**.
   - In **Server IP Address**, enter the IPv4 address.

     Use IPv4 addresses for hostnames of TACACS server.
   - In **Secret** enter the password and confirm the password in **Confirm Secret**.

3. Click **Add**

   The new TACACS server details are listed in the **TACACS** configuration window.

Note You can add a maximum of four TACACS servers.

4. To add another TACACS server, repeat step 2 to step 3.

   When authenticating users, if the first TACACS server is not reachable, the next server is verified until all the four servers are verified.

5. Click **Save**.

6. To delete a TACACS server configuration, choose a row from the TACACS server details list and click **Delete** under **Action**.

Note To modify an existing TACACS server information, ensure to delete a TACACS server and then add a new server.

7. To view the TACACS server configuration, in Cisco SD-WAN Manager, click **Configuration** > **Devices**.

   For the desired Cisco CSP device or Cisco Catalyst 9500 switch, click **...** and choose **Running Configuration**.

Configure TCP MSS and Clear Dont Fragment

Table 210: Feature History

Feature Name	Release Information	Description
Configure TCP MSS	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature lets you configure TCP MSS on Cisco IOS XE Catalyst SD-WAN devices on both directions of the Cisco Catalyst SD-WAN tunnel interface.
Configure Clear Don’t Fragment Option	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides you the option in Cisco SD-WAN Manager to clear the Don't Fragment bit in the IPv4 packet header for packets being sent out on a Cisco Catalyst SD-WAN tunnel.

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

2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Create a new CLI add-on feature template or edit one of the following templates. You can use any of the following feature templates to configure TCP MSS and clear Dont Fragment:
   - VPN Ethernet Interface
   - VPN Interface DSL IPoE
   - VPN Interface DSL PPoA
   - VPN Interface DSL PPPoE
   - VPN Interface Multilink
   - VPN Interface T1/E1
   - Cellular Interfaces

   For information on creating a new CLI add-on feature template, see Create a CLI Add-on Feature Template.
4. Click **Tunnel**.
5. To configure TCP MSS, in **Tunnel TCP MSS**, specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. *Range:* 552 to 1460 bytes *Default:* None

   TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, it flows through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU.
6. Click the **Clear-Dont-Fragment** option to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the Don't Fragment bit is cleared, packets larger than that interface's MTU are fragmented before being sent.

Note Clear-Dont-Fragment clears the Don't Fragment bit when there is fragmentation needed and the Don't Fragment bit is set. For packets that don't require fragmentation, the Don't Fragment bit is not affected.

7. Click **Save** or **Update**.

Configure Cisco Catalyst SD-WAN Validator

Once you have set up and started the virtual machine (VM) for Cisco SD-WAN Validator in your overlay network, Cisco SD-WAN Validator comes up with a factory-default configuration. You then need to manually configure few basic features and functions so that the devices can be authenticated and verified and can join

the overlay network. Among these features, you configure the device as Cisco SD-WAN Validator providing the system IP address, and you configure a WAN interface that connects to the Internet. This interface must have a public IP address so that all Cisco vEdge devices in the overlay network can connect to Cisco SD-WAN Validator.

You create the initial configuration by using SSH to open a CLI session to Cisco SD-WAN Validator.

After you have created the initial configuration, you create the full configuration by creating configuration templates on Cisco SD-WAN Manager and then attach the templates to Cisco SD-WAN Validator. When you attach the configuration templates to Cisco SD-WAN Validator, the configuration parameters in the templates overwrite the initial configuration.

Create Initial Configuration for Cisco Catalyst SD-WAN Validator

To create the initial configuration on Cisco SD-WAN Validator using a CLI session:

1. Open a CLI session to Cisco vEdge device via SSH.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

   ```
   vBond#config
   vBond(config)#
   ```

4. Configure the hostname:

   ```
   vBond(config)#system host-name hostname
   ```

   Configuring the hostname is optional, but is recommended because this name in included as part of the prompt in the CLI and it is used on various Cisco SD-WAN Manager screens to refer to the device.

5. Configure the system IP address:

   ```
   vBond(config-system)#system-ip ip-address
   ```

   Cisco SD-WAN Manager uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

6. Configure the IP address of Cisco SD-WAN Validator. Cisco SD-WAN Validator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach Cisco SD-WAN Validator:

   ```
   vBond(config-system)#vbond ip-address local
   ```

   In Releases 16.3 and later, the address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. A Cisco SD-WAN Manager is effectively a vEdge router that performs only the orchestrator functions. The **local** option designates the device to be Cisco SD-WAN Validator, not a vEdge router. Cisco SD-WAN Validator must run on a standalone virtual machine (VM) or hardware router; it cannot coexist in the same device as a software or hardware vEdge router.

7. Configure a time limit for confirming that a software upgrade is successful:

   ```
   vBond(config-system)#upgrade-confirm minutes
   ```

   The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, Cisco SD-WAN Manager (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not received the confirmation within the configured time, it reverts to the previous software image.

8. Change the password for the user "admin":

```
vBond(config-system)#user admin password password
```

The default password is "admin".

9. Configure an interface in VPN 0, to connect to the Internet or other WAN transport network. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. Ensure that the prefix you configure for the interface contains the IP address that you configure in the **vbond local** command.

```
vBond(config)#vpn 0 interface interface-name
vBond(config-interface)#ip address ipv4-prefix/length
vBond(config-interface)#ipv6 address ipv6-prefix/length
vBond(config-interface)#no shutdown
```

Note The IP address must be a public address so that all devices in the overlay network can reach Cisco SD-WAN Validator.

10. Commit the configuration:

```
vBond(config)#commit and-quit
vBond#
```

11. Verify that the configuration is correct and complete:

```
vBond#show running-config
```

After the overlay network is up and operational, create a Cisco SD-WAN Validator configuration template on the Cisco SD-WAN Manager that contains the initial configuration parameters. Use the following Cisco SD-WAN Manager feature templates:

- System feature template to configure the hostname, system IP address, and Cisco SD-WAN Validator functionality.
- AAA feature template to configure a password for the "admin" user.
- VPN Interface Ethernet feature template to configure the interface in VPN 0.

In addition, it is recommended that you configure the following general system parameters:

- From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and configure Organization name.
- From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**. From System configuration template drop-down, select **create template** and configure Timezone, NTP servers, and device physical location.
- Click **Additional Templates** and from banner feature template drop-down, select **Create Template**. Configure Login banner.
- From System feature configuration template drop-down, select **Create Template** and configure disk and server parameters.
- From AAA feature configuration template drop-down, select **Create Template** and configure AAA, RADIUS and TACACS servers.
- Click **Additional Templates** and from SNMP feature template drop-down, select **Create Template** and configure SNMP.

Note The IP address must be a public address so that all devices in the overlay network can reach Cisco SD-WAN Validator.

Sample Initial CLI Configuration

Below is an example of a simple configuration on Cisco SD-WAN Validator. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vBond#show running-config
system
 host-name         vBond
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip         172.16.240.161
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 vbond 11.1.1.14 local
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password encrypted-password
  !
 !
 logging
  disk
   enable
  !
!
vpn 0
 interface ge0/0
  ip address 11.1.1.14/24
  no shutdown
 !
 ip route 0.0.0.0/0 11.1.1.1
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

What's Next

See *Add Cisco SD-WAN Validator to the Overlay Network*.

Create Configuration Templates for Cisco Catalyst SD-WAN Validator

This article describes how to configure Cisco SD-WAN Validators that are being managed by Cisco SD-WAN Manager. These devices must be configured from Cisco SD-WAN Manager. If you configure them directly from the CLI on the router, Cisco SD-WAN Manager overwrites the configuration with the one stored on the NMS system.

Create Device Templates

Device templates contain all or large portions of a device's complete operational configuration. You create device templates by consolidating together individual feature templates. You can also create them by entering a CLI text-style configuration directly on Cisco SD-WAN Manager. You can use both styles of device templates when configuring the Cisco SD-WAN Validator.

To create Cisco SD-WAN Validator device templates from feature templates:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down, select **From Feature Templates**.
4. From the **Device Model** drop-down, select a **Cloud router**.
5. Enter a name and description for the Cisco SD-WAN Validator device template. These fields are mandatory. You cannot use any special characters in template names.
6. From the **Load Running config from reachable device** drop-down, select the desired group of templates.
7. In each section, select the desired template. All required templates are marked with an asterisk (*). Initially, the drop-down for each template lists the default feature template.
   a. For each required and optional template, select the feature template from the drop-down. These templates are the ones that you previously created (see Create Feature Templates above). Do not select a BFD or an OMP template for Cisco SD-WAN Validators.
   b. For additional templates, click the plus (+) sign next to the template name, and select the feature template from the drop-down.
8. Click **Create**. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

To create device templates by entering a CLI text-style configuration directly on Cisco SD-WAN Manager:

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

2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down, select **CLI Template**.
4. Enter a template name and description.
5. Enter the configuration in the **Config Preview** window, either by typing it, cutting and pasting it, or uploading a file.
6. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.
7. Click **Add**. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Create Feature Templates

Feature templates are the building blocks of a Cisco SD-WAN Validator's complete configuration. For each feature that you can enable on Cisco SD-WAN Validator, Cisco SD-WAN Manager provides a template form that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco SD-WAN Validator features.

You can create multiple templates for the same feature.

To create Cisco SD-WAN Validator feature templates:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select **Add Template**.
4. In the left pane, from **Select Devices**, select **Cloud router**.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters applicable to that template. Optional parameters are generally grayed out. A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.
6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu available to the left of each parameter's value box.

8. Click the plus sign (+) below the required parameters to set the values for additional parameters, if applicable.
9. Click **Create**.
10. Create feature templates for each of the required features listed in the previous section.
    a. In the System template, in the top portion, configure all desired parameters except for Controller Groups, Maximum Controllers, and Maximum OMP Sessions. These parameters are specific to routers and have no meaning for Cisco SD-WAN Validator. In the **Advanced Options** portion, in Cisco SD-WAN Validator Only and Local Cisco SD-WAN Validator, click **On**. These two parameters instantiates Cisco SD-WAN Validator.
    b. Create two VPN templates, one for VPN 0 (the VPN that connects to the Internet or other public transport network) and one for VPN 512 (the VPN that handles out-of-band management traffic).
    c. Create AAA and Security templates.
11. Create feature templates for each feature that you want to enable on Cisco SD-WAN Validators:
    a. Create Archive and Banner templates
    b. Create one Interface Ethernet template for each additional Ethernet interface you want to configure on the Cisco SD-WAN Validator. Do not create any tunnel interfaces, or tunnels of any kind, for Cisco SD-WAN Validators.

Feature Templates for Cisco Catalyst SD-WAN Validators

The following features are mandatory for Cisco SD-WAN Validator operation, and so creating a feature template for each of them is required:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Security	Security
System-wide parameters	System
Transport VPN (VPN 0)	VPN, with the VPN ID set to 0
Management VPN (for out-of-band management traffic)	VPN, with the VPN ID set to 512

Attach Device Templates To Cisco Catalyst SD-WAN Validator

To configure Cisco SD-WAN Validator, you attach one device template to the orchestrator. You can attach the same template to multiple Cisco SD-WAN Validators simultaneously.

To attach a device template to the Cisco SD-WAN Validator:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. Select the desired device template.
4. For the selected device template, click **...**, and select **Attach Devices**.
5. In the **Attach Devices** column, select the desired Cisco SD-WAN Validator from the **Available Devices** list, and click the right-pointing arrow to move them to the **Selected Devices** column. You can select one or more orchestrators. Click **Select All** to choose all listed orchestrator.
6. Click **Attach**.

Add Cisco Catalyst SD-WAN Validator to the Overlay Network

After you create a minimal configuration for Cisco SD-WAN Validator, you must add it to overlay network by making Cisco SD-WAN Manager aware of Cisco SD-WAN Validator. When you add Cisco SD-WAN Validator, a signed certificate is generated and is used to validate and authenticate the orchestrator.

Add Cisco Catalyst SD-WAN Validator and Generate Certificate

To add Cisco SD-WAN Validator to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, from **Add Controller** drop-down, select **vBond**.
3. In the **Add vBond** window:
   a. Enter the vBond management IP address.
   b. Enter the username and password to access Cisco SD-WAN Validator.
   c. Choose the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   d. Click **Add**.

Cisco SD-WAN Manager generates the CSR, retrieves the generated certificate, and automatically installs it on Cisco SD-WAN Validator. The new controller device is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on Cisco SD-WAN Validator:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose the new device listed, and check in the Certificate Status column to ensure that the certificate has been installed.

Create Configuration Templates for Cisco SD-WAN Manager

Feature Templates for Cisco SD-WAN Manager

The following features are mandatory for Cisco SD-WAN Manager operation, so you must create a feature template for each of them:

Table 211:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Security	Security
System-wide parameters	System
Transport VPN (VPN 0)	VPN, with the VPN ID set to 0.
Management VPN (for out-of-band management traffic)	VPN, with the VPN ID set to 512.

Create Feature Templates

Feature templates are the building blocks of a Cisco SD-WAN Manager's complete configuration. For each feature that you can enable on Cisco SD-WAN Manager, a template form is provided that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco SD-WAN Manager features.

You can create multiple templates for the same feature.

To create Cisco SD-WAN Manager feature templates:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. In the left pane, from **Select Devices**, select **vManage**. You can create a single feature template for features that are available on both the Cisco SD-WAN Manager and other devices. You must, however, create separate feature templates for software features that are available only on Cisco SD-WAN Manager.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining parameters applicable to that template. Optional parameters are generally grayed out. A plus (+) sign is displayed to the right when you can add multiple entries for the same parameter.
6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.

7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu available to the left of each parameter field.
8. Click the plus sign (+) below the required parameters to set values for additional parameters, if applicable.
9. Click **Create**.
10. Create feature templates for each of the required features listed in the previous section.
    a. For the transport VPN, use the template called VPN-Cisco SD-WAN Manager and in the VPN Template section, set the VPN to 0, with a scope of Global.
    b. For the management VPN, use the template called VPN-Cisco SD-WAN Manager and in the VPN Template section, set the VPN to 512, with a scope of Global.
11. Create any additional feature templates for each optional feature that you want to enable on Cisco SD-WAN Manager.

Release Information

Introduced in Cisco SD-WAN Manager in Release 15.3.

Create Configuration Templates for Cisco Catalyst SD-WAN Controller

For Cisco SD-WAN Controllers that are being managed by a Cisco SD-WAN Manager, you must configure them from Cisco SD-WAN Manager. If you configure them directly from the CLI on Cisco Catalyst SD-WAN Controller, Cisco SD-WAN Manager overwrites the configuration with the one stored on Cisco SD-WAN Manager.

Configuration Prerequisites

Security Prerequisites

Before you can configure Cisco SD-WAN Controllers in the Cisco overlay network, you must have generated a certificate for Cisco SD-WAN Controller, and the certificate must already be installed on the device. See Generate a Certificate.

Variables Spreadsheet

The feature templates that you create will most likely contain variables. To have Cisco SD-WAN Manager populate the variables with actual values when you attach a device template to a device, either enter the values manually or click **Import File** in the upper right corner to load an Excel file in CSV format that contains the variables values.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be (in order):

- csv-deviceId—Serial number of the device (used to uniquely identify the device).
- csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).

- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network— routers, Cisco SD-WAN Controllers, and Cisco SD-WAN Validators. You do not need to specify values for all variables for all devices.

Create Device Templates

Device templates contain a device's complete operational configuration. You create device templates by consolidating together individual feature templates. You can also create them by entering a CLI text-style configuration directly on Cisco SD-WAN Manager.

You can attach only one device template to configure a Cisco SD-WAN Controller, so it must contain, at a minimum, all the required portions of the Cisco SD-WAN Controller configuration. If it does not, the Cisco SD-WAN Manager returns an error message. If you attach a second device template to the Cisco SD-WAN Controller, it overwrites the first one.

To create device templates from feature templates:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down select **From Feature Templates**.
4. From the **Device Model** drop-down list, select **vSmart**.
5. Enter a name and description for the Cisco SD-WAN Controller device template. These fields are mandatory. You cannot use any special characters in template names.
6. Complete the **Required Templates** section. All required templates are marked with an asterisk.
   a. For each required template, select the feature template from the drop-down list. These templates are the ones that you previously created (see Create Feature Templates above). After you select a template, the circle next to the template name turns green and displays a green check mark.
   b. For templates that have Sub-Templates, click the plus (+) sign or the Sub-Templates title to display a list of sub-templates. As you select a sub-template, the name of the sub-template along with a drop-down is displayed. If the sub-template is mandatory, its name is marked with an asterisk.
   c. Select the desired sub-template.
7. Complete the **Optional Templates** section, if required. To do so:
   a. Click **Optional Templates** to add optional feature templates to the device template.
   b. Select the template to add.
   c. Click the template name and select a specific feature template.
8. Click **Create**. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

To create device templates by entering a CLI text-style configuration directly on Cisco SD-WAN Manager:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, select **CLI Template**.
4. In the **Add Device CLI Template** window, enter a template name and description, and select **vSmart**.
5. Enter the configuration in the **CLI Configuration** box, either by typing it, cutting and pasting it, or uploading a file.
6. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.
7. Click **Add**. The right pane on the screen lists the new device template. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Create Feature Templates

Feature templates are the building blocks of Cisco SD-WAN Controller's complete configuration. For each feature that you can enable on Cisco Catalyst SD-WAN Controller, Cisco SD-WAN Manager provides a template form that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco SD-WAN Controller features.

You can create multiple templates for the same feature.

To create Cisco SD-WAN Controller feature templates:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select **Add Template**.
4. In the left pane, from **Select Devices**, select **vSmart**. You can create a single feature template for features that are available on both Cisco SD-WAN Controllers and other devices. You must, however, create separate feature templates for software features that are available only on Cisco SD-WAN Controllers.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining parameters applicable to that template. Optional parameters are generally grayed out. A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.

6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu to the left of each parameter field.
8. Click the plus sign (+) below the required parameters to set values for additional parameters, if applicable.
9. Click **Create**.
10. Create feature templates for each of the required features listed in the previous section. For the transport VPN, use the template called VPN-vSmart and in the VPN Template section, set the VPN to 0, with a scope of Global. For the management VPN, use the template called VPN- and in the VPN Template section, set the VPN to 512, with a scope of Global.
11. Create any additional feature templates for each optional feature that you want to enable on Cisco SD-WAN Controllers.

Attach a Device Template To Cisco SD-WAN Controllers

To configure a Cisco SD-WAN Controller, you attach one device template to the controller. You can attach the same template to multiple Cisco SD-WAN Controller simultaneously.

To attach a device template to Cisco SD-WAN Controllers:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. For the desired device template, click **...**, and select **Attach Devices**.
4. In the **Attach Devices** window, select the desired Cisco SD-WAN Controller from the **Available Devices** column, and click the right-pointing arrow to move them to the **Selected Devices** column. You can select one or more controllers. Click **Select All** to choose all listed controllers.
5. Click **Attach**.
6. Click **Next**.
7. To preview the configuration that is about to be sent to Cisco SD-WAN Controller, in the left pane, click the device. The configuration is displayed in the right pane, in the **Device Configuration Preview** window.
8. To send the configuration in the device template to Cisco SD-WAN Controllers, click **Configure Devices**.

Add Cisco Catalyst SD-WAN Controller to the Overlay Network

After you create a minimal configuration for Cisco SD-WAN Controller, you must add it to an overlay network by making Cisco SD-WAN Manager aware of the controller. When you add Cisco SD-WAN Controller, a signed certificate is generated and is used to validate and authenticate the controller.

Cisco SD-WAN Manager can support up to 20 Cisco SD-WAN Controllers in the network.

Add a Cisco Catalyst SD-WAN Controller and Generate Certificate

To add a Cisco SD-WAN Controller to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and from the **Add Controller** drop-down menu, choose **vSmart**.
3. In the **Add vSmart** window:
   a. Enter the system IP address of Cisco SD-WAN Controller.
   b. Enter the username and password to access Cisco SD-WAN Controller.
   c. Choose the protocol to use for control-plane connections. The default is DTLS.
   d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.
   e. Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   f. Click **Add**.

Cisco SD-WAN Manager automatically generates the CSR, retrieves the generated certificate, and installs it on Cisco SD-WAN Controller. The new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on a Cisco SD-WAN Controller:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose the new controller listed and check in the Certificate Status column to ensure that the certificate has been installed.

Note If Cisco SD-WAN Controller and Cisco SD-WAN Validator have the same system IP addresses, they do not appear in Cisco SD-WAN Manager as devices or controllers. The certificate status of Cisco SD-WAN Controller and Cisco SD-WAN Validator is also not displayed. However, the control connections still successfully comes up.

What's Next

See *Deploy the vEdge Routers*.

Determine Why a Device Rejects a Template

When you attach a template to a device using the screen, the device might reject the template. One reason that this may occur is because the device template contains incorrect variable values. When a device rejects a template, it reverts to the previous configuration.

To determine why the device rejected the template:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Locate the device. The **Template Status** column indicates why the device rejected the template.

Export Device Data in CSV Format

In an overlay network, you might have multiple devices of the same type that have identical or effectively identical configurations. For example, in a network with redundant Cisco Catalyst SD-WAN Controllers, each controller must be configured with identical policies. Another example is a network with Cisco IOS XE Catalyst SD-WAN devices at multiple sites, where each Cisco IOS XE Catalyst SD-WAN device is providing identical services at each site.

Because the configurations for these devices are essentially identical, you can create one set of feature templates, which you then consolidate into one device template that you use to configure all the devices. You can create an Excel file in CSV format that lists the variables and defines each device specific variable value for each device. Then you can load the file when you attach a device template to a device.

To export data for all devices to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

Cisco SD-WAN Manager downloads all data from the device table to an Excel file in CSV format.

