# Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

**First Published:** 2019-04-15

**Last Modified:** 2024-04-24

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

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

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

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

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

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

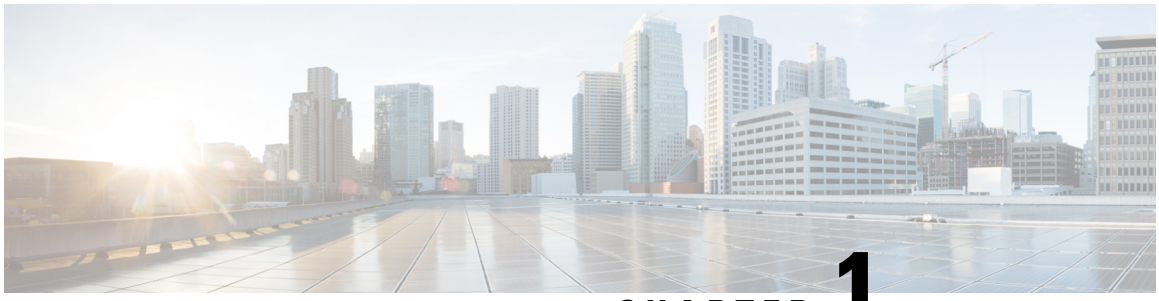
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

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

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

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

© 2019–2024 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

# Read Me First

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

### Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

### User Documentation

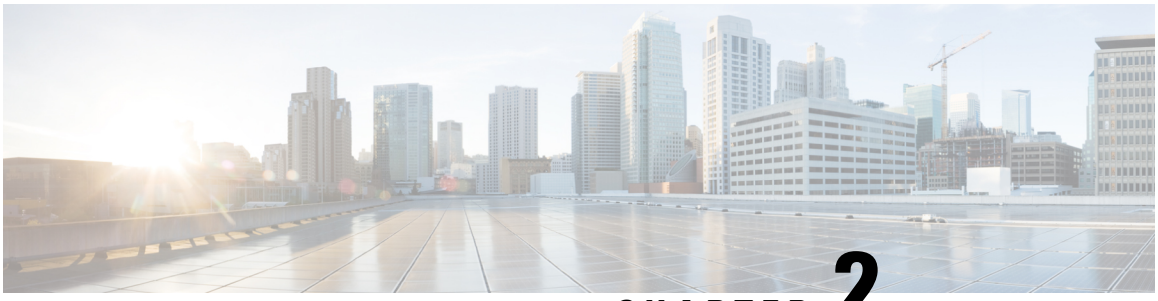
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

### Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

### Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



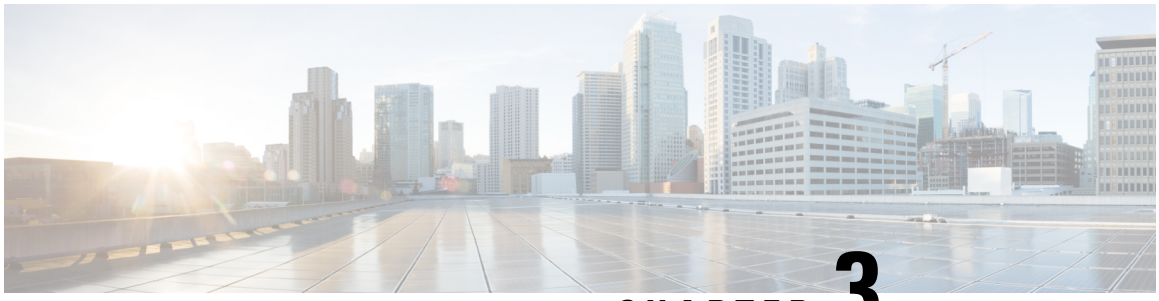
CHAPTER 2

# What's New in Cisco IOS XE (SD-WAN)

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

**Note** Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x



CHAPTER 3

# Cisco Catalyst SD-WAN Basic System Overview

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.


- Cisco Catalyst SD-WAN Basic System Overview, on page 6
- System and Interfaces Overview, on page 6
- Basic Settings for Cisco SD-WAN Manager, on page 10
- Configure Basic System Parameters, on page 17
- Configure Global Parameters, on page 23
- Configure NTP Servers Using Cisco SD-WAN Manager, on page 27
- Configure a Router as an NTP Primary, on page 30
- Configure NTP Servers for Cisco SD-WAN Control Components, on page 31
- Configure Time using CLI, on page 33
- Configure GPS Using Cisco SD-WAN Manager, on page 33
- Configure Automatic Bandwidth Detection, on page 35
- Configure System Logging Using CLI, on page 37
- SSH Terminal, on page 37
- HTTP/HTTPS Proxy Server for Cisco SD-WAN Manager Communication with External Servers, on page 38
- Bulk API Rate Limit for a Cisco SD-WAN Manager Cluster, on page 40

# Cisco Catalyst SD-WAN Basic System Overview

*Table 1: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| CMAC-AES-128 Authentication for NTP Servers | Cisco Catalyst SD-WAN Control Components Release 20.14.1 | Support for cipher-based message authentication code (CMAC) advanced encryption standard (AES) 128-bit (cmac-aes-128) authentication for network time protocol (NTP) server configuration for Cisco SD-WAN Control Components. |

# System and Interfaces Overview

Setting up the basic system-wide functionality of network devices is a simple and straightforward process. Basic parameters include defining host properties, such as name and IP address; setting time properties, including NTP; setting up user access to the devices; and defining system log (syslog) parameters.