Configure Cisco SD-WAN Controllers

Add a Cisco SD-WAN Controller

After the Cisco Catalyst SD-WAN Validator authenticates Cisco IOS XE Catalyst SD-WAN devices, the Cisco Catalyst SD-WAN Validator provides Cisco IOS XE Catalyst SD-WAN devices information that they need to connect to the Cisco Catalyst SD-WAN Controller. A Cisco Catalyst SD-WAN Controller controls the flow of data traffic throughout the network via data and app-route policies. To configure Cisco Catalyst SD-WAN Controllers:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**.
3. Click the **Add Controller** drop-down list and select **vSmart**.
4. In the **Add vSmart** window:
   a. Enter the system IP address of the Cisco Catalyst SD-WAN Controller.
   b. Enter the username and password to access the Cisco Catalyst SD-WAN Controller.

c. Select the protocol to use for control-plane connections. The default is DTLS. The DTLS (Datagram Transport Layer Security) protocol is designed to provide security for UDP communications.

d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.

   The TLS (Transport Socket Layer) protocol that provides communications security over a network.

e. Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.

f. Click **Add**.

5. Repeat Steps 2, 3 and 4 to add additional Cisco Catalyst SD-WAN Controllers. Cisco SD-WAN Manager can support up to 20 Cisco Catalyst SD-WAN Controllers in the network.

The new Cisco Catalyst SD-WAN Controller is added to the list of controllers in the Controllers screen.

Edit Controller Details

Editing controller details lets you update the IP address and login credentials of a controller device. To edit controller details:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select the controller.
3. Click **…**, and click **Edit**.
4. In the **Edit** window, edit the IP address and the login credentials.
5. Click **Save**.

Delete a Controller

Deleting a controller removes it from the overlay. Delete a controller it if you are replacing it or if you no longer need it in your network.

To delete a controller:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select the controller.
3. Click **…**, and click **Invalidate**.
4. To confirm the removal of the device and all its control connections, click **OK**.

Configure Reverse Proxy on Controllers

To configure reverse proxy on an individual Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select the controller.
3. Click **…**, and click **Add Reverse Proxy**.

   The **Add Reverse Proxy** dialog box is displayed.

4. Click **Add Reverse Proxy**.

5. Configure the private IP address and port number for the device. The private IP address is the IP address of the transport interface in VPN 0. The default port number is 12346. This is the port used to establish the connections that handle control and traffic in the overlay network.
6. Configure the proxy IP address and port number for the device, to create the mapping between the private and public IP addresses and port numbers.
7. If the Cisco SD-WAN Manager NMS or Cisco Catalyst SD-WAN Controller has multiple cores, repeat Steps 5 and 6 for each core.
8. Click **Add**.

To enable reverse proxy in the overlay network, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**. Then from the Reverse Proxy bar, click **Edit**. Click **Enabled**, and click **Save**.

Configure NAT DIA Tracker on IPv4 Interfaces Using Feature Templates in Cisco SD-WAN Manager

Table 212: Feature History

Feature Name	Release Information	Description
Dual Endpoint Support for Interface Status Tracking on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure tracker groups with dual endpoints using the Cisco SD-WAN Manager system template and associate each tracker group to an interface.
NAT DIA Tracker for IPv6 Interface	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	NAT DIA tracker is now supported on IPv6 interfaces. You can configure IPv6 DIA tracker using the **IPv6-Tracker** and **IPv6-Tracker Group** options under transport profile in configuration groups.

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

Use the **Cisco System** template to track the status of transport interfaces.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **…** adjacent to the **Cisco System** template that you want to modify and choose **Edit**.

4. Click **Tracker**, and click **New Endpoint Tracker** to configure the tracker parameters.

Table 213: Tracker Parameters

Parameter Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Threshold	Duration to wait for the probe to return a response before declaring that the transport interface is down. *Range:* 100 to 1000 milliseconds. *Default:* 300 milliseconds
Interval	Frequency at which a probe is sent to determine the status of the transport interface. *Range:* 20 to 600 seconds. *Default:* 60 seconds (1 minute)
Multiplier	Number of times a probe can be resent before declaring that the transport interface is down. *Range:* 1 to 10. *Default:* 3
Tracker Type	Choose **Interface** to configure the DIA tracker.
End Point Type: IP Address	IP address of the end point. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. Make sure that the IP address is enabled to respond to HTTP port 80 probes.
End Point Type: DNS Name	DNS name of the end point. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.

5. Click **Add**.

6. To create a tracker group and configure the parameters, click **Tracker Groups** > **New Endpoint Tracker Groups**.

Table 214: Tracker Group Parameters

Parameter Field	Description
Tracker Type: Tracker Elements	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to an interface.
Tracker Type: Tracker Boolean	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**. **OR** is the default boolean operation. An **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the interface is active. If you select the **AND** operation, the transport-interface status is reported as active if both the associated trackers of the tracker group, report that the interface is active.

Note Ensure that you have configured two single endpoint trackers before configuring a tracker group.

7. Click **Add**.
8. Click **Advanced** and enter the **Track Interface** information.

   Enter the name of the tracker to track the status of transport interfaces that connect to the internet.

Note Tracking the interface status is useful when you enable NAT in a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet rather than having to first go to a router in a data center. In this situation, enabling NAT in the transport interface splits the TLOC between the local router and the data center into two, with one going to the remote router and the other going to the internet. When you enable transport tunnel tracking, the software periodically probes the path to the internet to determine whether it is up. If the software detects that this path is down, it withdraws the route to the internet destination, and traffic destined to the internet is then routed through the data center router. When the software detects that the path to the internet is functioning again, the route to the internet is reinstalled.

Note Ensure that you complete filling all the mandatory fields before you update the template.

9. Click **Update**.

Monitor NAT DIA Tracker Configuration on IPv4 Interfaces

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

View Interface DIA Tracker

To view information about DIA tracker on a transport interface:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices.
3. Click **Real Time**.
4. For single endpoint tracker, from the **Device Options** drop-down list, choose **Endpoint Tracker Info**.
5. For dual endpoint tracker, from the **Device Options** drop-down list, choose **Endpoint Tracker Group Info**.

Enable Data Stream Collection from a WAN Edge Router

By default, collecting streams of data from a network device is not enabled.

To collect data streams from a WAN Edge router in the overlay network, perform the following steps.

Collecting data streams also requires that VPN 512 be configured in your Cisco Catalyst SD-WAN network.

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. For **Data Stream**, click **Edit**.
3. Click **Enabled**.
4. From Cisco vManage Release 20.4.1, choose one of the following **IP Address Type** options:
   - **Transport**: Click this option send the data stream to the transport IP address of the Cisco SD-WAN Manager node to which the device is connected.
   - **Management**: Click this option send the data stream to the management IP address of the Cisco SD-WAN Manager node to which the device is connected.
   - **System**: Click this option to send the data stream to the internally configured system IP address of theCisco SD-WAN Manager node to which the device is connected.

     In a Cisco SD-WAN Manager cluster deployment, we recommend that you choose **System** so that the data stream is collected from edge devices that are managed by all Cisco SD-WAN Manager instances in the cluster.
5. From Cisco vManage Release 20.4.1, perform one of these actions:
   - If you choose **Transport** as the IP address type, in the **Hostname** field, enter the public transports IP address that is used to connect to the router.

     You can determine this IP address by using an SSH client to access the router and entering the **`show interface`** CLI command.
   - If you choose **Management** as the IP address type, in the **Hostname** field, enter the IP address or name of the host to collect the data.

     We recommend that this host is one that is used for out-of-band management and that it is located in the management VPN.

   This **Hostname** option is dimmed when **IP Address Type** is **System**.
6. In the **VPN** field, enter the number of the VPN in which the host is located.

   We recommend that this VPN be the management VPN, which is typically VPN 512.

   This **VPN** option is dimmed when **IP Address Type** is **System**.
7. Click **Save**.

Enable Timeout Value for a Cisco SD-WAN Manager Client Session

By default, a user's session to a Cisco SD-WAN Manager client remains established indefinitely and never times out.

To set how long a Cisco SD-WAN Manager client session is inactive before a user is logged out:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. For Client Session Timeout option, click **Edit**.
3. Click **Enabled**, and enter the timeout value, in minutes. This value can be from 10 to 180 minutes.
4. Click **Save**.

The client session timeout value applies to all Cisco SD-WAN Manager servers in a Cisco SD-WAN Manager cluster.

Enable vAnalytics

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, you can easily onboard Cisco Catalyst SD-WAN Analytics into Cisco Catalyst SD-WAN Manager without having to raise a support case with Cisco. For more information, see Onboard Cisco SD-WAN Analytics.

Enforce Software Version on Devices

If you are using the Cisco Catalyst SD-WAN hosted service, you can enforce a version of the Cisco Catalyst SD-WAN software to run on a router when it first joins the overlay network.

To ensure that templates are in sync after an upgrade that enforces a software version, make sure of the following before you perform the upgrade:

- The bootflash and flash on the router must have enough free space to support the upgrade
- The version of the SD-WAN image that is on the device before the upgrade must be a lower version than the enforced SD-WAN version you specify in the following procedure

To enforce a version of the Cisco Catalyst SD-WAN software to run on a router when it first joins the overlay network, follow these steps:

1. Ensure that the software image for the desired device software version is present in the Cisco SD-WAN Manager software image repository:
   a. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

      The Software Repository screen opens and displays a table of software images. If the desired software image is present in the repository, continue with Step 2.

   b. If you need to add a software image, click **Add New Software**.

c. Select the location from which to download the software images, either Cisco SD-WAN Manager, Remote Server, or Remote Server - Cisco SD-WAN Manager.

d. Select an x86-based or a MIPS-based software image.

e. To place the image in the repository, click **Add**.

2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
3. From **Enforce Software Version (ZTP)**, click **Edit**.
4. In **Enforce Software Version**, click **Enabled**.
5. From the **Version** drop-down list, select the version of the software to enforce on the device when they join the network.
6. Click **Save**.

Enforce Strong Passwords

We recommend the use of strong passwords. You must enable password policy rules in Cisco SD-WAN Manager to enforce use of strong passwords.

After you enable a password policy rule, the passwords that are created for new users must meet the requirements that the rule defines. In addition, for releases from Cisco vManage Release 20.9.1, you are prompted to change your password the next time you log in if your existing password does not meet the requirements that the rule defines.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Password Policy**, choose **Edit**.
3. Perform one of these actions, based on your Cisco SD-WAN Manager release:
   - For releases before Cisco vManage Release 20.9.1, click **Enabled**.
   - For releases from Cisco vManage Release 20.9.1 click **Medium Security** or **High Security** to choose the password criteria.

   By default, **Password Policy** is set to **Disabled**.
4. In the **Password Expiration Time (Days)** field, you can specify the number of days for when the password expires.

   By default, password expiration is 90 days.

   Before your password expires, a banner prompts you to change your password. If the password expiration time is 60 days or more, this banner first appears at 30 days before your password expires. If the password expiration time is less than 60 days, this banner first appears at half the number of days that are configured for the expiration time. If you do not change your password before it expires, you are blocked from logging in. In such a scenario, an admin user can change your password and restore your access.

Note The password expiration policy does not apply to the admin user.

5. Click **Save**.

Configuring Posture Assessment on Cisco Catalyst SD-WAN

Table 215: Feature History

Feature Name	Release Information	Description
Posture Assessment Support	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can now configure Posture Assessment capabilities to validate compliance of endpoints according to security policies of your enterprise, through the Add-On feature template in Cisco SD-WAN Manager.

1. Use the CLI Add-on template in Cisco SD-WAN Manager to configure AAA, IEEE 802.1x, posture assessment and redirect ACL and device-tracking.

   Example configurations are given below.

Note `aaa new-model` is enabled by default on Cisco Catalyst SD-WAN and is not configurable by the user. However, it must be configured on a non SD-WAN image.

a. Configure AAA

```
aaa new-model
radius server ISE1

address ipv4 198.51.100.255 auth-port 1812 acct-port 1813
key cisco

aaa group server radius ISE
 server name ISE1
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

interface vlan 15
 ip address 198.51.100.1 198.51.100.254

interface GigabitEthernet0/1/0
 switchport mode access
 switchport access vlan 15

ip radius source-interface vlan 15
```

b. Configure IEEE 802.1x authentication and authorization

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
```

```
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

Note The IEEE 802.1x endpoint is connected to GigabitEthernet0/1/7.

c. Configure posture assessment and redirect ACL

```
ip http server
ip http secure-server

ip access-list extended ACL-POSTAUTH-REDIRECT
10 deny tcp any host 192.0.2.255
20 deny tcp any any eq domain
30 deny udp any any eq domain
40 deny udp any any eq bootpc
50 deny udp any any eq bootps
60 permit tcp any any eq www
70 permit tcp any any eq 443
```

d. Configure device tracking

```
!
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
!
interface GigabitEthernet0/1/7
 device-tracking attach-policy tracking_test
```

Note The IP address mentioned belongs to ISE.

The steps you have to perform to add this configuration into the CLI Add-On template on Cisco SD-WAN Manager are documented here.

2. To Configure CoA reauthentication and dACL on ISE:

   a. Create a downloadable ACL and define the ACEs in it.

      ACL name: TEST_IP_PERMIT_ALL

      ACEs: permit ip any any

   b. Create an authorization result and choose the downloadable ACL as dACL.

   c. Navigate to **Administration** > **System** > **Settings** > **Policy Settings**, and in **Policy Sets** configuration select the authorization result as authorization policy.

3. After creating the CLI Add-On template, attach it to a device template and then Cisco SD-WAN Manager pushes all the configuration in the device template onto your device.

How to Upload a Router Authorized Serial Number File

Table 216: Feature History

Feature Name	Release Information	Description
Device Onboarding Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature provides an enhancement to onboard your device to Cisco SD-WAN Manager by directly uploading a .csv file. You can now go to **Configuration** > **Devices** and directly onboard your device to Cisco SD-WAN Manager by uploading a .csv file containing details of your device.

The following sections describe how to upload the router authorized serial number file to Cisco SD-WAN Manager and distribute the file to all the overlay network controllers.

Enable PnP Connect Sync (Optional)

To sync the uploaded device to your Smart Account or Virtual Account and for your device to reflect on the PnP (Plug and Play) Connect portal, when an unsigned .csv file is uploaded through Cisco SD-WAN Manager, enable the PnP Connect Sync.

Ensure you have an active connection to the PnP (Plug and Play) Connect portal and an active Smart Account and Virtual Account. You have to also use a CCO ID that is associated as the Smart Account or Virtual Account admin of the account, on PnP Connect portal.

Note PnP Connect Sync is only applicable to .csv file upload. It does not affect the .viptela file (which is downloaded from the PnP Connect portal) upload process.

Note You will be allowed to enable PnP Connect Sync only once you enter the Smart Account credentials.

To enable the PnP Connect Sync:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. Go to **Smart Account Credentials** and click **Edit.**
3. Enter **Username** and **Password** and click **Save.**

4. Go to **PnP Connect Sync** and click **Edit.**
5. Click **Enabled** and click **Save.**

Place Routers in Valid State

Perform the following task to place the routers in the Valid state so that they can establish control and data plane connections and can receive their configurations from the Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. Click **WAN Edge List** and click **Upload WAN Edge List**.
3. You can upload WAN Edge devices in the following two ways:
   - Upload a signed file (.viptela file). You can download this .viptela file from the Plug and Play Connect portal.
   - Starting from Cisco vManage Release 20.3.1, you can upload an unsigned file (.csv file). This enhancement is only applicable when you add hardware platforms on-demand onto Cisco SD-WAN Manager. To upload the .csv file this:
     a. Click **Sample CSV**. An excel file will be downloaded.
     b. Open the downloaded .csv file. Enter the following parameters:
        - Chassis number
        - Product ID (mandatory for Cisco vEdge devices, blank value for all other devices)
        - Serial number
        - SUDI serial

        Either the Serial number or SUDI number is mandatory for Cisco IOS XE Catalyst SD-WAN devices, along with chassis number. Cisco ASR1002-X is an exception and does not need Serial or SUDI numbers, it can be onboarded with only the chassis number on the .csv file.
     c. To view your device details in Cisco SD-WAN Manager, go to **Tools** > **SSH Terminal**. Choose your device and use one of the following command-

        show certificate serial (for vEdge devices)

        show sdwan certificate serial (for Cisco IOS XE Catalyst SD-WAN devices)
     d. Enter the specific device details in the downloaded .csv file.
4. To upload the .viptela or .csv file on Cisco SD-WAN Manager click **Choose file** and upload the file that contains the product ID, serial number and chassis number of your device.

Note If you have enabled PnP Sync Connect, the .csv file can contain upto 25 devices. If you have more than 25 devices, you can split them and upload multiple files.

5. Check the check box next to **Validate the uploaded vEdge List and send to controllers**.

6. Click **Upload.**
7. You should now see your device listed in the table of devices.

   If you have enabled the PnP Sync Connect previously, your device will also reflect on the PnP Portal.

A list of routers in the network is displayed, showing detailed information about each router. To verify that the routers are in the Valid state, select **Configuration** > **Certificates.**

Place Routers in Invalid State

To upload the authorized serial number file to the Cisco SD-WAN Manager, but place the routers in Invalid state so that they cannot establish control plane or data plane connections and cannot receive their configurations from Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. Click **WAN Edge List** and click **Upload WAN Edge List**.
3. In the **Upload WAN Edge List** dialog box, choose the file to upload.
4. To upload the router serial number file to Cisco SD-WAN Manager, click **Upload**.

A list of routers in the network is displayed, showing detailed information about each router. To verify that the routers are in the Invalid state, from the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.

Place Routers in Staging State

To move the routers from the Invalid state to the Staging state and then send the serial number file to the controllers, follow the steps below. In the Staging state, the routers can establish control plane connections, over which they receive their configurations from Cisco SD-WAN Manager. However, the routers cannot establish data plane connections.

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. In the **Validate** column, click **Staging** for each router.
4. Click **Send to Controller**.
5. When you are ready to have the router join the data plane in the overlay network, in the **Validate** column, click **Valid** for each router, and then click **Send to Controller**. Placing the routers in the Valid state allows them to establish data plane connections and to communicate with other routers in the overlay network.

Install Signed Certificates on vEdge Cloud Routers

When a vEdge Cloud router virtual machine (VM) instance starts, it has a factory-default configuration, which allows the router to boot. However, the router is unable to join the overlay network. For the router to be able to join the overlay network, you must install a signed certificate on the router. The signed certificates are generated based on the router's serial number, and they are used to authorize the router to participate in the overlay network.

Starting from Releases 17.1, the Cisco SD-WAN Manager can act as a Certificate Authority (CA), and in this role it can automatically generate and install signed certificates on vEdge Cloud routers. You can also use another CA and then install the signed certificate manually. For Releases 16.3 and earlier, you manually install signed Symantec certificates on vEdge Cloud routers.

To install signed certificates:

1. Retrieve the vEdge authorized serial number file. This file contains the serial numbers of all the vEdge routers that are allowed to join the overlay network.
2. Upload the vEdge authorized serial number file to Cisco SD-WAN Manager.
3. Install a signed certificate on each vEdge Cloud router.

Retrieve vEdge Authorized Serial Number File

1. Go to http://viptela.com/support/ and log in.
2. Click **Downloads**.
3. Click **My Serial Number Files**. The screen displays the serial number files. Starting from Releases 17.1, the filename extension is .viptela. For Releases 16.3 and earlier, the filename extension is .txt.
4. Click the most recent serial number file to download it.

Upload vEdge Authorized Serial Number File

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. Click **vEdge List**, and select **Upload vEdge List**.
3. In the Upload vEdge window:
   a. Click **Choose File**, and select the vEdge authorized serial number file you downloaded from Cisco.
   b. To automatically validate the vEdge routers and send their serial numbers to the controllers, click and select the checkbox **Validate the Uploaded vEdge List** and **Send to Controllers**. If you do not select this option, you must individually validate each router in the **Configuration** > **Certificates** > **vEdge List** page.
4. Click **Upload**.

During the process of uploading the vEdge authorized serial number file, the Cisco SD-WAN Manager generates a token for each vEdge Cloud router listed in the file. This token is used as a one-time password for the router. The Cisco SD-WAN Manager sends the token to the Cisco SD-WAN Validator and the Cisco SD-WAN Controller.

After the vEdge authorized serial number file has been uploaded, a list of vEdge routers in the network is displayed in the vEdge Routers Table in the **Configuration** > **Devices** page, with details about each router, including the router's chassis number and its token.

Install Signed Certificates in Releases 17.1 and Later

Starting from Releases 17.1, to install a signed certificates on a vEdge Cloud router, you first generate and download a bootstrap configuration file for the router. This file contains all the information necessary to allow the Cisco SD-WAN Manager to generate a signed certificate for the vEdge Cloud router. You then copy the

contents of this file into the configuration for the router's VM instance. For this method to work, the router and the Cisco SD-WAN Manager must both be running Release 17.1 or later. Finally, you download the signed certificate to the router. You can configure the Cisco SD-WAN Manager to do this automatically or manually.

The bootstrap configuration file contains the following information:

- UUID, which is used as the router's chassis number.
- Token, which is a randomly generated one-time password that the router uses to authenticate itself with the Cisco SD-WAN Validator and the Cisco SD-WAN Manager.
- IP address or DNS name of the Cisco SD-WAN Validator.
- Organization name.
- If you have already created a device configuration template and attached it to the vEdge Cloud router, the bootstrap configuration file contains this configuration. For information about creating and attaching a configuration template, see Create Configuration Templates for a vEdge Router .

You can generate a bootstrap configuration file that contains information for an individual router or for multiple routers.

Starting from Releases 17.1, you can also have Symantec generate signed certificates that you install manually on each router, as described later in this article, but this method is not recommended.

Configure the Cisco Catalyst SD-WAN Validator and Organization Name

Before you can generate a bootstrap configuration file, you must configure the Cisco SD-WAN Validator DNS name or address and your organization name:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. For Cisco SD-WAN Validator, click **Edit**.
3. In the Cisco SD-WAN Validator DNS/IP Address: Port field, enter the DNS name or IP address of the Cisco SD-WAN Validator.
4. Click **Save**.
5. For Organization Name, click **View** and verify the orgnization name configured. This name must be identical to that configured on the Cisco SD-WAN Validator.
6. Click **Save**.

Configure Automatic or Manual vEdge Cloud Authorization

Signed certificates must be installed on each vEdge cloud router so that the router is authorized to participate in the overlay network. You can use the Cisco SD-WAN Manager as the CA to generate and install the signed certificate, or you can use an enterprise CA to install the signed certificate.

It is recommended that you use the Cisco SD-WAN Manager as a CA. In this role, Cisco SD-WAN Manager automatically generates and installs a signed certificate on the vEdge Cloud router. Having Cisco SD-WAN Manager act as a CA is the default setting. You can view this setting in the WAN vEdge Cloud Certificate Authorization, on the Cisco SD-WAN Manager **Administration** > **Settings** page.

To use an enterprise CA for generating signed certificates for vEdge Cloud routers:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. For WAN Edge Cloud Certificate Authorization, select **Manual**.
3. Click **Save**.

Generate a Bootstrap Configuration File

Note In Cisco SD-WAN Release 20.5.1, the cloud-init bootstrap configuration that you generate for the Cisco vEdge Cloud router cannot be used for deploying Cisco vEdge Cloud router 20.5.1. However, you can use the bootstrap configuration for deploying Cisco vEdge Cloud router 20.4.1 and the earlier versions.

To generate a bootstrap configuration file for a vEdge Cloud router:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. To generate a bootstrap configuration file for one or multiple vEdge Cloud routers:
   a. Click **WAN Edge List**, select **Export Bootstrap Configuration**.
   b. In the Generate Bootstrap Configuration field, select the file format:
      - For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select **Cloud-Init** to generate a token, Cisco SD-WAN Validator IP address, vEdge Cloud router UUID, and organization name.
      - For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.
   c. From the **Available Devices** column, select one or more routers.
   d. Click the arrow pointing to right to move the selected routers to **Selected Devices** column.
   e. Click **Generate Generic Configuration**. The bootstrap configuration is downloaded in a .zip file, which contains one .cfg file for each router.
3. To generate a bootstrap configuration file individually for each vEdge Cloud router:
   a. Click **WAN Edge List**, select the desired vEdge Cloud router.
   b. For the desired vEdge Cloud router, click **...**, and select **Generate Bootstrap Configuration**.
   c. In the **Generate Bootstrap Configuration** window, select the file format:
      - For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select Cloud-Init to generate a token, Cisco SD-WAN Validator IP address, vEdge Cloud router UUID, and organization name.
      - For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.

Note Beginning with Cisco vManage Release 20.7.1, there is an option available when generating a bootstrap configuration file for a Cisco vEdge device, enabling you generate two different forms of the bootstrap configuration file.

- If you are generating a bootstrap configuration file for a Cisco vEdge device that is using Cisco Catalyst SD-WAN Release 20.4.x or earlier, then check the **The version of this device is 20.4.x or earlier** check box.
- If you are generating a bootstrap configuration for a Cisco vEdge device that is using Cisco SD-WAN Release 20.5.1 or later, then do not use the check box.

d. Click **Download** to download the bootstrap configuration. The bootstrap configuration is downloaded in a .cfg file.

Then use the contents of the bootstrap configuration file to configure the vEdge Cloud router instance in AWS, ESXi, or KVM. For example, to configure a router instance in AWS, paste the text of the Cloud-Init configuration into the User data field:

By default, the **ge0/0** interface is the router's tunnel interface, and it is configured as a DHCP client. To use a different interface or to use a static IP address, and if you did not attach a device configuration template to the router, change the vEdge Cloud router's configuration from the CLI. See *Configuring Network Interfaces*.

Install the Certificate on the vEdge Cloud Router

If you are using automated vEdge Cloud certificate authorization, which is the default, after you configure the vEdge Cloud router instance, Cisco SD-WAN Manager automatically installs a certificate on the router and the router's token changes to its serial number. You can view the router's serial number in the **Configuration** > **Devices** page. After the router's control connections to the Cisco SD-WAN Manager come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:

   ```
   vEdge# request root-cert-chain install filename [vpn vpn-id]
   ```

   Then, Cisco SD-WAN Manager generates a CSR.

2. Download the CSR:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. For the selected vEdge Cloud router for which to sign a certificate, click **...** and select **View CSR**.
   c. To download the CSR, click **Download**.
3. Send the certificate to a third-party signing authority, to have them sign it.
4. Import the certificate into the device:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. Click **Controllers**, and select **Install Certificate**.

c. In the **Install Certificate** page, paste the certificate into the Certificate Text field, or click **Select a File** to upload the certificate in a file.

d. Click **Install**.

5. Issue the following REST API call, specifying the IP address of your Cisco SD-WAN Manager:

```
https://vmanage-ip-address/dataservice/system/device/sync/rootcertchain
```

Create the vEdge Cloud Router Bootstrap Configuration from the CLI

It is recommended that you generate the vEdge Cloud router's bootstrap configuration using Cisco SD-WAN Manager. If, for some reason, you do not want to do this, you can create the bootstrap configuration using the CLI. With this process, you must still, however, use Cisco SD-WAN Manager. You collect some of this information for the bootstrap configuration from Cisco SD-WAN Manager, and after you have created the bootstrap configuration, you use Cisco SD-WAN Manager to install the signed certificate on the router.

Installing signed certificates by creating a bootstrap configuration from the CLI is a three-step process:

1. Edit the router's configuration file to add the DNS name or IP address of the Cisco SD-WAN Validator and your organization name.
2. Send the router's chassis and token numbers to Cisco SD-WAN Manager.
3. Have Cisco SD-WAN Manager authenticate the vEdge Cloud router and install the signed certificate on the router.

To edit the vEdge Cloud router's configuration file from the CLI:

1. Open a CLI session to the vEdge Cloud router via SSH. To do this in Cisco SD-WAN Manager, select **Tools** > **SSH Terminal** page, and select the desired router.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

```
vEdge# config
vEdge(config)#
```

4. Configure the IP address of the Cisco SD-WAN Validator or a DNS name that points to the Cisco SD-WAN Validator. The Cisco SD-WAN Validator's IP address must be a public IP address:

```
vEdge(config)# system vbond (dns-name | ip-address)
```

5. Configure the organization name:

```
vEdge(config-system)# organization-name name
```

6. Commit the configuration:

```
vEdge(config)# commit and-quit
vEdge#
```

To send the vEdge Cloud router's chassis and token numbers to Cisco SD-WAN Manager:

1. Locate the vEdge Cloud router's token and chassis number:

a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.

b. Click **WAN Edge List**, locate the vEdge Cloud router.

c. Make a note of the values in the vEdge Cloud router's Serial No./Token and Chassis Number columns.

2. Send the router's bootstrap configuration information to Cisco SD-WAN Manager:

```
vEdge# request vedge-cloud activate chassis-number chassis-number token token-number
```

Issue the **show control local-properties** command on the router to verify the Cisco SD-WAN Validator IP address, the organization name the chassis number, and the token. You can also verify whether the certificate is valid.

Finally, have Cisco SD-WAN Manager authenticate the vEdge Cloud router and install the signed certificate on the router.

If you are using automated vEdge Cloud certificate authorization, which is the default, the Cisco SD-WAN Manager uses the chassis and token numbers to authenticate the router. Then, Cisco SD-WAN Manager automatically installs a certificate on the router and the router's token changes to a serial number. You can display the router's serial number in the **Configuration** > **Devices** page. After the router's control connections to Cisco SD-WAN Manager come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:

```
vEdge# request root-cert-chain install filename [vpn vpn-id]
```

After you install the root chain certificate on the router, and after Cisco SD-WAN Manager receives the chassis and token numbers, Cisco SD-WAN Manager generates a CSR.

2. Download the CSR:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. For the selected vEdge Cloud router for which to sign a certificate, click **...** and select **View CSR**.
   c. To download the CSR, click **Download**.
3. Send the certificate to a third-party signing authority, to have them sign it.
4. Import the certificate into the device:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. Click Controllers and select **Install Certificate**.
   c. In the **Install Certificate** page, paste the certificate into the Certificate Text field, or click **Select a File** to upload the certificate in a file.
   d. Click **Install**.
5. Issue the following REST API call, specifying the IP address of your Cisco SD-WAN Manager:

https://*vmanage-ip-address***/dataservice/system/device/sync/rootcertchain**

Install Signed Certificates in Releases 16.3 and Earlier

For vEdge Cloud router virtual machine (VM) instances running Releases 16.3 and earlier, when the vEdge Cloud router VM starts, it has a factory-default configuration, but is unable to join the overlay network because

no signed certificate is installed. You must install a signed Symantec certificate on the vEdge Cloud router so that it can participate in the overlay network.

To generate a certificate signing request (CSR) and install the signed certificate on the vEdge Cloud router:

1. Log in to the vEdge Cloud router as the user **admin**, using the default password, **admin**. If the vEdge Cloud router is provided through AWS, use your AWS key pair to log in. The CLI prompt is displayed.
2. Generate a CSR for the vEdge Cloud router:

   ```
   vEdge# request csr upload path
   ```

   path is the full path and filename where you want to upload the CSR. The path can be in a directory on the local device or on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided. When prompted, enter and then confirm your organization name. For example:

   ```
   vEdge# request csr upload home/admin/vm9.csr
   Uploading CSR via VPN 0
   Enter organization name            : Cisco
   Re-enter organization name         : Cisco
   Generating CSR for this vEdge device
   ........[DONE]
   Copying ... /home/admin/vm9.csr via VPN 0
   CSR upload successful
   ```
3. Log in to the Symantec Certificate Enrollment portal:

   https://certmanager.<wbr>websecurity.symantec.com/<wbr>mcelp/enroll/index?jur_hash=<wbr>f422d7ceb508a24e32ea7de4f78d37<wbr>f8
4. In the **Select Certificate Type** drop-down, select **Standard Intranet SSL** and click **Go**. The Certificate Enrollment page is displayed. Cisco Catalyst SD-WAN uses the information you provide on this form to confirm the identity of the certificate requestor and to approve your certificate request. To complete the Certificate Enrollment form:
   a. In the Your Contact Information section, specify the First Name, Last Name, and Email Address of the requestor.
   b. In the Server Platform and Certificate Signing section, select Apache from the Select Server Platform drop-down. In the Enter Certificate Signing Request (CSR) box, upload the generated CSR file, or copy and paste the contents of the CSR file. (For details about how to do this, log in to support.viptela.com. Click Certificate, and read the Symantec certificate instructions.)
   c. In the Certificate Options section, enter the validity period for the certificate.
   d. In the Challenge Phrase section, enter and then re-enter a challenge phrase. You use the challenge phrase to renew, and, if necessary, to revoke a certificate on the Symantec Customer Portal. It is recommended that you specify a different challenge phrase for each CSR.
   e. Accept the Subscriber Agreement. The system generates a confirmation message and sends an email to the requestor confirming the certificate request. It also sends an email to the Cisco to approve the CSR.
5. After Cisco approves the CSR, Symantec sends the signed certificate to the requestor. The signed certificate is also available through the Symantec Enrollment portal.
6. Install the certificate on the vEdge Cloud router:

   ```
   vEdge# request certificate install filename [vpn vpn-id]
   ```

The file can be in your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided.

7. Verify that the certificate is installed and valid:

```
vEdge# show certificate validity
```

After you have installed the certificate on the vEdge Cloud router, the Cisco SD-WAN Validator is able to validate and authenticate the router, and the router is able to join the overlay network.

What's Next

See *Send vEdge Serial Numbers to the Controller Devices*.

Manage a Network Hierarchy

Table 217: Feature History

Feature Name	Release Information	Description
Network Hierarchy and Resource Management	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.
Network Hierarchy and Resource Management (Phase II)	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	You can create a system IP pool on the **Configuration** > **Network Hierarchy** page.
Support for Software Defined Remote Access Pools	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	Remote access refers to enabling secure access to an organization's network from devices at remote locations. The resource pool manager manages the IPv4 and IPv6 private IP address pools for Cisco Catalyst SD-WAN remote access devices. You can create a software defined remote access pool using the **Configuration** > **Network Hierarchy** page.

The Network Hierarchy and Resource Management feature enables you to do the following:

- Create a region
- Create an area
- Create, edit, and delete a site

Create a Region in a Network Hierarchy

Before You Begin

Ensure that the **Multi-Region Fabric** option in Cisco SD-WAN Manager is enabled.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit** adjacent to the **Multi-Region Fabric** option.
3. Click **Enabled**, and then click **Save**.

Create a Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global or area) in the left pane and choose **Add MRF Region**.

Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add a region.

3. In the **Name** field, enter a name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the region.
5. From the **Parent** drop-down list, choose a parent node.
6. Click **Add**.

Create an Area in a Network Hierarchy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global, region, or area) in the left pane and choose **Add Area**.

Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add an area.

3. In the **Name** field, enter a name for the area. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the area.
5. From the **Parent** drop-down list, choose a parent node.
6. Click **Add**.

Create a Site in a Network Hierarchy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

2. Click **…** adjacent to a node (global, region, or area) in the left pane and choose **Add Site**.

Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add a site.

3. In the **Name** field, enter a name for the site. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the site.
5. From the **Parent** drop-down list, choose a parent node.
6. In the **Site ID** field, enter a site ID.

   If you do not enter the site ID, Cisco SD-WAN Manager generates a site ID for the site.
7. Click **Add**.

Create a System IP Pool

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

   The page displays the site pool and region pool for the Global node.
2. Click **Add**.
3. In the **Pool Name** field, enter a name for the pool.
4. In the **Pool Description** field, enter a description of the pool.
5. From the **Pool Type** drop-down list, choose **System IP**.
6. In the **IP Subnet*** field, enter an IP address.
7. In the **Prefix Length*** field, enter the prefix length of the system IP pool.
8. Click **Add**.

Note You can create only one system IP pool. If you want to make any changes to the pool, you must edit the existing pool.

Assign a Site ID to a Device

You can assign a site ID to a device using one of the following ways.

Use the Quick Connect Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Quick Connect** workflow.

3. Follow the instructions provided in the workflow.
4. On the **Add and Review Device Configuration** page, enter the site ID of the device.

Note

- You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
- (Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1) If you want Cisco SD-WAN Manager to automatically generate a site ID for the device, do not make any change to the default value, **AUTO**.

Use a Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
2. Check if a device is attached to a device template.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.
4. Click **…** adjacent to the System feature template and choose **Edit**.
5. Click the **Basic Configuration** tab and set the scope of the **Site ID** field to **Global** and enter the site ID.
6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

In Step 5, if you set the scope of the **Site ID** field to **Device Specific**, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.
2. Click **…** adjacent to the device template and choose **Edit Device Template**.
3. In the **Site ID** field, enter the site ID.

   You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
4. Click **Update**.
5. Click **Configure Devices** to push the configuration to the device.

Use a Configuration Group

The configuration group flow is applicable only for the Cisco IOS XE Catalyst SD-WAN devices.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**.
4. Choose a device that is associated with the configuration group and click **Deploy**.

The **Deploy Configuration Group** workflow starts.

5. Follow the instructions provided in the workflow.
6. On the **Add and Review Device Configuration** page, enter the site ID of the device.

   You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

Assign a Region ID to a Device

Before You Begin

- Have access to the **Multi-Region Fabric** feature.
- Ensure that the region is available in the network hierarchy.

Assign a Region ID

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
2. Check if the corresponding device is attached to a device template.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.
4. Click **…** adjacent to the System feature template and choose **Edit**.
5. Click the **Basic Configuration** tab and set the scope of the **Region ID** field to **Global** and enter the region ID.

   You can use any of the existing region IDs that are available in the network hierarchy. If the specified region ID is not available in the network hierarchy, the template push operation to the devices fails.
6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

In Step 5, if you set the scope of the **Region ID** field to **Device Specific**, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.
2. Click **…** adjacent to the device template and choose **Edit Device Template**.
3. In the **Region ID** field, enter the region ID.
4. Click **Update**.
5. Click **Configure Devices** to push the configuration to the device.

Assign a System IP to a Device

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

2. Start the **Quick Connect** workflow.
3. Follow the instructions provided in the workflow.
4. On the **Add and Review Device Configuration** page, enter the system IP of the device. If you want Cisco SD-WAN Manager to automatically generate a system IP for the device, do not make any change to the default value, **AUTO**.

Assign a Hostname to a Device

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Quick Connect** workflow.
3. Follow the instructions provided in the workflow.
4. On the **Add and Review Device Configuration** page, enter the hostname of the device. If you want Cisco SD-WAN Manager to automatically generate a hostname for the device, do not make any change to the default value, **AUTO**.

Manage Certificates in Cisco Catalyst SD-WAN Manager

Perform certificate operations in Cisco SD-WAN Manager on the **Configuration** > **Certificates** page.

- Top bar—On the left are the menu icon, for expanding and collapsing the Cisco SD-WAN Manager menu, and the Cisco SD-WAN Manager product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Certificates.
- WAN Edge List tab—Install the router authorized serial number file on the controllers in the overlay network and manage the serial numbers in the file. When you first open the Certificates screen, the WAN Edge List tab is selected.
  - Send to Controllers—Send the WAN edge router chassis and serial numbers to the controllers in the network.
  - Table of WAN edge routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Controllers tab—Install certificates and download the device serial numbers to the Cisco SD-WAN Validator.
  - Send to Cisco SD-WAN Validator—Send the controller serial numbers to the Cisco SD-WAN Validator.
  - Install Certificate—Install the signed certificates on the controller devices. This button is available only if you select Manual in **Administration** > **Settings** > **Certificate Signing by Symantec**.
  - Export Root Certificate—Display a copy of the root certificate for the controller devices that you can download to a file.

- Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Certificate status bar—Located at the bottom of the screen, this bar is available only if you select Server Automated in **Administration** > **Settings** > **Certificate Authorization**. It displays the states of the certificate installation process:
  - Device Added
  - Generate CSR
  - Waiting for Certificate
  - Send to Controllers

  A green check mark indicates that the step has been completed. A grey check mark indicates that the step has not yet been performed.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.
- Show Table Fields icon—Click the icon to display or hide columns from the device table. By default, all columns are displayed.

Authorize a Controller Certificate for an Enterprise Root Certificate

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Controller Certificate Authorization** area, click **Edit**.
3. Click **Enterprise Root Certificate**. If a warning appears, click **Proceed** to continue.
4. Optionally, click **Set CSR Properties** to configure certificate signing request (CSR) details manually.

Note In a multi-tenant scenario, if you configure CSR properties manually and if you are using Cisco Catalyst SD-WAN Control Components Release 20.11.1 or later, then ensure that devices in the network are using Cisco IOS XE Catalyst SD-WAN Release 17.11.1a or later. In a single-tenant scenario, this is not required.

In a multi-tenant scenario, if you configure CSR properties manually, then when you are ready to generate a CSR for a tenant device, enter the tenant's organization name in the **Secondary Organizational Unit** field described below. In a multi-tenant scenario, if you are generating a CSR for a service provider device, this is not required.

The following properties appear:

- **Domain Name**: Network domain name
- **Organizational Unit**

Note **Organizational Unit** is a noneditable field. This field is auto-filled with the organization name that you have configured for Cisco SD-WAN Manager in **Administration** > **Settings** > **Organization Name**.

- **Secondary Organizational Unit**: This optional field is only available in Cisco IOS XE Release 17.2 or Cisco SD-WAN Release 20.1.x and onwards. Note that if this optional field is specified, it will be applied to all controllers and edge devices.
- **Organization**: Beginning with Cisco vManage Release 20.11.1, when configuring controller certificate authorization for enterprise certificates on WAN edge cloud devices, you can specify any organization in this field. You are not limited to names such as **Viptela LLC**, **vIPtela Inc**, or **Cisco Systems**. This enables you to use your organization's certificate authority name or a third-party certificate authority name. The maximum length is 64 characters, and can include spaces and special characters. Cisco SD-WAN Manager validates the name when you enter it.
- **City**
- **State**
- **Email**
- **2-Letter Country Code**
- **Subject Altenative Name (SAN) DNS Names**: (optional) You can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com
- **Subject Altenative Name (SAN) URIs**: (optional) You can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

5. Paste an SSL certificate into the **Certificate** field or click **Select a file** and navigate to an SSL certificate file.
6. (Optional) In the **Subject Alternative Name (SAN) DNS Names** field, you can enter multiple host names to use the same SSL certificate.

   Example: cisco.com and cisco2.com
7. (Optional) In the **Subject Alternative Name (SAN) URIs** field, you can enter multiple URIs to use the same SSL certificate.

   Example: cisco.com and support.cisco.com

   This is helpful for an organization that uses a single certificate for a host name, without using different subdomains for different parts of the organization.

Check the WAN Edge Router Certificate Status

In the **WAN Edge List** tab, check the **Validate** column. The status can be one of the following:

- Valid (shown in green)—The router's certificate is valid.
- Staging (shown in yellow)—The router is in the staging state.
- Invalid (shown in red)—The router's certificate is not valid.

Validate a WAN Edge Router

When you add Cisco vEdge devices and WAN routers to the network using the **Configuration** > **Devices** screen, you can automatically validate the routers and send their chassis and serial numbers to the controller devices by clicking the checkbox Validate the uploaded WAN Edge List and send to controllers. If you do not select this option, you must individually validate each router and send their chassis and serial numbers to the controller devices. To do so:

1. In the **WAN Edge List** tab, select the router to validate.
2. In the **Validate** column, click **Valid**.
3. Click **OK** to confirm the move to the valid state.
4. Repeat the steps above for each router you wish to validate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco SD-WAN Manager NMS displays the Push WAN Edge List screen showing the status of the push operation.

Stage a WAN Edge Router

When you initially bring up and configure a WAN Edge router, you can place it in staging state using the Cisco SD-WAN Manager instance. When the router is in this state, you can configure the router, and you can test that the router is able to establish operational connections with the Cisco SD-WAN Controller and the Cisco SD-WAN Manager instance.

After you physically place the router at its production site, you change the router's state from staging to valid. It is only at this point that the router joins the actual production network. To stage a router:

1. In the WAN Edge List tab, select the router to stage.
2. In the **Validate** column, click **Staging**.
3. Click **OK** to confirm the move to the staging state.
4. Click **Send to Controllers** in the upper left corner of the screen to sync the WAN edge authorized serial number file with the controllers. Cisco SD-WAN Manager NMS displays the **Push WAN Edge List** screen showing the status of the push operation.
5. To unstage, validate the WAN Edge Router.

Invalidate a WAN Edge Router

1. In the **WAN Edge List** tab, select the router to invalidate.
2. In the **Validate** column, click **Invalid**.
3. Click **OK** to confirm the move to the invalid state.
4. Repeat the steps above for each router you wish to invalidate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco SD-WAN Manager instance displays the **Push WAN Edge List** screen showing the status of the push operation.

Send the Controller Serial Numbers to Cisco Catalyst SD-WAN Validator

To determine which controllers in the overlay network are valid, the Cisco SD-WAN Validator keeps a list of the controller serial numbers. The Cisco SD-WAN Manager instance learns these serial numbers during the certificate-generation process.

To send the controller serial numbers to the Cisco SD-WAN Validator:

1. In the **Controllers** tab, check the certificate status bar at the bottom of the screen. If the **Send to Controllers** check mark is green, all serial numbers have already been sent to the Cisco SD-WAN Validator. If it is grey, you can send one or more serial numbers to the Cisco SD-WAN Validator.
2. Click the **Send to vBond** button in the **Controllers** tab. A controller's serial number is sent only once to the Cisco SD-WAN Validator. If all serial numbers have been sent, when you click **Send to vBond**, an error message is displayed. To resend a controller's serial number, you must first select the device and then select **Invalid in the Validity** column.

After the serial numbers have been sent, click the **Tasks** icon in the Cisco SD-WAN Manager toolbar to display a log of the file download and other recent activities.

Install Signed Certificate

If in **Administration** > **Settings** > **Certificate Signing by Symantec**, you selected the **Manual** option for the certificate-generation process, use the **Install Certificate** button to manually install certificates on the controller devices.

After Symantec or your enterprise root CA has signed the certificates, they return the files containing the individual signed certificates. Place them on a server in your local network. Then install them on each controller:

1. In the **Controllers** tab, click **Install Certificate**.
2. In the **Install Certificate** window, select a file, or copy and paste the certificate text.
3. Click **Install** to install the certificate on the device. The certificate contains information that identifies the controller, so you do not need to select the device on which to install the certificate.
4. Repeat Steps the steps above to install additional certificates.

Export Root Certificate

1. In the **Controllers** tab, click the **Export Root Certificate** button.
2. In the **Export Root Certificate** window, click **Download** to export the root certificate to a file.
3. Click **Close**.

View a Certificate Signing Request

1. In the WAN Edge List or **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row, and click **View CSR** to view the certificate signing request (CSR).

View a Device Certificate Signing Request

1. In the **WAN Edge List** or **Controllers** tab, select a Cisco IOS XE Catalyst SD-WAN device.
2. Click the **More Actions** icon to the right of the row, and click **View Device CSR** to view the certificate signing request (CSR).

   For a Cisco IOS XE Catalyst SD-WAN device where trustpoint has been configured, clicking the **More Actions** icon allows you to view three options:

   - View Device CSR
   - Generate Feature CSR
   - View Feature CSR

Note Cisco SD-WAN Manager will generate alarms only if device certificate is installed through Cisco SD-WAN Manager. If you install certificate manually, Cisco SD-WAN Manager will not generate alarms for certificate expiration.

View the Certificate

1. In the **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row and click **View Certificate**.

Generate a Controller Certificate Signing Request

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **Controllers**.
3. For the desired controller, click **…** and choose **Generate CSR**.

   The **Generate CSR** window is displayed.
4. In the **Generate CSR** window, click **Download** to download the file to your local PC (that is, to the PC you are using to connect to the Cisco SD-WAN Manager NMS).
5. Repeat the preceding steps to generate a CSR for another controller.

Generate a Feature Certificate Signing Request

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired device, click **…** and choose **Generate Feature CSR**.

   The **Generate Feature CSR** window is displayed.

4. In the **Generate Feature CSR** window, click **OK** to continue with the generation of feature CSR. This step authenticates the device trustpoint that has been set and extracts the CSR from the device.
5. Repeat the steps above for each device for which you are generating a CSR.

Reset the RSA Key Pair

1. In the **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row and click **Reset RSA**.
3. Click **OK** to confirm resetting of the device's RSA key and to generate a new CSR with new public or private keys.

Invalidate a Device

1. In the **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row and click **Invalidate**.
3. Click **OK** to confirm invalidation of the device.

View Log of Certificate Activities

To view the status of certificate-related activities:

1. Click the **Tasks** icon located in the Cisco SD-WAN Manager toolbar. Cisco SD-WAN Manager NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. Cisco SD-WAN Manager NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

View a Signed Certificate

Signed certificates are used to authenticate Cisco SD-WAN devices in the overlay network. To view the contents of a signed certificate using Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **Controllers**.
3. For the desired device, click **...** and choose **View Certificate** to view the installed certificate.

Manage Root Certificate Authority Certificates in Cisco Catalyst SD-WAN Manager

Feature Name	Release Information	Description
Support for Managing Root CA Certificates in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	Add and manage root certificate authority (CA) certificates.

Add a Root Certificate Authority Certificate

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. In the **Root Certificate** field, paste in certificate text, or click **Select a File** to load a certificate from a file.
4. Click **Add**. The new certificate appears in the certificate table. The **Recent Status** column indicates that the certificate has not yet been installed.
5. Click **Next** and review the details of any certificates that have not been installed.
6. Click **Save** to install the certificate(s). The new certificate appears in the certificate table.

View a Root Certificate Authority Certificate

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. (optional) In the search field, enter text to filter the certificate view. You can filter by certificate text or attribute values, such as serial number.
3. In the table of certificates, click **More Actions** (**…**) and choose **View**. A pop-up window appears, displaying the certificate and its details.

Delete a Root Certificate

Use this procedure to delete a root Certificate Authority (CA) certificate.

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. Select one or more root certificates in the table and click the **trash** icon in the **Action** column. The table shows the certificate as marked for deletion.
4. Click **Next** and review the details of any certificates that are marked for deletion.
5. Click **Save** to delete the certificate(s).

Manage Device Templates

Table 218: Feature History

Feature Name	Release Information	Description
Support for Draft Mode in Device Template	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	To save device template configuration changes in Cisco SD-WAN Manager, enable the draft mode. To save device template configuration changes on the devices attached to the template, disable the draft mode.

Edit a Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** or **Feature Templates**, and select a template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Edit**.

You cannot change the name of a device or feature template when that is attached to a device.

Note You can edit templates simultaneously from one or more Cisco SD-WAN Manager servers. For simultaneous template edit operations, the following rules apply:

- You cannot edit the same device or feature template simultaneously.
- When you are editing a device template, all other feature templates attached to that device template are locked and you cannot perform any edit operations on them.
- When you are editing a feature template that is attached to a device template, that device template as well as all other feature templates attached to it are locked and you cannot perform any edit operations on them.

Delete a Template

Deleting a template does not remove the associated configuration from devices.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** or **Feature Templates**, and select a template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Delete**.
4. To confirm the deletion of the template, click **OK**.

Copy a Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** or **Feature Templates**, and select a template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Copy**.
4. Enter a new template name and description.
5. Click **Copy**.

Edit a CLI Device Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Edit**.
4. Under **Device CLI Template**, edit the template.
5. Click **Update**.

Manage Licenses for Smart Licensing Using Policy

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

Table 219: Feature History

Feature Name	Release Information	Description
License Management for Smart Licensing Using Policy, Using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	Cisco SD-WAN Manager shows available DNA licenses, assigns licenses to devices, and reports license consumption to Cisco Smart Software Manager (Cisco SSM).
Support for License Management Offline Mode and Compliance Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	You can manage Cisco Catalyst SD-WAN licenses through a Cisco SD-WAN Manager instance that is not connected to the internet. To synchronize license and compliance information between Cisco SD-WAN Manager and Cisco SSM, you must periodically download synchronization files from Cisco SD-WAN Manager and upload the files to Cisco SSM.
Support for Postpaid MSLA License Billing Models	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	For postpaid Managed Services License Agreement (MSLA) program licenses, Cisco Catalyst SD-WAN supports two distinct billing models for licenses—committed (MSLA-C) and uncommitted (MSLA-U). The procedure for assigning a postpaid license enables you to choose one of these two MSLA license types.
Support for License Management Using a Proxy Server	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	If you configure Cisco SD-WAN Manager to use a proxy server for internet access, Cisco SD-WAN Manager uses the proxy server to connect to Cisco SSM or an on-prem SSM.

Feature Name	Release Information	Description
Support for Managing Licenses Using Cisco Smart Software Manager On-Prem	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	Cisco SD-WAN Manager can synchronize device licenses using a Cisco SSM on-prem license server. This is useful for organizations that use Cisco SSM on-prem to accommodate a strict security policy that does not permit devices to communicate with Cisco SSM over a direct internet connection.

Configure the License Reporting Mode

Before You Begin

When using Cisco Catalyst SD-WAN multitenancy, only the service provider configures the Cisco SSM license server details, using the license server credentials.

Configure the License Reporting Mode

1. For Cisco vManage Release 20.9.1 and later, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Note In Cisco vManage Release 20.8.x and earlier, to configure the license reporting mode, from the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**. Click **Sync Licenses & Refresh Devices** and choose a license reporting mode. Then continue with the procedure for synchronizing licenses.

2. In the **License Reporting** section, click **Edit** and choose one of the following:

Note Changing the mode causes Cisco SD-WAN Manager to permanently clear any license information that it is currently storing.

- Online
- Offline
- On-prem

Enter the following information for the Cisco SSM on-prem server:

Field	Description
SSM Server	IP address of the Cisco SSM on-prem license server.
SSM Credentials **Client ID** and **Client Secret**	Client ID and client secret credentials for the Cisco SSM on-prem license server. This information is available from the administrator who manages the license server.

3. Click **Save**.

Enter Smart Account Credentials in Cisco Catalyst SD-WAN Manager

Before You Begin

Ensure that you have configured DNS host and next-hop IP route entries for the Cisco SSM servers under VPN 0 on Cisco SD-WAN Manager. Without this configuration, Cisco SD-WAN Manager cannot communicate with Cisco SSM.

Enter Smart Account Credentials

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
2. Click **Sync Licenses & Refresh Devices**.

   The **Reporting Mode** area shows the reporting mode configured on the **Administration** > **Settings** page (requires administrator permissions).
3. Click **Smart Account Credentials**.
4. In the **Smart Account Credentials** dialog box, configure the following:

Field	Description
Username	Username of the account you use to access the Smart Accounts and Virtual Accounts for which you have administrative privileges.
Password	Password for the account you use to access Smart Accounts and Virtual Accounts.

5. Click **Save**.

   Cisco SD-WAN Manager authenticates the Smart Account credentials, and on successful authentication, saves the credentials in the database.

Synchronize Licenses

Before You Begin

- You use this procedure to specify Smart Account and Virtual Account information, or synchronize licenses on-demand, which is useful if you have recently added licenses to your Smart Account and want to bring those licenses into Cisco SD-WAN Manager.
- Ensure licenses belong to the correct Smart Accounts or Virtual Accounts on Cisco SSM.

  When the selected Smart Accounts and Virtual Accounts are registered with Cisco SD-WAN Manager, Cisco SD-WAN Manager fetches and synchronizes the license information with Cisco SSM, and reports usage of the licenses in these accounts.

Synchronize Licenses

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
2. Click **Sync Licenses & Refresh Devices**.
3. In the **Sync Licenses & Refresh Devices** dialog box, configure the following:

Note If these details are already configured, you can skip this step and proceed to the next step to synchronize licenses again. This is useful if you have recently added licenses to your Smart Account and want to bring those licenses into Cisco SD-WAN Manager.

Item	Description
Select Smart/Virtual Accounts to Fetch/Sync Licenses	Select the Smart Accounts or Virtual Accounts for which Cisco SD-WAN Manager must fetch licenses from the Cisco SSM. Cisco SD-WAN Manager also reports license usage for the licenses in these accounts. **Note** Selecting an Smart Account automatically selects all the Virtual Accounts under the Smart Account. To stop Cisco SD-WAN Manager from fetching and synchronizing license information with Cisco SSM for an Smart Account or Virtual Account registered earlier, deselect the Smart Account or Virtual Account. You can deregister the Smart Account or Virtual Account only if you have not assigned any licenses from the account.
Advanced > **Type of Licenses**	Choose the type of licenses that must be fetched by Cisco SD-WAN Manager from among the license types that may belong to the selected Smart Accounts and Virtual Accounts. Select one of the following: • **Prepaid** • **Postpaid** • **Mixed** (both Prepaid and Postpaid) From Cisco vManage Release 20.8.1, if you choose to synchronize postpaid licenses, the license assignment procedure enables you to select committed MSLA licenses (MSLA-C) or uncommitted MSLA licenses (MSLA-U). See Assign a License to a Device.

Item	Description
Advanced > **Multiple Entitlement**	Select one of the following: • **On**: You can assign more than one license to a device. • **Off**: You can assign only one license to a device. **Note** Set this setting to **On** only if you need to map more than one DNA entitlement to a single device.

4. Click **Sync**.

Assign a License to a Device

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
2. Click **Device**.
3. Select the devices to which to assign a license using the check box for each device.
4. Click **Assign License/Subscription**.

   The **Assign License/Subscription** dialog box appears.
5. In the **Assign License/Subscription** dialog box, configure the following:
   - In Cisco vManage Release 20.8.1 and later, the following options appear:

Template Name	To use a new template, enter a unique name for the template. To use an existing template, do the following: **a.** Turn on the **Use existing template** toggle. **b.** Choose an existing template.
Virtual Account	Choose the virtual account from which you wish to assign a license to the device.
MSLA Type	Choose one of the following: • **MSLA-C**: MSLA licenses using the committed billing model • **MSLA-U**: MSLA licenses using the uncommitted billing model
Subscription ID	Choose the subscription ID to track the license consumption. This option appears only if both of the following are true: • The license mode is postpaid. • You have chosen an option in the **MSLA Type** field.

License	Choose license to apply to the device. If you have enabled Multiple Entitlements in the **Sync Licenses & Refresh Devices** dialog box, you can assign up to three licenses to the device. **Note** • Select a license that belongs to the Virtual Account you have selected. On Cisco SSM, you can check the licenses that are available in a Virtual Account. • Check the device license applicability matrix in the Cisco DNA Software for SD-WAN and Routing Ordering Guide to ensure that you assign a license that is applicable to the device. Different device models support different throughputs. If you apply an incompatible license, the license may have no effect on device behavior. However, Cisco SD-WAN Manager will record the consumption of the license. • When assigning licenses, Cisco SD-WAN Manager shows the throughput entitlement levels as tiers. Select the tier that matches the license you have purchased. If you purchased a license with a throughput expressed as a throughput value, find the tier that corresponds to the throughput that the license provides. For example, for a Routing DNA Advantage license, Tier 2 provides up to 1 Gbps throughput. If your DNA Advantage license provides 1 Gbps, choose Tier 2. Tier 0: 10M-15M (up to 30M aggregate) Tier 1: 25M-100M (up to 200M aggregate) Tier 2: 250M-1G (up to 2G aggregate) Tier 3: 2.5G-10G (up to 20G aggregate) The list includes the predefined licenses that Cisco SD-WAN Manager provides, together with the licenses in the virtual account that you have chosen, that meet the MSLA type and subscription ID criteria.

• In Cisco vManage Release 20.7.x and earlier, the following options appear:

Are you using utility-based licensing (MSLA)?	Check this check box if you wish to apply an MSLA license. By default, the check box is unchecked.
Template Name	To use a new template, enter a unique name for the template. To use an existing template, do the following: **a.** Turn on the **Use existing template** toggle. **b.** Choose an existing template.
Virtual Account	Choose the virtual account from which you wish to assign a license to the device.

License	Choose license to apply to the device. If you have enabled Multiple Entitlements in the **Sync Licenses & Refresh Devices** dialog box, you can assign up to three licenses to the device. **Note** • Select a license that belongs to the Virtual Account you have selected. On Cisco SSM, you can check the licenses that are available in a Virtual Account. • Check the device license applicability matrix in the Cisco DNA Software for SD-WAN and Routing Ordering Guide to ensure that you assign a license that is applicable to the device. Different device models support different throughputs. If you apply an incompatible license, the license may have no effect on device behavior. However, Cisco SD-WAN Manager will record the consumption of the license. • When assigning licenses, Cisco SD-WAN Manager shows the throughput entitlement levels as tiers. Select the tier that matches the license you have purchased. If you purchased a license with a throughput expressed as a throughput value, find the tier that corresponds to the throughput that the license provides. For example, for a Routing DNA Advantage license, Tier 2 provides up to 1 Gbps throughput. If your DNA Advantage license provides 1 Gbps, choose Tier 2. Tier 0: 10M-15M (up to 30M aggregate) Tier 1: 25M-100M (up to 200M aggregate) Tier 2: 250M-1G (up to 2G aggregate) Tier 3: 2.5G-10G (up to 20G aggregate)
Subscription ID	Choose the subscription ID to be used to track the license consumption. The subscription ID field is displayed only for the following conditions: • if mode is postpaid. • if mode is mixed and MSLA is true and if there are any subscriptions available.

6. Click **Save**.

The license is assigned and you are returned to **License Management** > **Device** tab. In the table listing the devices, entries are made in the following columns in accordance with the license assignment:

- Template Name: name of the template used to assign the license
- Virtual Account: name of Virtual Account to which license belongs
- MSLA:
  - True for an MSLA license

    - False for an a la carte or EA license

- License Status: subscribed
- License Type: prepaid, postpaid, or mixed based on the types of licenses assigned to the device.
- Subscription ID: The subscription ID used for billing purposes in case of a postpaid license. For a prepaid license, this column has a blank entry.

Monitor License Usage

License Management Overview

From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management** to display the **License Management Overview**.

The **License Management Overview** page shows license information, including what percentage of devices have licenses assigned, the top types of licenses assigned to devices, license usage, license alarms, and so on.

License alarms alert you to licensing issues affecting devices in the Cisco Catalyst SD-WAN network. You can click the alarm icon to display details of the problem. Issues include the following:

- A device is not licensed.
- The interval for reporting license usage to Cisco SSM has been exceeded.
    - Prepaid licenses: A report is required every three months.
    - Postpaid licenses: A report is required each month.

License Management Overview

After you have assigned at least one license, the **Overview** tab in the **Administration** > **License Management** page provides the following information:

Device Assignment Distribution	• Percentage of licensed devices • Percentage of unlicensed devices
Top 5 licenses	Lists the top 5 licenses in use and shows the usage percentage for each license.
License Usage vs Availability	The dashlet features a bar chart with stacked columns. The chart uses two stacked columns for each of the three license packages Advantage, Essentials, and Premier. For each package, the column on the left represents the count of used licenses; the column on the right represents the count of available licenses. The stacked segments in each column represent a particular license tier (such as Tier 0 or Tier 1). The segment for each tier is of a different color, as identified in the legend.

License and Devices Overview	This section provides the following details for each license assigned: • Name (for example, Routing DNA Essentials: Tier 0) • Number of Licensed Devices: Number of devices to which this license is assigned. • Number of Total Licenses: Sum of the number of licenses assigned and number of licenses available. • Last Assigned On: Date and time when the license was most recently assigned.

Enable Offline Mode

Before You Begin

Note Changing the mode from online to offline, or from offline to online causes Cisco SD-WAN Manager to permanently clear any license information that it is currently storing.

Enable Offline Mode, Cisco vManage Release 20.9.1 and Later

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **License Reporting** area, click the **Offline** option.

Enable Offline Mode, Before Cisco vManage Release 20.9.1

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
2. Click **Overview**.
3. Click **Sync Licenses & Refresh Devices**.
4. Click the **Offline** option.
5. (Optional) Click **Advanced** and select license types or configure multiple entitlement. For information about these options, see Fetch and Synchronize Licenses.
6. Click **Sync**.

Note If you are configuring offline mode for the first time, we recommend uploading a license summary file. See Generate a Cisco SSM License Summary File and Upload It into Cisco Catalyst SD-WAN Manager.

Generate a Cisco SSM License Summary File and Upload It into Cisco Catalyst SD-WAN Manager

Generating a license summary file in Cisco SSM and uploading the file to Cisco SD-WAN Manager brings all of the license information from your Cisco smart account into Cisco SD-WAN Manager.

Note Generating a license summary file in the Cisco SSM portal is outside the scope of Cisco Catalyst SD-WAN documentation and is subject to change.

1. In Cisco Software Central, navigate to **Manage Licenses**, then navigate to **Reports**.
2. Locate the option for downloading a synchronization file for device controllers. Specify Cisco SD-WAN Manager as the controller type, and include all virtual accounts.
3. Download the license summary file, which is in tar.gz format.
4. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
5. Click **Overview**.
6. Click **Sync Licenses & Refresh Devices**.
7. Click the **Offline** option.
8. In the **Attach License File** area, click the option to upload a file. Browse to the license summary file and upload it.
9. Click **Sync**.

Generate a Usage Report File in Cisco Catalyst SD-WAN Manager and Synchronize with Cisco SSM

When managing licenses with Cisco SD-WAN Manager in the offline mode, use manually generated files to enable Cisco SD-WAN Manager to provide information about license assignment to Cisco SSM.

To generate a usage report file in Cisco SD-WAN Manager, upload it to Cisco SSM, receive an acknowledgement file from Cisco SSM, and upload the acknowledgement file to Cisco SD-WAN Manager, perform the following steps.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
2. Click **Reporting**.
3. In the table, in the row with the Cisco Smart Account, click **…** and choose **Generate Report** to generate the usage report file.

   When you generate a report, the Cisco Catalyst SD-WAN Controller starts a 48-hour timer. If you do not upload an acknowledgement file from Cisco SSM within that time, an alert appears in the **License Management Overview** dashboard.
4. In Cisco SSM, upload the usage report file.

Note The details of procedures in the Cisco SSM portal are outside the scope of this documentation and subject to change.

a. In Cisco Software Central, navigate to **Manage Licenses**.

b. Navigate to **Reports**.

c. Navigate to **Upload Usage Data** > **Select and Upload File** or the equivalent, and upload the report file generated by Cisco SD-WAN Manager.

d. If prompted to select a virtual account, select the desired virtual account.

Note In a scenario where you have not yet generated a license summary in Cisco SSM and uploaded it to Cisco SD-WAN Manager, Cisco SSM prompts you to select a virtual account. After you have generated a license summary in Cisco SSM and uploaded it to Cisco SD-WAN Manager, Cisco SD-WAN Manager has the virtual account information that it needs to associate licenses with the correct virtual account.

For information about the scenario of assigning licenses to devices before providing Smart Account details to Cisco SD-WAN Manager, see Information About Offline Mode

.

Cisco SSM generates an acknowledgement file.

e. When Cisco SSM finishes generating an acknowledgement file, click **Download** or the equivalent to download the file.

5. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
6. Click **Reporting**.
7. In the table, in the row with the Cisco Smart Account, click **…** and choose **Upload Ack** to upload the acknowledgement file from Cisco SSM.

Manage HSEC Licenses

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

Table 220: Feature History

Feature Name	Release Information	Description
Manage HSEC Licenses	Cisco IOS XE Catalyst SD-WAN Release 17.9.2a Cisco vManage Release 20.9.2	You can use Cisco SD-WAN Manager to install HSEC licenses on devices An HSEC license is required to enable devices to support encrypted traffic throughput of 250 Mbps or higher.

Synchronize HSEC Licenses, Online Mode

Information about synchronizing HSEC licenses in the online mode.

Before You Begin

- This procedure requires Cisco SD-WAN Manager to have internet access. If Cisco SD-WAN Manager does not have internet access, such as for security reasons, use the Synchronize HSEC Licenses, Offline Mode, on page 614 procedure.
- This procedure requires entering credentials for your Cisco Smart Account

Synchronize HSEC Licenses, Online Mode

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Click the **Sync and Install HSEC Devices** workflow.
3. Click **Sync Licenses** and then click **Next**.
4. Click **Online** and then click **Next**.
5. Enter the credentials for your Cisco SSM account and then click **Next**.
6. On the **HSEC Device Activation Overview** page, click **Next**.
7. On the **Select Virtual Account** page, choose a virtual account from the drop-down list. The list is populated by the Cisco SSM account that you logged into in a previous step.
8. On the **Select HSEC-Compatible Devices** page, select the devices on which you want to install an HSEC license and then click **Summary**.

Note If an HSEC-compatible device already has an HSEC license installed by Cisco SD-WAN Manager, then the device is not selectable.

9. Review the summary and then click **Assign** to begin the synchronization. Cisco SD-WAN Manager loads the requested licenses from Cisco SSM and assigns them to the devices.
10. The process of loading and assigning licenses may take several minutes. You can monitor the progress by viewing the Cisco SD-WAN Manager task list.

11. After the HSEC licenses have been loaded and assigned, to install them, use the Install HSEC Licenses, on page 615 procedure.

Synchronize HSEC Licenses, Offline Mode

Before You Begin

- If Cisco SD-WAN Manager has internet access, we recommend using the Synchronize HSEC Licenses, Online Mode, on page 613 procedure.
- Use this procedure if Cisco SD-WAN Manager does not have internet access, such as for security reasons.
- This procedure requires entering credentials for your Cisco SSM Account.

Synchronize HSEC Licenses, Offline Mode

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Click the **Sync and Install HSEC Licenses** workflow.
3. Click **Sync Licenses** and then click **Next**.
4. Click **Offline** and then click **Next**.
5. On the **HSEC Device Activation Overview** page, click **Next**.
6. Click **Download Process** and then click **Next**.
7. On the **Offline Mode - Sync Licenses Task** page, select the devices on which to install an HSEC license.
8. Click **Next**.
9. Click **Download HSEC Device File**.
10. On the summary page, click **Download** to download a file to a local location.

    The file contains the list of devices that require an HSEC license.
11. Click **Done**.
12. Click **Cisco Smart Software Manager** to open Cisco SSM.
13. Log in to Cisco SSM and complete the following two steps:

Note The details of procedures in the Cisco SSM portal are outside the scope of this documentation and subject to change.

   a. Upload the file that you downloaded from Cisco SD-WAN Manager. The procedure is identical to uploading a usage report file, as described in License Management Offline Mode.

   b. Download the Acknowledgement file.

      This file contains the HSEC licenses required for the devices that you selected.

14. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
15. Click the **Sync and Install HSEC Devices** workflow.
16. Click **Sync Licenses** and then click **Next**.
17. Click **Offline** and then click **Next**.
18. On the **HSEC Device Activation Overview** page, click **Next**.
19. Click **Upload Process** and then click **Next**.
20. On the **Upload Smart License Authorization Code File** page, upload the acknowledgement file that you downloaded from Cisco SSM.
21. Click **Summary**.

    The process of loading and assigning licenses may take several minutes. You can monitor the progress by viewing the Cisco SD-WAN Manager task list.

After the HSEC licenses have been loaded and assigned, to install them, use the Install HSEC Licenses, on page 615 procedure.

Install HSEC Licenses

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Click the **Sync and Install HSEC Licenses** workflow.
3. Click **Install Devices**.
4. Select the desired devices on which to install an HSEC license.
5. Click **Install** to install the licenses.

   You can monitor the progress by viewing the Cisco SD-WAN Manager task list.

Verify HSEC License Installation

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **License Management**.
2. Above the table click **Device**. The HSEC license information appears in two columns.

Column	Description
HSEC Compatible	**Yes** or **No** indicate HSEC compatibility.
HSEC Status	• **scheduled**: An HSEC license is pending installation on the device. • **success**: An HSEC license is installed on the device.

Monitor Packet Trace on Cisco IOS XE Catalyst SD-WAN Devices

Table 221: Feature History

Feature Name	Release Information	Description
Bidirectional Support for Packet Tracing	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	You can configure packet tracing on edge devices.
Packet Trace Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature offers the following enhancements to packet trace: • View Feature Invocation Array (FIA) statistics about a feature in a packet trace using the command `show platform packet-trace fia-statistics` • View label information for the Multiprotocol Label Switching (MPLS) feature in packet trace.

Summary View

Use the **show platform packet-trace summary** command on Cisco IOS XE Catalyst SD-WAN devices to view the summary of all the packets matching the specified condition.

The following example displays a packet trace summary on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace summary

Pkt    Input                     Output                    State  Reason
0      INJ.12                    Gi2                       FWD
1      Gi2                       internal0/0/rp:0          PUNT   5
2      INJ.1                     Gi2                       FWD
3      INJ.1                     Gi2                       FWD
4      Gi2                       internal0/0/rp:0          PUNT   5
5      Gi2                       internal0/0/rp:0          PUNT   5
6      INJ.1                     Gi2                       FWD
7      INJ.1                     Gi2                       FWD
8      Gi2                       internal0/0/rp:0          PUNT   5
9      Gi2                       internal0/0/rp:0          PUNT   5
10     Gi2                       internal0/0/rp:0          PUNT   5
11     INJ.1                     Gi2                       FWD
12     Gi2                       internal0/0/rp:0          PUNT   5
13     INJ.1                     Gi2                       FWD
14     INJ.1                     Gi2                       FWD
```

Detailed Packet View

The following is a sample output of the **show platform packet-trace packet 0** command on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace packet 0

Packet: 0           CBUG ID: 4321
Summary
  Input     : GigabitEthernet2
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 1124044721695603 ns (09/20/2022 01:47:28.531049 UTC)
    Stop    : 1124044722142898 ns (09/20/2022 01:47:28.531497 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 10.10.10.10
    Destination : 20.20.20.20
    Protocol    : 1 (ICMP)
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x814670b0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 600 ns
  Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
    Entry       : Input - 0x81494d2c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1709 ns
  Feature: IPV4_INPUT_ARL_SANITY
    Entry       : Input - 0x814690e0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1274 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x81494d28
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 269 ns
  Feature: IPV4_INPUT_FOR_US_MARTIAN
    Entry       : Input - 0x81494d34
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 384 ns
  Feature: DEBUG_COND_APPLICATION_IN
    Entry       : Input - 0x814670a0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 107 ns
  Feature: DEBUG_COND_APPLICATION_IN_CLR_TXT
    Entry       : Input - 0x8146709c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 36 ns
  Feature: IPV4_INPUT_LOOKUP_PROCESS
    Entry       : Input - 0x81494d40
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 38331 ns
  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x81495258
```

```
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 259 ns
  Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
    Entry       : Input - 0x8146ab58
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 9485 ns
  Feature: IPV4_VFR_REFRAG
    Entry       : Output - 0x81495c6c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 520 ns
  Feature: IPV6_VFR_REFRAG
    Entry       : Output - 0x81496600
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 296 ns
  Feature: MPLS(Output)
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Label Stack Entry[1]: 0x03e850fe
      StackEnd:NO, TTL:254, EXP:0, Label:16005, is SDWAN:NO
    Label Stack Entry[2]: 0x000121fe
      StackEnd:YES, TTL:254, EXP:0, Label:18, is SDWAN:NO
  Feature: MPLS_OUTPUT_ADD_LABEL
    Entry       : Output - 0x8145e130
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 29790 ns
  Feature: MPLS_OUTPUT_L2_REWRITE
    Entry       : Output - 0x812f4724
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 23041 ns
  Feature: MPLS_OUTPUT_FRAG
    Entry       : Output - 0x8149ae5c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 785 ns
  Feature: MPLS_OUTPUT_DROP_POLICY
    Entry       : Output - 0x8149ebdc
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 14697 ns
  Feature: MARMOT_SPA_D_TRANSMIT_PKT
    Entry       : Output - 0x814ac56c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 45662 ns
Packet Copy In
  00505683 d54f0050 56830863 08004500 00641018 0000ff01 6f450a0a 0a0a1414
  14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd abcdabcd abcdabcd
Packet Copy Out
  00505683 d4900050 5683429a 884703e8 50fe0001 21fe4500 00641018 0000fe01
  70450a0a 0a0a1414 14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd
```

Use the **show platform packet-trace summary** command to view detailed information for the specified trace ID. The detailed packet view output displays three sections—summary data section, packet dump section, and featured data section.

- Summary data section: Displays packet trace ID, ingress interface, egress interface, and the forward decision taken for the packet to traverse across the device information for the specified trace ID.

- Packet dump section: Displays ingress and egress packet information. Only the first 96 bytes of packet header details are displayed.

Note The complete packet dump is not displayed because of tracer-memory limitations.

- Feature data section: Displays forwarding plane features that generate feature-specific tracing data and provides feature data decodes. These features provide debugging information to packet tracer, such as forward result, drop reason, and other behavior.

Preview Device Configuration and View Configuration Differences

For a configuration that you have created from the CLI:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **...**, and click **Change Device Values**.

   The right pane displays the device's configuration, and **Config Preview** is selected.
4. Click the name of a device.
5. Click **Config Diff** to view the differences between this configuration and the configuration currently running on the device, if applicable. Click **Back** to edit the variable values entered in the previous screen.
6. Click **Configure Devices** to push the configuration to the devices. The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to display details of the push operation.

Reset Interfaces

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation without having to modify the device's configuration.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. For the desired template, click **…** and choose **Reset Interface**.
3. In the **Interface Reset** dialog box, choose the desired interface.
4. Click **Reset**.

Reset a Locked User

If a user is locked out after multiple password attempts, an administrator with the required rights can update passwords for this user.

There are two ways to unlock a user account, by changing the password or by getting the user account unlocked.

Note Only a **netadmin** user or a user with the User Management Write role can perform this operation.

To reset the password of a user who has been locked out:

1. In **Users** (**Administration** > **Manage Users**), choose the user in the list whose account you want to unlock.
2. Click **. . .** and choose **Reset Locked User**.
3. Click **OK** to confirm that you want to reset the password of the locked user. Note that this operation cannot be undone.

   Alternatively, you can click **Cancel** to cancel the operation.

Review Last Edited Configuration in Cisco SD-WAN Manager

Table 222: Feature History

Feature Name	Release Information	Description
Retrieve Last Edited Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature lets you review the last edited configuration in Cisco SD-WAN Manager when a configuration push to the device fails.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **...**, and choose **Edit**.

   The **CLI Configuration** box displays the current running configuration on the device.
4. Click **Load Last Attempted Config** to view the last edited configuration.
5. Click **Config Diff** to view the differences in the current configuration versus the last edited configuration. The **Config Diff** option is available when you modify the configuration or when you click **Load Last Attempted Config**.

6. Click **Config Preview**.

Note **Load Last Attempted Config** and the **Config Diff** option is available only when the configuration is not being pushed to the device.

7. Click **Update**.
8. Click **Configure Devices** to push the configuration to the devices. The **Status** column displays whether the configuration was successfully pushed. Click > to view the details of the push operation.

Steps to Bring Up the Overlay Network

Bringing Up the Overlay Network

The following table lists the tasks for bringing up the overlay network using Cisco SD-WAN Manager.

Table 223:

Bring-Up Task	Step-by-Step Procedure
Step 1: Start the Cisco SD-WAN Manager.	**1.** On the hypervisor, create a VM instance. **2.** Boot Cisco SD-WAN Manager server, start the VM, and enter login information. **3.** From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**, configure certificate authorization settings. Select Automated to allow the certificate-generation process to occur automatically when a CSR is generated for a controller device. **4.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**, generate the CSR. **5.** Check for a confirmation email from Symantec that your request has been received. **6.** Check for an email from Symantec that Viptela has approved your request and the certificate is signed. **7.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, and check if the certificate has been installed.

Bring-Up Task	Step-by-Step Procedure
Step 2: Start the Cisco SD-WAN Validator.	**1.** On the hypervisor, create a VM instance. **2.** Boot the Cisco SD-WAN Validator server and start the VM. **3.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controllers**, add Cisco SD-WAN Validator and generate the CSR. **4.** Check for a confirmation email from Symantec that your request has been received. **5.** Check for an email from Symantec that Viptela has approved your request and the certificate is signed. **6.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, and check if the certificate has been installed. **7.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**: **a.** Create a configuration template for the Cisco SD-WAN Validator. **b.** Attach the template to Cisco SD-WAN Validator. **8.** From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, and verify that the Cisco SD-WAN Validator is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**, and verify that the Cisco SD-WAN Validator is operational.
Step 3: Start the Cisco Catalyst SD-WAN Controller.	**1.** On the hypervisor, create a VM instance. **2.** Boot the Cisco SD-WAN Controller server and start the VM. **3.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controller**, add Cisco Catalyst SD-WAN Controller and generate the CSR. **4.** Check for a confirmation email from Symantec that your request has been received. **5.** Check for an email from Symantec that Viptela has approved your request and the certificate is signed. **6.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, check that the certificate has been installed. **7.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**: **a.** Create a configuration template for Cisco Catalyst SD-WAN Controller. **b.** Attach the template to Cisco Catalyst SD-WAN Controller. **8.** From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, and verify that Cisco Catalyst SD-WAN Controller is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**, and verify that Cisco Catalyst SD-WAN Controller is operational.

Bring-Up Task	Step-by-Step Procedure
Step 4: Configure the router.	1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**, upload the router authorized serial number file. 2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, check that the router's chassis and serial number are in the list. 3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, authorize each router by marking it Valid in the Validity column. 4. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, send the WAN Edge list to the controller devices. 5. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**: a. Create a configuration template for the router. b. Attach the template to the router.
Step 5: Connect AC power and boot a hardware router.	1. Connect AC power to the router. 2. If needed, flip the On/Off switch on the rear of the router to the ON position. 3. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** or choose **Monitor** > **Devices** > **Device Dashboard**, verify that the router is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard** or choose **Monitor** > **Network** > **Device Dashboard**, verify that the router is operational.

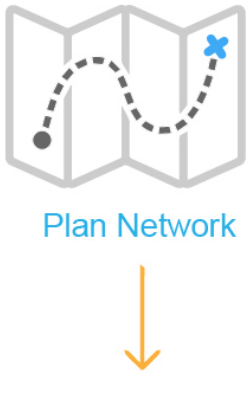
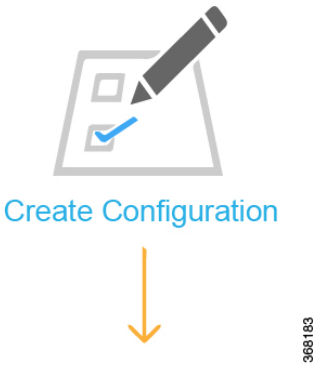
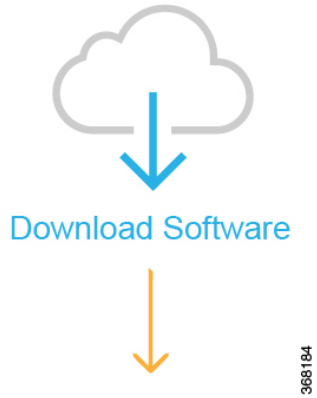
Summary of the User Portion of the Bring-Up Sequence

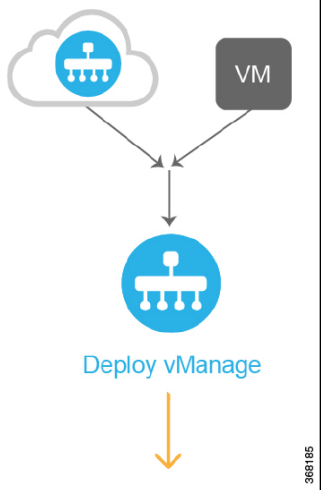
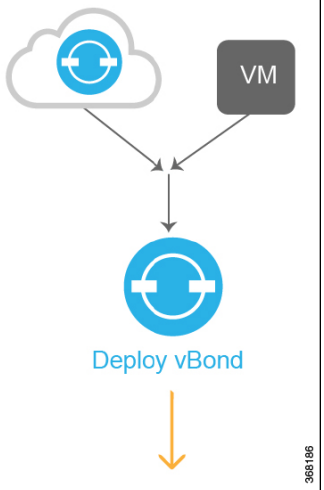
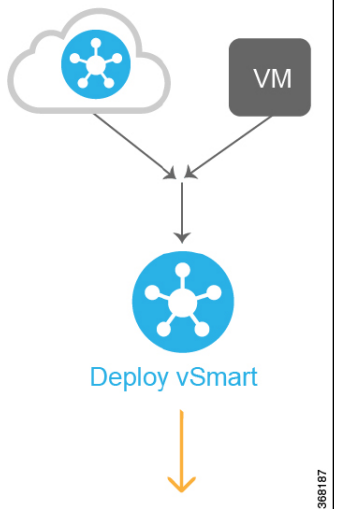
Generally, what you do to bring up the Cisco Catalyst SD-WAN overlay network is what you do to bring up any network. You plan out the network, create device configurations, and then deploy the network hardware and software components. These components include all the Cisco vEdge devices, all the traditional routers that participate in the overlay network, and all the network devices that provide shared services across the overlay network, such as firewalls, load balancers, and IDP systems.

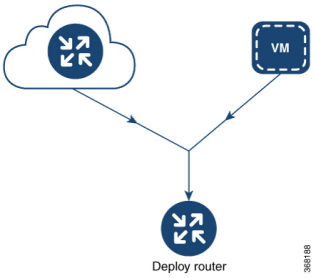
The following table summarizes the steps for the user portion of the Cisco Catalyst SD-WAN overlay network bring-up sequence. The details of each step are provided in the articles that are listed in the **Procedure** column. While you can bring up the Cisco vEdge devices in any order, it is recommended that you deploy them in the order listed below, which is the functional order in which the devices verify and authenticate themselves.

If your network has firewall devices, see Firewall Ports for Cisco Catalyst SD-WAN Deployments.

Table 224:

	Workflow	Procedure
1		Plan out your overlay network. See Components of the Cisco Catalyst SD-WAN Solution.
2		On paper, create device configurations that implement the desired architecture and functionality. See the Software documentation for your software release.
3		Download the software images.

	Workflow	Procedure
4		Deploy Cisco SD-WAN Manager in the data center: 1. Create a Cisco SD-WAN Manager VM instance, either on an ESXi or a KVM hypervisor. 2. Create either a minimal or a full configuration for each Cisco SD-WAN Manager server. 3. Configure certificate settings and generate a certificate for Cisco SD-WAN Manager. 4. Create a Cisco SD-WAN Manager cluster.
5		Deploy the Cisco SD-WAN Validator: 1. Create a Cisco SD-WAN Validator VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the Cisco SD-WAN Validator. 3. Add the Cisco SD-WAN Validator to the overlay network. During this process, you generate a certificate for the Cisco SD-WAN Validator. 4. Create a full configuration for the Cisco SD-WAN Validator.
6		Deploy the Cisco SD-WAN Controller in the data center: 1. Create a Cisco SD-WAN Controller VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the Cisco SD-WAN Controller. 3. Add the Cisco SD-WAN Controller to the overlay network. During this process, you generate a certificate for the Cisco SD-WAN Controller. 4. Create a full configuration for the Cisco SD-WAN Controller.

	Workflow	Procedure
7		Deploy the Cisco vEdge routers in the overlay network: 1. For software vEdge Cloud routers, create a VM instance, either on an AWS server, or on an ESXi or a KVM hypervisor. 2. For software vEdge Cloud routers, send a certificate signing request to Symantec and then install the signed certificate on the router. 3. From Cisco SD-WAN Manager, send the serial numbers of all Cisco vEdge routers to the Cisco SD-WAN Controller and Cisco SD-WAN Validator in the overlay network. 4. Create a full configuration for the Cisco vEdge routers.

Use the Configuration Group Workflows

Before You Begin

Ensure that the IP address of the Cisco SD-WAN Validator is specified.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **vBond**.
2. Enter the IP address of the Cisco SD-WAN Validator.

Ensure that granular RBAC for each feature profile is specified by expanding it. With the set permissions to the usergroup, ensure that you are able to access required feature profiles from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.
2. Click **Add User Group**.
3. Enter **User Group Name**.
4. Select the **Read** or **Write** check box against feature that you want to assign to a user group.
5. Click **Save**.

Note To create Service, System and Tranport feature profiles using configuration groups, you need to provide read and write permissions on the following features to access each configuration group.

- **Feature Profile** > **System**
- **Feature Profile** > **System** > **AAA**
- **Feature Profile** > **System** > **BFD**
- **Feature Profile** > **System** > **Banner**
- **Feature Profile** > **System** > **Basic**
- **Feature Profile** > **System** > **Logging**
- **Feature Profile** > **System** > **NTP**
- **Feature Profile** > **System** > **OMP**
- **Feature Profile** > **System** > **SNMP**
- **Feature Profile** > **Service**
- **Feature Profile** > **Service** > **BFD**
- **Feature Profile** > **Service** > **LAN/VPN**
- **Feature Profile** > **Service** > **LAN/VPN/Interface/Ethernet**
- **Feature Profile** > **Service** > **Routing/BGP**
- **Feature Profile** > **Service** > **Routing/OSPF**
- **Feature Profile** > **Service** > **Routing/DHCP**
- **Feature Profile** > **Service** > **Routing/Multicast**
- **Feature Profile** > **Transport**
- **Feature Profile** > **Transport** > **Routing/BGP**
- **Feature Profile** > **Transport** > **WAN/VPN**
- **Feature Profile** > **Transport** > **WAN/VPN/Interface/Ethernet**

For more details on adding user groups, see Create User Groups.

Run the Create Configuration Group Workflow

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

From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create Configuration Group**. Alternatively, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. On the **Workflow Library** page, start a new workflow or resume an existing workflow:

a. Start a new workflow: In the **Library** section, click **Create Configuration Group**. Alternatively, From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu, and click **Add Configuration Group**.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

b. Resume an in-progress workflow: In the **In-progress** section, click **Create Configuration Group**.

The workflow generates the following components:

- A configuration group
- Five feature profiles: System profile, transport and management profile, service profile, CLI profile (optional), and other profile (optional). The other profile includes the optional ThousandEyes feature.

Run the Rapid Site Configuration Group Workflow

Note This workflow is available only in Cisco vManage Release 20.8.x.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. On the **Workflow Library** page, start a new workflow or resume an existing workflow:

   a. Start a new workflow: In the **Library** section, click **Create Configuration Group**. Alternatively, From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu, and click **Add Configuration Group**.

      In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

   b. Resume an in-progress workflow: In the **In-progress** section, click **Rapid Site Configuration Group**.

The workflow generates the following components:

- A configuration group
- Four feature profiles: System profile, transport and management profile, service profile, and CLI profile (optional)

Run the Custom Configuration Group Workflow

Note This workflow is available only in Cisco vManage Release 20.8.x.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. On the **Workflow Library** page, start a new workflow or resume an existing workflow:

a. Start a new workflow: In the **Library** section, click **Create Configuration Group**. Alternatively, From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu, and click **Add Configuration Group**.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

b. Resume an in-progress workflow: In the **In-progress** section, click **Custom Configuration Group**.

The workflow generates the following components:

- A configuration group
- Three feature profiles: System profile, transport and management profile, and service profile

Add Devices to a Configuration Group

After creating a configuration group, you can add devices to the group in one of the following ways:

- Add the devices manually.
- Use rules to automatically add devices to the group.

Add Devices to a Configuration Group Manually

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**, and then click **Add Devices**.

   The **Add Devices to Configuration** workflow starts.

4. Follow the instructions provided in the workflow.

   The selected devices are listed in the **Devices** table.

Add Devices to a Configuration Group Using Rules

Before You Begin

Ensure that you have added tags to devices. For more information about tagging, see Device Tagging.

Add Devices to a Configuration Group Using Rules

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**, and then click **Add and Edit Rules**.

   The **Automated Rules** sidebar is displayed.
4. In the **Rules** section, choose values for the following options:
   - (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)

     Rule Conditions: Choose one of the following conditions: **Match All** or **Match Any**.
   - **Device Attribute**: Choose **Tags**.
   - **Condition**: Choose one of the following operators: **Equal**, **Contains**, **Not contain**, **Not equal**, **Starts with**, **Ends with**. For more information about these operators, see Examples of Applying Rules Using Tags.
   - **Select Value**: Select a tag from the list of available tags.

Note If a device matches a tag rule, the device is added to the configuration group. If you edit the tag rule by changing any of the specified values, the device is removed from the group.

5. Click **Apply**.

   A list displays the devices that will be added to the configuration group or removed from the group based on the rule.
6. Click **Confirm** to apply the changes.

Note
- You cannot create a new rule if it conflicts with an existing rule.
- You cannot add a tag to a device if it is already attached to a device template.
- If you have attached a template to a device, and the task is in progress, you can add a tag to the device. However, you cannot apply a rule to add this device to a configuration group using the same tag. To do this, you must either detach the device from the template or use a different tag.

Check Task Details

To check the status of all the active and completed tasks, do the following:

1. Click the + icon to view the details of a task.

   Cisco SD-WAN Manager displays the status of the task and details of the device on which the task was performed.
2. From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon.

   Cisco SD-WAN Manager displays a list of all the running tasks along with the total number of successes and failures.

Deploy Devices

Any field in a feature can be marked as device-specific which is referred as device variable. You can provide device variable values while adding devices for deploying them for any features.

Deploy Devices Manually

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**.
4. Choose one or more devices, and then click **Deploy**.

Deploy Devices Using the Deploy Configuration Group Workflow

Before You Begin

Ensure that one or more configuration groups are created so that you can choose a group from the list to deploy the associated devices.

Note In Cisco vManage Release 20.8.x, the Deploy Configuration Group workflow is called the Provision WAN Sites and Devices workflow.

Deploy Devices

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Deploy Configuration Group** workflow.
3. Follow the instructions provided in the workflow.

Add a Feature

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click the desired feature profile.
4. Click **Add Feature**.
5. From the feature drop-down list, choose a feature.

6. In the **Name** field, enter a name for the feature.
7. In the **Description** field, enter a description of the feature. The description can contain any characters and spaces.
8. Configure the options as needed.

   For information about the configuration options, see Feature Configuration.
9. Click **Save**.

Add a Sub Feature

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click the desired feature profile.
4. Click **…** adjacent to a feature and choose **Add Sub-Feature**.
5. From the feature drop-down list, choose a feature.
6. In the **Name** field, enter a name for the feature.
7. In the **Description** field, enter a description of the feature. The description can contain any characters and spaces.
8. Configure the options as needed.

   For information about the configuration options, see Feature Configuration.
9. Click **Save**.

Security Profile

The following table lists the options to configure a security profile.

Field	Description
Choose existing	Choose an existing profile from the **Profiles** table.
Create new	When you choose this option, the following fields are displayed: • **Name**: Enter a name for the profile. • **Description**: Enter a description for the profile. The description can contain any number of characters and spaces.

Edit a Security Profile

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. In the **Associate Profiles** list, click **Security Profile**.
3. Click **Actions** adjacent to the security profile configuration group that you want to edit and choose **Edit Profile**.

   The **Edit Feature Profile** window is displayed.

4. Edit the **Name** and **Description** fields.
5. Click **Save**.

Switch to Another Security Profile

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. In the list of **Associate Profiles**, click **Security Profile**.
3. Click **Actions** adjacent to the security profile configuration group and choose **Switch to Another Profile**.

   The **Switch to another profile** dialog box is displayed.

4. Click the corresponding profile in the **Profiles** table.
5. Click **Save**.

Dissociate a Security Profile

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. In the list of **Associate Profiles**, click **Security Profile**.
3. Click **Actions** adjacent to the security profile configuration group that you want to dissociate and choose **Dissociate Profile**.

   The **Detach Profile** dialog box is displayed.

4. Click **Yes**.

Add a Legacy Feature to a Security Profile

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. In the **Associate Profiles** list, click **Security Profile**.
3. Click **Add Feature** in the security profile drop-down list.

   The **Add Feature** dialog box is displayed.
4. Choose **Legacy Policy** from the feature **Type** drop-down list.
5. Enter the following details.

Field	Description
Type	Choose a legacy policy feature from the drop-down list.
Feature Name	Enter a name for the feature.
Description	Enter a description of the feature.

Security Policy	Choose the available security policy from the drop- list. You can configure the following if the security policy has Unified Threat Defense (UTD) elements in it, and requires app hosting:
	• NAT
	• Database URL
	• Resource Profile: Choose a resource profile priority option:
	  • **Low**
	  • **Medium**
	  • **High**
	Note The **app-hosting option** is displayed only if you select a security policy that has UTD features. If you create a security profile without UTD features, the app-hosting section is not displayed. If you update the security policy with UTD features later, then you must edit the security profile and update the app-hosting section, as needed.

6. Click **Save**.

Policy Profile

The Policy feature profile enables you to attach policy configurations to a device.

The following table describes the options for configuring the policy profile.

Field	Description
Choose existing	Choose an existing profile from the **Profiles** table.

Field	Description
Create new	When you choose this option, the following fields appear: • **Name**: Enter a name for the profile. • **Description**: Enter a description of the profile. The description can contain any characters and spaces.

Edit a Policy Profile

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Profile**.
3. Click **Actions** adjacent to the policy object profile configuration group and choose **Edit Profile**. The **Edit Feature Profile** page displays.
4. Edit the **Name** and **Description** fields.
5. Click **Save**.

Switch to Another Policy Profile

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Actions** adjacent to the policy object profile configuration group and choose **Switch to Another Profile**. The **Switch to another profile** page displays.
4. In the **Switch to another profile**, choose the desired profile from the **Profiles** table.
5. Click **Save**.

Note You can also create a new policy-object profile from the **Switch to another profile** page. Once you create a new policy-object profile, it detaches the current profile from the configuration group.

Dissociate a Policy Object Profile

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Actions** adjacent to the policy object profile configuration group and choose **Dissociate Profile**. The **Detach Profile** page displays.
4. Click **Yes**.

AS Path

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **AS Path** policy object from the **Select Policy Object** drop-down list.
5. Enter the AS Path list name in the **AS Path List Name** field.
6. Enter the AS Path list ID in the **AS Path List ID** field.
7. In the **Add AS Path** field, enter the AS path number.
8. Click **Save**.

The following table describes the options for configuring the class map.

Field	Description
AS Path List Name	Enter a name for the class map list.
Add AS Path	Specify the AS path number. The range is 1 to 65535.

Standard Community

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **Standard Community** policy object from the **Select Policy Object** drop-down list.
5. Enter the **Standard Community List Name**.
6. In the **Add Standard Community** field, enter the community details. The format example is given in the field.
7. Click **Save**.

The following table describes the options for configuring the standard community.

Field	Description
Standard Community List Name	Enter a name for the community list.
Add Standard Community	Specify the standard community. the options are: • *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS number. • **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.

Expanded Community

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **Expanded Community** policy object from the **Select Policy Object** drop-down list.
5. Enter the **Expanded Community List Name**.
6. In the **Add Expanded Community** field, enter the community details. The format example is given in the field.
7. Click **Save**.

The following table describes the options for configuring the expanded community.

Field	Description
Expanded Community List Name	Enter a name for the community list.
Add Expanded Community	Specify the expanded community.

Data Prefix

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **Data Prefix** policy object from the **Select Policy Object** drop-down list.
5. Enter the **Data Prefix List Name**.
6. In the **Internet Protocol** field, click **IPv4** or **IPv6**.
7. Click **Save**.

The following table describes the options for configuring the data prefix.

Field	Description
Prefix List Name	Enter a name for the prefix list.
Internet Protocol	Specify the internet protocol. The options are IPv4 and IPv6.

Extended Community

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **Extended Community** policy object from the **Select Policy Object** drop-down list.
5. Enter the **Extended Community List Name**.
6. In the **Add Extended Community** field, enter the community details. The format example is given in the field.
7. Click **Save**.

The following table describes the options for configuring the extended community.

Field	Description
Extended Community List Name	Enter a name for the community list.

Field	Description
Add Extended Community	Specify the extended community. The format is as follows: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.

Class Map

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **Class Map** policy object from the **Select Policy Object** drop-down list.
5. Enter the class map name in the **Class** field.
6. In the **Select a Queue** drop-down list, choose the required queue.
7. Click **Save**.

The following table describes the options for configuring the class map.

Field	Description
Class	Enter a name for the class map list.
Queue	Specify the queue number.

Mirror

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.

4. Choose the **Mirror** policy object from the **Select Policy Object** drop-down list.
5. Enter the **Mirror List Name**.
6. In the **Remote Destination IP** field, enter the IP address of the destination for which to mirror the packets.
7. In the **Source IP** field, enter the IP address of the source of the packets to mirror.
8. Click **Save**.

Note To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets. Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

The following table describes the options for configuring the mirror.

Field	Description
Mirror List Name	Enter a name for the mirror list.
Remote Destination IP	Specify the IP address of the remote destination.
Source IP	Specify the IP address of the source.

Policer

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **Policer** policy object from the **Select Policy Object** drop-down list.
5. Enter the **Policer List Name**.
6. In the **Burst (bytes)** field.
7. In the **Exceed** drop-down list, choose the action **Drop** or **Remark**.
8. Enter the **Rate (bps)**
9. Click **Save**.

The following table describes the options for configuring the policer.

Field	Description
Policer List Name	Enter a name for the policer list.

Field	Description
Burst (bytes)	Specify the maximum traffic burst size. Range is from 15000 to 10000000.
Exceed	Specify an action to take when the burst size or traffic rate is exceeded. The options are: **Drop**—Sets the packet loss priority (PLP) to low. **Remark**—Sets the PLP to high. The default option is **Drop**.
Rate	Specify the maximum traffic rate. It can be a value from 8 through 2^{64} bps (8 through 100000000000).

Prefix

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. From the list of **Associate Profiles**, select **Policy Object Profile**.
3. Click **Add Policy Object Profile** to add policy objects. A **New Policy** page displays.
4. Choose the **Prefix** policy object from the **Select Policy Object** drop-down list.
5. Enter the **Prefix List Name**.
6. In the **Internet Protocol** field, click **IPv4** or **IPv6**.
7. Under **Add Prefix**, enter the prefix for the list. Optionally, click the **Choose a file** link to import a prefix list.
8. Click **Save**.

The following table describes the options for configuring the prefix.

Field	Description
Prefix List Name	Enter a name for the prefix list.
Internet Protocol	Specify the internet protocol. The options are IPv4 and IPv6.

QoS Map

Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

You can configure quality of service (QoS) to classify data packets and control how traffic flows out of and into the interfaces and on the interface queues.

Note Cisco vManage Release 20.11.1 does not support the QoS map feature in the transport profile and the service profile.

Before upgrading to Cisco vManage Release 20.11.1, ensure that you delete the QoS map feature from the transport profile or the service profile if you have already configured it.

Delete the QoS map feature

To delete the QoS map feature, do the following:

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** under **Actions** for the configuration group that you want to remove the QoS map feature from and choose **Edit**.
3. Click the feature profile from which you want to remove the QoS map.
4. Dissociate the QoS map feature from the VPN interface by clicking **…** next to the feature and click **Edit Feature**.
5. Choose **ACL/QoS** > **Select QoS Map**.
6. Choose the QoS map from the drop-down list and click the delete button.
7. Click **Save** to exit the **Edit Transport VPN Feature** page.
8. In the **Configuration Groups** page, click **…** under **Actions** for the QoS Map feature and click **Delete Feature**.
9. Click **Yes** to confirm.

Configure the QoS map feature

You can select the specific queue in the QoS Map window to edit, delete, or add. The following tables describe the options for configuring the QoS Map feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Select Queue	Specifies the queue number from the drop-down list. The range is 1 to 7.
Enter Class	Specifies the forwarding class from the drop-down.
Select Drop	Specifies the drop type. The options are, Random Early and Tail.

Field	Description
Bandwidth %	Specifies the maximum bandwidth. The range is 1 to 99 %.
Scheduling Type	Specifies the scheduling type. For example, Weighted Round Robin (WRR) or Low Latency Queuing(LLQ).

Route Policy

Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

Routing is a process whereby the device puts packets through a route map before routing them. The route map determines which packets are routed to which device next. You might enable policy-based routing if you want certain packets to be routed through a specific path other than the obvious shortest path.

1. In the **Add Feature** page, choose **Route Policy** from the drop-down list.
2. Enter a name and description for the route policy.
3. Click **Add Routing Sequence**. The Add Route Sequence page displays.
4. Enter **Routing Sequence Name**.
5. Select a desired protocol from the **Protocol** drop-down list. The options are: IPv4, IPv6, or both.
6. Select a condition from the **Condition** drop-down list.
7. Select the action types **Accept** or **Reject** from the **Action Type** drop-down list.
8. For the **Accept** action type, choose the accept condition from the **Accept Condition** drop-down list.
9. Click **Save**.

   To copy, delete, or rename the route policy sequence rule, click **...** next to the rule's name and select the desired option.
10. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
    a. Click **Default Action** in the left pane.
    b. Click the Pencil icon.
    c. Change the default action to **Accept**.
    d. Click **Save**.
11. Click **Save Route Policy**.

The following table describes the options for configuring the route policy feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.

Field	Description
Description	Enter a description of the feature. The description can contain any characters and spaces.
Routing Sequence Name	Specify the name of the routing sequence.
Protocol	Specify the internet protocol. The options are IPv4, IPv6, or Both.
Condition	Specify the routing condition. The options are: • Address • AS Path List • Community List • Extended Community List • BGP Local Preference • Metric • Next Hop • OMP Tag • OSPF Tag
Action Type	Specify the action type. The options are: Accept or Reject.
Accept Condition	Specify the accept condition type. The options are: • AS Path • Community • Local Preference • Metric • Metric Type • Next Hop • OMP Tag • Origin • OSPF Tag • Weight

You can select the specific route sequence in the Route Policy page to edit, delete or add a route sequence.

Note You can also configure the **Route Policy** feature from the Transport and Service profiles in configuration groups.

ACL IPv4

Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

Access Control Lists (ACLs) determine what traffic is blocked and what traffic is forwarded at device interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. Perform the following steps to configure ACL on IPv4 interfaces.

1. In the **Add Feature** page, choose **ACL IPv4** from the drop-down list.
2. Enter the **Feature Name** and the **Description** for the ACL feature.
3. Click **Add ACL Sequence**. The **Add ACL Sequence** page appears.
4. Enter the name in the **ACL Sequence Name** field.
5. Select the required condition from the **Condition** drop-down list.
6. Select the action types **Accept** or **Reject** from the **Action Type** drop-down list.
7. For the **Accept** action type, choose the accept condition from the **Accept Condition** drop-down list.
8. Click **Save**.

   To copy, delete, or rename the ACL policy sequence rule, click **...** next to the name of the rule and select the desired option.
9. If no packets match any of the ACL policy sequence rules, the default action is to drop the packets. To change the default action:
   a. Click **Default Action** in the left pane.
   b. Click the Pencil icon.
   c. Change the default action to **Accept**.
   d. Click **Save**.
10. Click **Save ACL IPv4 Policy**.

The following table describes the options for configuring the ACL IPv4 feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
ACL Sequence Name	Specify the name of the ACL sequence.

Field	Description
Condition	Specify the ACL condition. The options are: • DSCP • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Peer
Action Type	Specify the action type. The options are: Accept or Reject.
Accept Condition	Specify the accept condition type. The options are: • Counter • DSCP • Log • Next Hop • Mirror List • Class • Policer

You can select the specific ACL sequence in the ACL Policy page to edit, delete or add a sequence.

Note You can also configure the **ACL Policy** features from the Transport and Service profiles in configuration groups.

ACL IPv6

Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

Perform the following steps to configure ACL on IPv6 interfaces.

1. In the **Add Feature** page, choose **ACL IPv6** from the drop-down list.

2. Enter the **Feature Name** and the **Description** for the ACL feature.
3. Click **Add ACL Sequence**. The **Add ACL Sequence** page appears.
4. Enter the name in the **ACL Sequence Name** field.
5. Select the required condition from the **Condition** drop-down list.
6. Select the action types **Accept** or **Reject** from the **Action Type** drop-down list.
7. For the **Accept** action type, choose the accept condition from the **Accept Condition** drop-down list.
8. Click **Save**.

   To copy, delete, or rename the ACL policy sequence rule, click **...** next to the name of the rule and select the desired option.
9. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
   a. Click **Default Action** in the left pane.
   b. Click the Pencil icon.
   c. Change the default action to **Accept**.
   d. Click **Save**.
10. Click **Save ACL IPv6 Policy**.

The following table describes the options for configuring the ACL IPv6 feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
ACL Sequence Name	Specify the name of the ACL sequence.

Field	Description
Condition	Specify the ACL condition. The options are: • Next Header • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Traffic Class
Action Type	Specify the action type. The options are: Accept or Reject.
Accept Condition	Specify the accept condition type. The options are: • Counter • Log • Next Hop • Traffic Class • Mirror List • Class • Policer

You can select the specific ACL sequence in the ACL Policy page to edit, delete or add a sequence.

Note You can also configure the **ACL Policy** features from the Transport and Service profiles in configuration groups.

Use Variable Values in Configuration Templates

An overlay network might have multiple devices of the same type that have nearly identical configurations. This situation most commonly occurs with routers when the routers that are located in multiple stores or branch locations provide identical services, but each individual router has its own hostname, IP address, GPS

location, and other site-specific properties, such as BGP neighbors. This situation also occurs in a network with redundant controller devices, such as Cisco Catalyst SD-WAN Controllers, which must all be configured with identical policies, and Cisco SD-WAN Manager systems. Again, each controller has its own individual parameters, such as hostname and IP address.

To simplify the configuration process for these devices, you can create a single configuration template that contains both static configuration values and variable values. The static values are common across all the devices, and the variable values apply only to an individual device. You provide the actual values for the variables when you attach the individual device to the device configuration template.

You can configure a variable value for a parameter in a feature configuration template in two ways:

- Select the parameter scope to be Device Specific—For an individual configuration parameter, select Device Specific to mark the parameter as a variable. Each variable must be identified by a unique text string, which is called a *key*. When you select Device Specific, an Enter Key box opens and displays the default key. You can use the default key, or you can change it by typing a new string and then moving the cursor out of the Enter Key box.
- Mark a group of related parameters as optional—For some features in some feature configuration templates, you can mark the entire feature as optional. To mark the feature in this way, click Mark as Optional Row in a section of a feature configuration template. The variable parameters are then dimmed, and you cannot configure values for them in the feature configuration template.

You enter the device-specific values for the variables when you attach the device to the configuration, in one of the following ways:

- From a file—When you are attaching a template to a device, you load a file to Cisco SD-WAN Manager. This is an Excel file in CSV format that lists all the variables and defines the variable's value for each device.
- Manually—When you attach a device template to a device, the Cisco SD-WAN Manager prompts you for the values for each of device-specific parameters, and you type in the value for each parameter.

Note Cisco Catalyst SD-WAN supports up to 500 variables in a template push operation.

Use a File for Variable Parameters

To load device-specific variable values from a file, you create a template variables file. This file is an Excel file in CSV format that lists all the variables in your the configurations of your devices and defines the values for each variable. You create this file offline and then import it into Cisco SD-WAN Manager server when you attach a device configuration to one or more devices in the overlay network.

We recommend that you create a template variables CSV file when your overlay network has more than a small number of Cisco IOS XE Catalyst SD-WAN devices.

CSV File Format

The CSV file is an Excel spreadsheet that contains one column for each variable that is required for the configuration of a device. The header row contains the variable names (one variable per column), and each row after that corresponds to a device and defines the values of the variables for that device.

You can create a single spreadsheet for all devices in the overlay network—Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager systems, Cisco Catalyst SD-WAN Controllers, and Cisco Catalyst SD-WAN Validators—or you can create one spreadsheet for each device type. The system determines the device type from its serial number.

In the spreadsheet, for each device type and for each individual device, you specify values only for the required variables. When you do not need to specify a value for a variable, simply leave that cell blank.

The first three columns in the spreadsheet must be the following items and must be in the order shown:

Column	Column Heading	Description
1	csv-deviceId	Serial number of the device (used to uniquely identify the device). For Cisco IOS XE Catalyst SD-WAN devices, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.
2	csv-deviceIP	System IP address of the device (used to populate the **system ip address** command).
3	csv-host-name	Hostname of the device (used to populate the **system hostname** command).

The headings for the remaining columns must be unique variable keys that are defined in the Enter Key box of a feature configuration template. These remaining columns can be in any order.

Generate a Skeleton CSV File

You can create a template variables CSV file manually, with the format described in the previous section, or you can haveCisco SD-WAN Manager generate a skeleton CSV file that contains all the required columns and column headings. This generated CSV file has one row for each Cisco device type, and it has the column headings for each of the variables that are required by all the feature templates included in the device configuration. The column heading text corresponds to the key string that identifies a device-specific parameter. Then you populate the rows with values for each variable.

To have Cisco SD-WAN Manager generate a skeleton CSV file:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Create the required feature templates for one Cisco IOS XE Catalyst SD-WAN device router, one Cisco Catalyst SD-WAN Controller, one Cisco SD-WAN Manager system, and one Cisco Catalyst SD-WAN Validator.

   In each feature template:

a. For fields that have default values, verify that you want to use that value for all devices. If you do not want to use the default, change the scope to **Global** or **Device-specific**.

b. For fields that apply to all devices, select the **Global** icon next to the field and set the desired global values.

c. For fields that are device specific, select the **Device-specific** icon next to the field and leave the field blank.

4. For each Cisco device type, create a device template.
5. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
6. Click **Device Templates**, and select the desired device template from the template list table.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

7. Click **…**, and click **Export CSV**.
8. Repeat Steps 7 and 8 for each device template.

Edit the exported CSV file, adding at a minimum the device serial number, device system IP address, and device hostname for each device in the overlay network. Then add values for desired device-specific variables for each device. Note that variable names cannot contain forward slashes (/), backwards slashes (\), or parentheses (( )).

If desired, you can combine the CSV files into a single file.

Import a CSV File

To use the device-specific variable values in the CSV file, import the file when you are attaching a device template to the Viptela device:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. For the desired template, click **...**, and select **Attach Devices**.
4. In the **Attach Devices** dialog box, select the desired devices in **Available Devices** and click the arrow to move them to **Selected Devices**.
5. Click **Attach**.
6. Click the Up arrow. The Upload CSV File box displays.
7. Choose the CSV file to upload, and click **Upload**.

During the attachment process, click Import file to load the Excel file. If Cisco SD-WAN Manager detects duplicate system IP addresses for devices in the overlay network, it displays a warning message or a pop-up

window. You must correct the system IP addresses to remove any duplicates before you can continue the process of attaching device templates to Viptela devices.

Manually Enter Values for Device-Specific Variables and for Optional Rows

For parameters in a feature template that you configure as device-specific, when you attach a device template to a device, Cisco SD-WAN Manager prompts you for the values to use for these parameters. Entering device-specific values in this manner is useful in test or POC networks, or if you are deploying a small network. This method generally does not scale well for larger networks.

For situations in which the configuration for many devices is identical except for a few parameters, in the feature configuration template, you can specify that the parameter be an optional row in the configuration. By selecting optional row, the feature template automatically marks the parameters as device-specific, and these parameters are dimmed so that you cannot set them in the template. You do not have to individually mark the parameters as device specific. Then, when you attach a device template to a device, Cisco SD-WAN Manager prompts you for the values to use for these parameters. Using optional rows to enter device-specific values is useful when a group of many Cisco IOS XE Catalyst SD-WAN devices provide identical services at their branch or site, but individual routers have their own hostname, IP address, GPS location, and other site or store properties, such as BGP neighbors.

Optional rows are available for some parameters in some feature configuration templates. To treat a parameter or set of parameters as an optional row, click the **Mark as Optional Row** box. For these types of parameters, the feature configuration template has a table listing all the configured parameters. The Optional column indicates which are optional rows,

To manually enter values for device-specific variables or for variables in optional rows when you attach the template to a device:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select the desired device template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Attach Devices**. The **Attach Devices** dialog box opens.
4. Choose one or more devices from **Available Devices** and move them to **Selected Devices**.
5. Click **Attach**.
6. In the **Chassis Number** list, select the desired device.
7. Click **…**, and click **Edit Device Template**. The **Update Device Template** dialog box opens.
8. Enter values for the optional parameters. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
9. Click **Update**.
10. Click **Next**.

    If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.

Note You need to shut down the OMP on the device, before changing the system-ip on the device.

11. In the left pane, select the device. The right pane displays the device configuration and the **Config Preview** tab in the upper right corner is selected.
12. Click **Config Diff** to preview the differences between this configuration and the configuration currently running on the device, if applicable. To edit the variable values entered in the previous screen, click **Back**.
13. Click **Configure Devices** to push the configuration to the devices.

    The Status column displays whether the configuration was successfully pushed. Click the **right angle bracket** to the left of the row to display details of the push operation.

Upgrade Existing Templates to Type 6 Passwords

To upgrade passwords in your existing templates on Cisco SD-WAN Manager to type 6 passwords, do the following:

Note When you upgrade your routers to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, all supported passwords are automatically upgraded to type 6 passwords.

1. Navigate to **Configuration** > **Templates**
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. For the template that you want to upgrade to type 6 passwords, click the **…** button.
4. Click **Edit**.
5. Click **Save**.

Note To update the passwords, you do not need to make any other changes to the template. When you click **Save**, Cisco SD-WAN Manager automatically upgrades the passwords to type 6 passwords.

Upgrade the Software Image on a Device

Note

- This procedure does not enable downgrading to an older software version. If you need to downgrade, see Downgrade a Cisco vEdge Device to an Older Software Image in the Cisco Catalyst SD-WAN Getting Started Guide.
- If you want to perform a Cisco SD-WAN Manager cluster upgrade see, Upgrade Cisco SD-WAN Manager Cluster.
- Starting from Cisco vManage Release 20.11.1, before upgrading the configuration database, ensure that you verify the database size. We recommend that the database size is less than or equal to 5 GB. To verify the database size, use the following diagnostic command:

  request nms *configuration-db diagnostics*

To upgrade the software image on a device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Controller**, or **vManage** based on the type of device for which you wish to upgrade the software.
3. In the table of devices, select the devices to upgrade by selecting the check box on the far left.

Note While upgrading Cisco SD-WAN Manager clusters, select all the nodes of the cluster in the table.

4. Click **Upgrade**.
5. In the **Software Upgrade** slide-in pane, do as follows:
   a. Choose the server from which the device should download the image: **vManage**, **Remote Server**, or **Remote Server – vManage**.

Note

- The Remote Server option is introduced in Cisco vManage Release 20.7.1. If you chose **Remote Server**, ensure that the device can reach the remote server.
- Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:
  - User ID: a-z, 0-9, ., _, -
  - Password: a-z, A-Z, 0-9, _, *, ., +, =, %, -
  - URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -, :, /, @, ?, ~

   b. For **vManage**, choose the image version from the **Version** drop-down list.

c. For **Remote Server – vManage**, choose the **vManage OOB VPN** from the drop-down list and choose the image version from the **Version** drop-down list.

d. For **Remote Server**, configure the following:

Remote Server Name	Choose the remote server that has the image.
Image Filename	Choose the image filename from the drop-down list.

e. Check the **Activate and Reboot** check box.

If you do not check this check box, the software image is downloaded and installed on the device, but, the image is not activated, and the device is not rebooted. You must activate the image after the upgrade task is completed.

f. Click **Upgrade**.

The device restarts, using the new software version, preserving the current device configuration. The **Task View** page opens, showing the progress of the upgrade on the devices.

6. Wait for the upgrade process, which takes several minutes, to complete. When the **Status** column indicates Success, the upgrade is complete.
7. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** and view the devices.
8. Click **WAN Edge**, **Controller**, or **vManage** based on the type of device for which you wish to upgrade the software.
9. In the table of devices, confirm that the **Current Version** column for the upgraded devices shows the new version. Confirm that the **Reachability** column says reachable.

Note

- If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image. The configured time limit for all Cisco Catalyst SD-WAN devices to come up after a software upgrade is 5 minutes, except for Cisco vEdge devices, which have a default time of 12 minutes.
- If you upgrade the Cisco vEdge device software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first before upgrading the Cisco vEdge device software.
- When upgrading a Cisco CSR1000V or Cisco ISRv device to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a or later, the software upgrade also upgrades the device to a Cisco Catalyst 8000V. After the upgrade, on the Devices page, the **Chassis Number** and **Device Model** columns show the device as a Cisco CSR1000V or Cisco ISRv, but the device has actually been upgraded to a Cisco Catalyst 8000V. The reason for preserving the old name is to avoid invalidating licenses, and so on. To confirm that the device has been upgraded to a Cisco Catalyst 8000V, note that the **Current Version** column for the device indicates 17.4.1 or later.

Upload WAN Edge Router Authorized Serial Number File

Table 225: Feature History

Feature Name	Release Information	Description
Remove Certificate SUDI requirement	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to use a subject SUDI serial number instead of a certificate serial number to add a device to a Cisco Catalyst SD-WAN overlay network.

The WAN eEdge router authorized serial number file contains, as applicable, the subject SUDI serial number, the chassis number, and the certificate serial numbers of all valid Cisco IOS XE Catalyst SD-WAN devices in the overlay network. You retrieve a serial number file from the Cisco Plug-and-Play (PnP) portal and upload it to Cisco SD-WAN Manager. (For more information abou Cisco PnP, see Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products.) From Cisco SD-WAN Manager, you send the file to the controllers in the network. This file is required to allow the Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational.

To upload the WAN edge router authorized serial number file to Cisco SD-WAN Manager and then download it to controllers in the network:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List**, and click **Upload WAN Edge List**.
3. Under **Upload WAN Edge List** screen:
   a. Click **Choose File** and select the WAN edge router authorized serial number file you received from Cisco PnP.
   b. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the **Validate the uploaded vEdge List and send to controllers** check box is selected. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > **WAN Edge List**.
   c. Click **Upload**.

A list of routers in the network is displayed in the router table, with details about each router.

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

Upload WAN Edge Router Serial Numbers from Cisco Smart Account

To allow Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational, Cisco Catalyst SD-WAN requires chassis numbers of all valid Cisco IOS XE Catalyst SD-WAN devices in the overlay network.

In addition, certificate serial numbers, subject SUDI serial numbers, or both numbers are required for all devices.

To upload the WAN edge router authorized serial numbers from a Cisco Smart account to Cisco SD-WAN Manager and then download it to all the controllers in the overlay network:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List**, and click **Sync Smart Account**.
3. In the **Sync Smart Account** window:
   a. Enter the **Username** and **Password** for your Smart account.
   b. To automatically validate the routers and send their chassis and serial numbers to the controllers, check the **Validate the Uploaded WAN Edge List and Send to Controllers** check box. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > **WAN Edge List**.
   c. Click **Sync**.

A list of routers in the network is displayed in the router table, with details about each router.

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

View and Copy Device Configuration

View a Device's Running Configuration

Running configuration is configuration information that Cisco SD-WAN Manager obtains from the memory of a device. This information can be useful for troubleshooting.

To view a device's running configuration:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List** or **Controllers**, and select the device.
3. Click **…**, and click **Running Configuration**.

View a Device's Local Configuration

Local configuration is configuration that Cisco SD-WAN Manager has stored for a device. This information can be useful for troubleshooting or for determining how to access a device if, for example, a device is not reachable from Cisco SD-WAN Manager.

To view a device's local configuration created using Configuration ► Templates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List** or **Controllers**, and select the device.
3. Click **…**, and click **Local Configuration**.

Copy Router Configuration

When you are replacing one router at a site with another router, you copy the old router's configuration to the new router. Then you remove the old router from the network and add the new one.

To copy the configuration from the old router to the new router:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Mark the new Cisco IOS XE Catalyst SD-WAN device as invalid.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
4. Under **WAN Edge List**, select the old router.
5. Click **…**, and click **Copy Configuration**.
6. In the **Copy Configuration** window, select the new router.
7. To confirm the copy of the configuration, click **Update**.

After you have copied the configuration to the new router, you can add the new router to the network. First, delete the old router from the network, as described below. Then add the new router to the network:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Mark the new router as valid.
3. Click **Send to Controller**.

View Device Templates

View a Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** or **Feature Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and then click **View**.

View Device Templates Attached to a Feature Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Show Attached Device Templates**.

   Device Templates dailog box opens, displaying the names of the device templates to which the feature template is attached.

View Devices Attached to a Device Template

For a device template that you created from feature templates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Attach Devices**.
4. From **Attach Devices**, click **Attached Devices**.

For a device template that you created from a CLI template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and then click **Show Attached Devices**.

View FIA Statistics

Table 226: Feature History

Feature Name	Release Information	Description
Bidirectional Support for Packet Tracing	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	You can configure packet tracing on edge devices.

Feature Name	Release Information	Description
Packet Trace Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature offers the following enhancements to packet trace: • View Feature Invocation Array (FIA) statistics about a feature in a packet trace using the command `show platform packet-trace fia-statistics` • View label information for the Multiprotocol Label Switching (MPLS) feature in packet trace.

Minimum supported releases: Cisco vManage Release 20.11.1 and Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Use the **show platform packet-trace fia-statistics** command on Cisco IOS XE Catalyst SD-WAN devices to view to FIA statistics. FIA statistics provides details about the number of features, and the time details–minimum time, maximum time, and average time about a feature.

The following example displays FIA statistics on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace fia-statistics

Feature                                          Count  Min(ns)   Max(ns)   Avg(ns)
-------------------------------------------------------------------------------
INTERNAL_TRANSMIT_PKT_EXT                           66     4720     28400     13333
MARMOT_SPA_D_TRANSMIT_PKT_EXT                       16     4560     16920     11955
L2_SVI_OUTPUT_BRIDGE_EXT                             1     3640      3640      3640
INTERNAL_INPUT_GOTO_OUTPUT_FEATURE_EXT              16     1680      3880      2755
IPV4_INPUT_LOOKUP_PROCESS_EXT                        1     2720      2720      2720
IPV4_OUTPUT_L2_REWRITE_EXT                           1     2240      2240      2240
IPV4_OUTPUT_DROP_POLICY_EXT                          4     1040      2880      2050
IPV4_INTERNAL_DST_LOOKUP_CONSUME_EXT                 1     1960      1960      1960
SSLVPN_INJECT_TX_MSG_EXT                            15      600      2440      1746
IPV4_INTERNAL_FOR_US_EXT                             1     1560      1560      1560
LAYER2_OUTPUT_QOS_EXT                               63      280      2480      1537
LAYER2_OUTPUT_DROP_POLICY_EXT                       78      120      3120      1525
LAYER2_INPUT_LOOKUP_PROCESS_EXT                     15      280      2240      1312
UPDATE_ICMP_PKT_EXT                                  1     1280      1280      1280
DEBUG_COND_MAC_EGRESS_EXT                            3      840      1160       973
IPV4_INTERNAL_INPUT_SRC_LOOKUP_CONSUME_EXT           1      960       960       960
IPV4_PREF_TX_IF_SELECT_EXT                           1      800       800       800
DEBUG_COND_OUTPUT_PKT_EXT                           66       80      1640       707
IPV4_INTERNAL_ARL_SANITY_EXT                         3      240       960       666
IPV4_INTERNAL_INPUT_SRC_LOOKUP_ISSUE_EXT             1      640       640       640
IPV4_VFR_REFRAG_EXT                                  5      320       920       640
EVC_EFP_VLAN_TAG_ATTACH_EXT                         15       80      1040       629
L2_SVI_OUTPUT_GOTO_OUTPUT_FEATURE_EXT                1      520       520       520
LAYER2_VLAN_INJECT_EXT                              15      120       760       504
L2_ES_OUTPUT_PRE_TX_EXT                             16        0      1000       502
DEBUG_COND_APPLICATION_IN_EXT                        1      480       480       480
DEBUG_COND_APPLICATION_OUT_CLR_TXT_EXT               3       80       720       426
DEBUG_COND_INPUT_PKT_EXT                            16       80       880       417
IPV4_OUTPUT_FRAG_EXT                                 1      360       360       360
DEBUG_COND_APPLICATION_IN_CLR_TXT_EXT                1      320       320       320
```

```
DEBUG_COND_APPLICATION_OUT_EXT                3      240       280       266
LFTS_INJECT_PKT_EXT                          16       40       480       250
LAYER2_BRIDGE_INJECT_EXT                     15       40       560       234
```

Web Server Certificate for Cisco SD-WAN Manager

To establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, you must generate a CSR to create a certificate, have it signed by a root CA, and then install it. You must install a separate certificate on each Cisco SD-WAN Manager server in a cluster by performing the following steps for each server:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Web Server Certificate** area, click **CSR**.
3. In the **Common Name** field, enter the domain name or IP address of the Cisco SD-WAN Manager server. For example, the fully-qualified domain name of Cisco SD-WAN Manager could be vmanage.org.local.
4. In the **Organizational Unit** field, enter the unit name within your organization — for example, Network Engineering.
5. In the **Organization** field, enter the exact name of your organization as specified by your root CA — for example, Viptela Inc.
6. In the **City** field, enter the name of the city where your organization is located — for example, San Jose.
7. In the **State** field, enter the state in which your city is located — for example, California.
8. In the **2-Letter Country Code** field, enter the two-letter code for the country in which your state is located. For example, the two-letter country code for the United States of America is US.
9. Click **Validity** and choose the validity period for the certificate.
10. Optionally, in the **Subject Alternative Name (SAN) DNS Names** field, enter the names of DNS severs to which the certificate trust should be extended. If you enter more than one DNS server name, separate each name with a space or a comma.

Note Cisco Catalyst SD-WAN supports SAN DNS names, from Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

11. Optionally, in the **Subject Alternative Name (SAN) URIs** field, enter the URIs of resources to which the certificate trust should be extended. If you enter more than one URI, separate each URI with a space or a comma.

    Enter each URI in *scheme*:*value* format, where *scheme* is the protocol for accessing the resource and *value* is the resource. For example, **`https://example.example.com`** or **`scp://example.example.com`**.

Note Cisco Catalyst SD-WAN supports SAN URIs beginning with Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

12. Click **Generate** to generate the CSR.
13. Send the CSR to your CA server to have it signed.
14. When you receive the signed certificate, click **Certificate** near the **Web Server Certificate** bar to install the new certificate. The **View** box displays the current certificate on the Cisco SD-WAN Manager server.
15. Copy and paste the new certificate in the box. Alternatively, click **Import** and **Select a File** to download the new certificate file.
16. Restart the application server and log in to Cisco SD-WAN Manager.

View Web Server Certificate Expiration Date

When you establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, configure the time period for which the certification is valid (in Step 8 in the previous section). At the end of this time period, the certificate expires. The **Web Server Certificate** bar shows the expiration date and time.

Starting 60 days before the certificate expires, the Cisco SD-WAN Manager dashboard displays a notification indicating that the certificate will expire soon. This notification is then displayed again 30, 15, and 7 days before the expiration date, and then daily.

Workflow to Configure IPv4 Static Route Tracking

Table 227: Feature History

Feature Name	Release Information	Description
Static Route Tracker for Service VPNs	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	To configure Static Route Tracking on Cisco vManage, configure an endpoint tracker using Cisco System template, and Configure a static route using the Cisco VPN template.
TCP/UDP Endpoint Tracker and Dual Endpoint Static Route Tracker for Cisco IOS XE Catalyst SD-WAN devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can now configure static route tracker with TCP/UDP endpoint using Cisco system template, and configure a static route using the Cisco VPN template. You can then add the configured dual trackers in a tracker group using **New Endpoint Tracker Groups** option.

1. Configure an endpoint tracker using the System template.
2. Configure a static route using the VPN template.
3. Apply the tracker to the next-hop address.

Create a Static Route Tracker

Use the **System Template** to create a tracker for static routes.

Note Delete existing static routes, if any, before you create a static route tracker. Configure a new static route tracker using the same prefix and next hop as the deleted static route.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Navigate to the **Cisco System** template for the device.

Note For information about creating a System template, see Create System Template.

4. Click **Tracker**. Click **New Endpoint Tracker** to configure the tracker parameters.

Table 228: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range is from 100 to 1000 milliseconds. Default is 300 milliseconds.
Interval	Time interval between probes to determine the status of the configured endpoint. Default is 60 seconds (1 minute). Range is from 20 to 600 seconds.
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range is from 1 to 10. Default is 3.
Tracker Type	From the drop-down, choose Global. From the Tracker Type field drop-down, choose Static Route. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure a tracker group with dual endpoints on Cisco IOS XE Catalyst SD-WAN devices and associate this tracker group to a static route.
Endpoint Type	Choose endpoint type IP Address.

Field	Description
End-Point Type: IP Address	IP address of the static route end point. This is the destination on the internet to which the router sends probes to determine the status of the route.

5. Click **Add**.
6. Click **Save**.
7. To create a tracker group, click **Tracker Groups** > **New Endpoint Tracker Groups** and configure the tracker parameters.

Note Ensure that you have created two trackers to form a tracker group.

Table 229: Tracker Group Parameters

Fields	Description
Name	Name of the tracker group.
Tracker Type	From the drop-down, choose **Global**. From the Tracker Type field drop-down, choose **Static Route**. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure a tracker group with dual endpoints on Cisco IOS XE Catalyst SD-WAN devices and associate this tracker group to a static route.
Tracker Elements	This field is displayed only if you chose **Tracker-group** as the tracker type. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to a static route.
Tracker Boolean	From the drop-down list, choose **Global**. This field is displayed only if you chose **tracker-group** as the **Tracker Type**. By default, the **OR** option is selected. Choose **AND** or **OR**. **OR** ensures that the static route status is reported as active if either one of the associated trackers of the tracker group report that the route is active. If you select **AND**, the static route status is reported as active if both the associated trackers of the tracker group report that the route is active.

8. Click **Add**.
9. Click **Save**.

Note Complete all the mandatory actions before you save the template.

Configure a Next Hop Static Route with Tracker

Use the **VPN** template to associate a tracker to a static route next hop.

Note You can apply only one tracker per static route next hop.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Navigate to the **Cisco VPN Template** for the device.

Note For information about creating a VPN template, see Create VPN Template.

4. Enter **Template Name** and **Description** as required.
5. In Basic Configuration, by default, VPN is set to 0. Set a VPN value within (1–511, 513–65530) range for service VPNs, for service-side data traffic on Cisco IOS XE Catalyst SD-WAN devices.

Note You can configure static route tracker only on service VPNs.

6. Click **IPv4 Route**.
7. Click **New IPv4 Route**.
8. In the **IPv4 Prefix** field, enter a value.
9. Click **Next Hop**.
10. Click **Add Next Hop with Tracker** and enter values for the fields listed in the table.

Parameter Name	Description
Address	Specify the next-hop IPv4 address.
Distance	Specify the administrative distance for the route.
Tracker	Enter the name of the gateway tracker to determine whether the next hop is reachable before adding that route to the route table of the device.
Add Next Hop with Tracker	Enter the name of the gateway tracker with the next hop address to determine whether the next hop is reachable before adding that route to the route table of the device.

11. Click **Add** to create the static route with the next-hop tracker.
12. Click **Save**.

Note You need to fill all the mandatory fields in the form to save the VPN template.

Monitor Static Route Tracker Configuration

View Static Route Tracker

To view information about a static tracker on a transport interface:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices.
3. Click **Real Time**.
4. From the **Device Options** drop-down list, choose **Endpoint Tracker Info**.

Verify Static Route Tracking Configuration Using CLI

Command Verification

Use the following command to verify if the configuration is committed. The following sample configuration shows tracker definition for a static route tracker and it's application to an IPv4 static route:

```
Device# show running-config | sec endpoint-tracker
endpoint-tracker tracker1
endpoint-ip 10.1.1.1
interval 60
multiplier 5
tracker-type static-route
endpoint-tracker tracker2
endpoint-ip 10.1.1.12
interval 40
multiplier 2
tracker-type static-route
track tracker2 endpoint-tracker
track tracker1 endpoint-tracker
```

Use the following command to verify the IPv4 route:

```
Device# show running-config | inc ip route
ip route vrf 1 10.1.1.11 255.255.0.0 10.20.2.17 track name tracker2
ip route vrf 1 10.1.1.12 255.255.0.0 10.20.24.17 track name tracker1
```

The following is a sample output from the **show endpoint-tracker static-route** command displaying individual static route tracker status:

```
Device#  show endpoint-tracker static-route
Tracker Name   Status     RTT (in msec) Probe ID
```

```
tcp-10001         UP         3             1
udp-10002         UP         1             6
```

The following is a sample output from the **show endpoint-tracker tracker-group** command displaying tracker group status:

```
Device# show endpoint-tracker group
Tracker Name               Element trackers name    Status         RTT in msec  Probe ID

group-tcp-10001-udp-10002  tcp-10001, udp-10002     UP(UP AND UP)  5, 1          9, 10
```

The following is a sample output from the **show endpoint-tracker records** command displaying tracker/tracker group configuration:

```
Device# show endpoint-tracker records
Record Name                Endpoint                 EndPoint Type Threshold(ms) Multiplier
 Interval(s) Tracker-Type
group-tcp-10001-udp-10002  tcp-10001 AND udp-10002  N/A           N/A           N/A
 N/A         static-tracker-group
tcp-10001                  10.1.1.1                 TCP           100           1
 20          static-route
udp-10002                  10.2.2.2                 UDP           100           1
 20          static-route
```

The following is a sample output from the **show ip static route vrf** command:

```
Device# show ip static route vrf 1
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, I - iEdge
       D1 - Dot1x Vlan Network, K - MWAM Route
       PP - PPP default route, MR - MRIPv6, SS - SSLVPN
       H - IPe Host, ID - IPe Domain Broadcast
       U - User GPRS, TE - MPLS Traffic-eng, LI - LIIN
       IR - ICMP Redirect, Vx - VXLAN static route
       LT - Cellular LTE, Ev - L2EVPN static route
Codes in []: A - active, N - non-active, B - BFD-tracked, D - Not Tracked, P - permanent,
-T Default Track
Codes in (): UP - up, DN - Down, AD-DN - Admin-Down, DL - Deleted
Static local RIB for 1
T  192.168.0.0 [1/0] via 10.1.19.16 [A]
```

Workflow to Configure RBAC for Policies

Table 230: Feature History

Feature Name	Release Information	Description
Role-Based Access Control By Resource Group	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can configure role-based access control (RBAC) based on sites or resource groups in Cisco vManage.

Feature Name	Release Information	Description
RBAC for Policies	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Configure RBAC for policies in Cisco vManage.
Co-Management: Granular Role-Based Access Control for Feature Templates	Cisco vManage Release 20.7.1	This feature introduces greater granularity in assigning RBAC permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.
Co-Management: Improved Granular Configuration Task Permissions	Cisco vManage Release 20.9.1	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user. .
RBAC for Security Operations and Network Operations Default User Groups	Cisco vManage Release 20.9.1	This feature provides the following default user groups: • network_operations user group for non-security policies • security_operations user group for security policies RBAC for policies allows you to create users and user groups with the required read and write permissions for security and non-security policies. Users can perform configuration and monitoring actions only for the authorized policy type.

Feature Name	Release Information	Description
Co-Management: Improved Granular Configuration for Resource group features	Cisco vManage Release 20.11.1	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces new permission options for the following configuration groups and feature profiles. • AppQoE under other feature profile • GPS under transport feature profile • Cisco VPN Interface GRE under WAN/LAN profile. • Cisco VPN Interface IPsec under WAN profile. • Cisco Multicast under LAN profile. • UCSE under other feature profile. • IPv4 Tracker and Tracker Group under transport and service feature profiles. • IPv6 DIA Tracker and Tracker Group, under transport feature profile.
Assigning Roles Locally for SSO-Authenticated Users	Cisco vManage Release 20.11.1	If you are using an identity provider, such as Okta, for security assertion markup language (SAML)-based single sign-on (SSO), then in most use cases, you define user roles through the identity provider. This feature enables you to assign user groups locally in Cisco SD-WAN Manager, in case no roles are defined for the user by the identity provider.

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

To configure RBAC for policies, use the following workflow:

1. Create user groups with required Read or Write (R/W) access to selected control or data policies. For details on creating user groups, refer Create User Groups .
2. Create users and assign them to required user groups. Refer Create Users.
3. Create or modify or view policy configurations as required. For information about configuring policies, see Configure Centralized Policies Using Cisco SD-WAN Manager.

Manage Users

From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** to add, edit, view, or delete users and user groups.

Please note the following:

- Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from Cisco SD-WAN Manager.
- Each user group can have read or write permission for the features listed in this section. Write permission includes Read permission.
- All user groups, regardless of the read or write permissions selected, can view the information displayed in the Cisco SD-WAN Manager Dashboard.

Table 231: User Group Permissions for Different Device Types

Permissions	See This Section
User group permissions related to Cisco IOS XE Catalyst SD-WAN device configuration.	User Group Permissions: Cisco IOS XE Catalyst SD-WAN Devices
User group permissions related to Cisco Catalyst Wireless Gateway device configuration.	User Group Permissions: Cisco Catalyst Wireless Gateway Devices

Manage a User Group

Users are placed in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. Cisco Catalyst SD-WAN software provides standard user groups, and you can create custom user groups, as needed:

- **basic**: Includes users who have permission to view interface and system information.
- **netadmin**: Includes the admin user, by default, who can perform all operations on the Cisco SD-WAN Manager. You can add other users to this group.
- **operator**: Includes users who have permission only to view information.
- Minimum supported release: Cisco vManage Release 20.9.1

  network_operations: Includes users who can perform non-security operations on Cisco SD-WAN Manager, such as viewing and modifying non-security policies, attaching and detaching device templates, and monitoring non-security data.
- Minimum supported release: Cisco vManage Release 20.9.1

  security_operations: Includes users who can perform security operations on Cisco SD-WAN Manager, such as viewing and modifying security policies, and monitoring security data.

Note: All user groups, regardless of the read or write permissions selected, can view the information displayed on the Cisco SD-WAN Manager Dashboard screen.

Delete a User Group

You can delete a user group when it is no longer needed. For example, you might delete a user group that you created for a specific project when that project ends.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.

3. Click the name of the user group you wish to delete.

Note You cannot delete any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

4. Click **Trash** icon.
5. To confirm the deletion of the user group, click **OK**.

Edit User Group Privileges

You can edit group privileges for an existing user group. This procedure lets you change configured feature read and write permissions for the user group needed.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. Select the name of the user group whose privileges you wish to edit.

Note You cannot edit privileges for the any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

4. Click **Edit**, and edit privileges as needed.
5. Click **Save**.

If an **admin** user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

Managing Resource Groups

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1

To configure Resource Groups:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Resource Groups**. The table dispalys a list of resource groups that are configured in Cisco SD-WAN Manager.
2. To edit or delete a resource group, click **...**, and click **Edit** or **Delete**.
3. To add new resource group, click **Add Resource Group**.
4. Enter **Resource Group Name** and the **Description**.
5. Under **Site ID**, enter **Range** or **Select ID(S)** from the drop-down list to include in the resource group.
6. To add the resource group to a device, click **Add**.

To add Users:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**. The Manage Users screen appears.
2. By default **Users** is selected. The table displays the list of users configured in the device.
3. To edit, delete, or change password for an existing user, click **...**, and click **Edit**, **Delete**, or **Change Password** respectively.
4. To add a new user, click **Add User**.
5. Add **Full Name**, **Username**, **Password**, and **Confirm Password** details.
6. From the **User Groups** drop-down list, select the user group where you want to add a user.
7. From the **Resource Group** drop-down list, select the resource group.

Note This field is available from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a.

8. Click **Add**.

Modify Policy Configurations

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

1. Login to Cisco SD-WAN Manager with the new user details.
2. You can modify or update the configurations based on the requirement.

When you login to Cisco SD-WAN Manager with new user details, you can view only the user group components that are assigned to you. For more details on configuring policies, see Cisco Catalyst SD-WAN Policies Configuration Guide

Assign Users to Configure RBAC for Policies

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

To Assign User to Create or Modify a CFlowd Data Policy

To create a CFlowd user group:

1. From Cisco SD-WAN Manager, choose **Administration** > **Manage Users**.
2. Click **User Groups** and **Add User Group**.
3. Enter **User Group Name**.

   For example, cflowd-policy-only.
4. Check the Read or Write check box against the CFlowD Policy feature that you want to assign to a user group.

5. Click **Add**.
6. You can view the new user group in the left navigation path. Click **Edit** to edit the existing read or write rules.
7. Click **Save**.

To create a CFlowd user:

1. In Cisco SD-WAN Manager, choose **Administration** > **Manage Users**.
2. Click **Users**.
3. Click **Add User**.
4. In the Add New User page, enter **Full Name**, **Username**, **Password**, and **Confirm Password** details.
5. Choose **cflowd-policy-only** from the **User Groups** drop-down.

   Allow the **Resource Group** to select the default resource group.
6. Click **Add**. You can view the new user in the Users window.
7. To edit the existing read or write rules for a user, click **Edit**.

To modify a Cflowd policy:

1. Login to Cisco SD-WAN Manager with the new user credentials.

   You can view access only to CFlowd Policies as your login is assigend to **cflowd-policy-only** user group.
2. You can create, modify, or update the configurations based on the requirement.

Verify Granular RBAC Permissions

Minimum supported release: Cisco vManage Release 20.7.1

Use this procedure to verify the permissions that you have configured for a user group.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. In the pane that displays the user groups, select a user group to display the read and write permissions assigned to the user group.
4. Scroll to the permissions that control template access to verify your configuration for the user group.

Workflow to Configure Route Leaking Using Cisco SD-WAN Manager

Table 232: Feature History

Feature Name	Release Information	Description
Route Leaking Between Global VRF and Service VPNs	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can configure route leaking between global VRF and service VPNs using the **Global Route Leak** option under the Cisco VPN feature template.
Redistribution of Replicated Routes to BGP, OSPF, and EIGRP Protocols	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	You can configure route redistribution between the global VRF and service VPNs using the **Global Route Leak** option under the Cisco VPN feature template.
Route Leaking between Inter-Service VPN	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	You can configure to leak routes and redistribute the leaked routes between the service VPNs at the same site using the **Route Leak** option in the Cisco SD-WAN Manager.

1. Configure and enable the Localized Policy and attach the Route Policy.
2. Configure and enable the Route Leaking feature between Global and Service VPN.
3. Configure and enable the Route Leaking feature between Service VPNs.
4. Attach the Service Side VPN Feature Template to the Device Template.

Configure Localized Route Policy

Configure Route Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Select **Localized Policy**.
3. From the **Custom Options** drop-down, under Localized Policy, select **Route Policy**.
4. Click **Add Route Policy**, and select **Create New**.
5. Enter a name and description for the route policy.
6. In the left pane, click **Add Sequence Type**.
7. In the right pane, click **Add Sequence Rule** to create a single sequence in the policy. Match is selected by default.
8. Select a desired protocol from the **Protocol** drop-down list. The options are: IPv4, IPv6, or both.

9. Click a match condition.
10. On the left, enter the values for the match condition.
11. On the right enter the action or actions to take if the policy matches.
12. Click **Save Match and Actions** to save a sequence rule.
13. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
    a. Click **Default Action** in the left pane.
    b. Click the **Pencil** icon.
    c. Change the default action to **Accept**.
    d. Click **Save Match and Actions**.
14. Click **Save Route Policy**.

Add the Route Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Choose the **Localized Policy**.
3. Click **Add Policy**.
4. Click **Next** in the Local Policy Wizard until you arrive at the **Configure Route Policy** option.
5. Click **Add Route Policy** and choose **Import Existing**.
6. From the **Policy** drop-down choose the route policy that is created. Click **Import**.
7. Click **Next**.
8. Enter the **Policy Name** and **Description**.
9. Click **Preview** to view the policy configurations in CLI format.
10. Click **Save Policy**.

Attach the Localized Policy to the Device Template

Note The first step in utilizing the Localized Policy that was created previously is to attach it to the device template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** and select the desired template.
3. Click **…**, and click **Edit**.
4. Click **Additional Templates**.
5. From the **Policy** drop-down, choose the **Localized Policy** that is created.

6. Click **Update**.

Note Once the localized policy has been added to the device template, selecting the **Update** option immediately pushes a configuration change to all of the devices that are attached to this device template. If more than one device is attached to the device template, you will receive a warning that they are changing multiple devices.

7. Click **Next** and then **Configure Devices**.
8. Wait for the validation process and push configuration from Cisco SD-WAN Manager to the device.

Configure and Enable Route Leaking between Global and Service VPNs

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. To configure route leaking, click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

Do one of the following:

- To create a feature template:
  a. Click **Add Template**. Choose a device from the list of devices. The templates available for the selected device display in the right pane.
  b. Choose the **Cisco VPN** template from the right pane.

Note Route leaking can be configured on service VPNs only. Therefore, ensure that the number you enter in the **VPN** field under **Basic Configuration** is one of the following: 1—511 or 513—65527.

For details on configuring various VPN parameters such as basic configuration, DNS, Virtual Router Redundancy Protocol (VRRP) tracking, and so on, see Configure a VPN Template. For details specific to the route leaking feature, proceed to Step c.

c. Enter Template Name and Description for the feature template.
d. Click **Global Route Leak** below the **Description** field.
e. To leak routes from the global VRF, click **Add New Route Leak from Global VPN to Service VPN**.
   1. In the **Route Protocol Leak from Global to Service** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.
   2. In the **Route Policy Leak from Global to Service** drop-down list, choose **Global**. Next, choose one of the available route policies from the drop-down list.
   3. For the **Redistribute to protocol (in Service VPN)** field, click **Add Protocol**.

In the **Protocol** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.

In the **Redistribution Policy** drop-down list, choose **Global**. Next, choose one of the available redistribution policies from the drop-down list.

4. Click **Add**.

f. To leak routes from the service VPNs to the global VRF, click **Add New Route Leak from Service VPN to Global VPN**.

1. In the **Route Protocol Leak from Service to Global** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.
2. In the **Route Policy Leak from Service to Global** drop-down list, choose **Global**. Next, choose one of the available route policies from the drop-down list.
3. For the **Redistribute to protocol (in Global VPN)** field, click **Add Protocol**.

   In the **Protocol** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.

   In the **Redistribution Policy** drop-down list, choose **Global**. Next, choose one of the available redistribution policies from the drop-down list.
4. Click **Add**.

g. Click **Save/Update**. The configuration does not take effect till the feature template is attached to the device template.

h. To redistribute the leaked routes using Cisco SD-WAN Manager, use CLI Add-on Feature templates to enter the configuration applicable to your environment. Here's an example.

```
Device(config)# router ospf 65535
Device(config-router)# redistribute vrf 1 ospf 103

Device(config)# router eigrp vpn
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 50
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global  ospf 65535
metric  1 2 3 4 5
```

After you create the CLI add-on template, you need to attach it to the protocol template to which you are redistributing routes. In this example, you would attach it to the EIGRP template.

- To modify an existing feature template:

a. Choose a feature template you wish to modify.

b. Click **...** next to the row in the table, and click **Edit**.

c. Click **Global Route Leak**.

d. To edit information, from the table under **Add New Route Leak from Global VPN to Service VPN** or **Add New Route Leak from Service VPN to Global VPN**, click **Edit**.

The update route leak dialog box appears.

e. Perform all operations from Step d of creating a feature template.

   Perform all operations from Step c of creating a feature template.

f. Click **Save Changes**.

g. Click **Update**.

Note

- The configuration does not take effect till the Service VPN feature template is attached to the device template.

Attach the Service Side VPN Feature Template to the Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** and select the desired template.
3. Click **…**, and click **Edit**.
4. Click **Service VPN**.
5. Click **Add VPN**. Select the Service VPN feature template listed in the Available VPN Templates pane. Click right-shift arrow and add the template to Selected VPN Templates list.
6. Click **Next** once it moves from the left (Available VPN Templates) to the right side (Selected VPN Templates).
7. Click **Add**.
8. Click **Update**.
9. Click **Next** and then **Configure Devices**.
10. Finally, wait for the validation process and push configuration from Cisco SD-WAN Manager to the device.

Workflow to Configure VRRP Tracking

Table 233: Feature History

Feature Name	Release Information	Description
VRRP Interface Tracking for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Starting this release, you can configure VRRP interface tracking through Cisco SD-WAN Manager feature template on Cisco IOS XE Catalyst SD-WAN Device.

1. Configure an object tracker. For more information, see Configure an Object Tracker, on page 679.

2. Configure VRRP for a VPN Interface template and associate the object tracker with the template. For more information, see Configure VRRP for a VPN Interface Template and Associate Interface Object Tracker, on page 680.

Configure an Object Tracker

Use the **Cisco System** template to configure an object tracker.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Navigate to the **Cisco System** template for the device.

Note To create a **System** template, see Create System Template

4. Click **Tracker** and choose **New Object Tracker** to configure the tracker parameters.

Table 234: Tracker Parameters

Field	Description
Tracker Type	Choose **Interface** or **SIG** to configure the object tracker.
Object ID	Enter the object ID number.
Interface	Choose global or device-specific tracker interface name.

5. Click **Add**.
6. Optionally, to create a tracker group, click **Tracker**, and click **Tracker Groups** > **New Object Tracker Groups** to configure the tracker parameters.

Note Ensure that you have created two trackers to create a track group.

Table 235: Object Tracker Group Parameters

Field	Description
Group Tracker ID	Enter the name of the tracker group.
Tracker ID	Enter the name of the object tracker that you want to group.

Field	Description
Criteria	Choose **AND** or **OR** explicitly. **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the route is active. If you choose **AND** operation, the transport interface status is reported as active if both the associated trackers of the tracker group report that the route is active.

Note Provide information in all the mandatory fields before you save the template.

7. Click **Add**.
8. Click **Save**.

Configure VRRP for a VPN Interface Template and Associate Interface Object Tracker

To configure VRRP for a **Cisco VPN** template, do the following:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Navigate to the **Cisco VPN Interface Ethernet** template for the device.

Note For information about creating a new **Cisco VPN Interface Ethernet** template, see Configure VPN Ethernet Interface.

4. Click **VRRP** and choose **IPv4**.
5. Click **New VRRP** to create a new VRRP or edit the existing VRRP and configure the following parameters:

Parameter Name	Description
TLOC Preference Change	(Optional) Choose **On** or **Off** to set whether the TLOC preference can be changed or not.
TLOC Preference Change Value	(Optional) Enter the TLOC preference change. Range: 1 to 4294967295.

6. Click the **Add Tracking Object** link, and in the **Tracking Object** dialog box that is displayed, click **Add Tracking Object**.
7. In the **Tracker ID** field, enter the Interface Object ID or Object Group Tracker ID.
8. From the **Action** drop-down list, choose **Decrement** and enter the **Decrement Value** as 1. Cisco vEdge Devices supports decrement value of 1.

   Or

   Choose **Shutdown**.
9. Click **Add**.
10. Click **Add** to save the VRRP details.
11. Click **Save**.

Monitor VRRP Configuration

To view information about VRRP configuration:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices.
3. Click **Real Time**.
4. From the **Device Options** drop-down list, choose **VRRP Information**.

Note You can view the status of the VRRP configuration in **Track State**.