In addition, the Cisco Catalyst SD-WAN software provides a number of management interfaces for accessing the Cisco Catalyst SD-WAN devices in the overlay network.

### Host Properties

All devices have basic system-wide properties that specify information that the Cisco Catalyst SD-WAN software uses to construct a view of the network topology. Each device has a system IP address that provides a fixed location of the device in the overlay network. This address, which functions the same way as a router ID on a router, is independent of any of the interfaces and interface IP addresses on the device. The system IP address is one of the four components of the Transport Location (TLOC) property of each device.

A second host property that must be set on all devices is the IP address of the Cisco SD-WAN Validator for the network domain, or a Domain Name System (DNS) name that resolves to one or more IP addresses for Cisco SD-WAN Validators. A Cisco SD-WAN Validator automatically orchestrates the process of bringing up the overlay network, admitting a new device into the overlay, and providing the introductions that allow the device and Cisco SD-WAN Controllers to locate each other.

Two other system-wide host properties are required on all devices, except for the Cisco SD-WAN Validators, to allow the Cisco Catalyst SD-WAN software to construct a view of the topology—the domain identifier and the site identifier.

To configure the host properties, see Cisco Catalyst SD-WAN Overlay Network Bring-Up Process.

### Time and NTP

The Cisco Catalyst SD-WAN software implements the Network Time Protocol (NTP) to synchronize and coordinate time distribution across the Cisco Catalyst SD-WAN overlay network. NTP uses a intersection algorithm to select the applicable time servers and avoid issues caused due to network latency. The servers can also redistribute reference time using local routing algorithms and time daemons. NTP is defined in RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification.

### User Authentication and Access with AAA, RADIUS, and TACACS+

The Cisco Catalyst SD-WAN software uses Authentication, Authorization, and Accounting (AAA) to provide security for the devices on a network. AAA, in combination with RADIUS and Terminal Access Controller Access-Control System (TACACS+) user authentication, controls which users are allowed access to devices, and what operations they are authorized to perform after they are logged in or connected to the devices.

Authentication refers to the process by which users trying to access the devices are authenticated. To access devices, users log in with a username and a password. The local device can authenticate users. Alternatively, authentication can be performed by a remote device, either a RADIUS server or a TACACS+ server, or both in a sequence.

Authorization determines whether a user is authorized to perform a given activity on a device. In the Cisco Catalyst SD-WAN software, authorization is implemented using role-based access. Access is based on groups that are configured on the devices. A user can be a member of one or more groups. User-defined groups are considered when performing authorization, that is, the Cisco Catalyst SD-WAN software uses group names received from RADIUS or TACACS+ servers to check the authorization level of a user. Each group is assigned privileges that authorize the group members to perform specific functions on the corresponding device. These privileges correspond to specific hierarchies of the configuration commands and the corresponding hierarchies of operational commands that members of the group are allowed to view or modify.

Beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, accounting generates a record of commands that a user executes on a device. Accounting is performed by a TACACS+ server.

For more information, see Role-Based Access with AAA.

### Authentication for WANs and WLANs

For wired networks (WANs), Cisco Catalyst SD-WAN devices can run IEEE 802.1X software to prevent unauthorized network devices from gaining access to the WAN. IEEE 802.1X is a port-based network access control (PNAC) protocol that uses a client–server mechanism to provide authentication for devices wishing to connect to the network.

IEEE 802.1X authentication requires three components:

- Requester: Client device, such as a laptop, that requests access to the Wide-Area Network (WAN). In the Cisco Catalyst SD-WAN overlay network, a supplicant is any service-side device that is running 802.1X-compliant software. These devices send network access requests to the router.
- Authenticator: A network device that provides a barrier to the WAN. In the overlay network, you can configure an interface device to act as an 802.1X authenticator. The device supports both controlled and uncontrolled ports. For controlled ports, the Cisco Catalyst SD-WAN device acts as an 802.1X port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port. For uncontrolled ports, Cisco Catalyst SD-WAN, acting as an 802.1X PAE, transmits and receives Extensible Authentication Protocol over IEEE 802 (EAP over LAN, or EAPOL) frames.
- Authentication server: Host that is running authentication software that validates and authenticates requesters that want to connect to the WAN. In the overlay network, this host is an external RADIUS server. This RADIUS server authenticates each client connected to the 802.1X port interface Cisco Catalyst SD-WAN device and assigns the interface to a virtual LAN (VLAN) before the client is allowed to access any of the services offered by the router or by the LAN.

For wireless LANs (WLANs), routers can run IEEE 802.11i to prevent unauthorized network devices from gaining access to the WLANs. IEEE 802.11i implements Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) to provide authentication and encryption for devices that want to connect to a WLAN.

WPA authenticates individual users on the WLAN using a username and a password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2–compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher. Authentication is done by either using preshared keys or through RADIUS authentication.

### Network Segmentation

The Layer 3 network segmentation in Cisco Catalyst SD-WAN is achieved through VRFs on Cisco IOS XE Catalyst SD-WAN devices. When you configure the network segmentation on a Cisco IOS XE Catalyst SD-WAN device using Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

### Network Interfaces

In the Cisco Catalyst SD-WAN overlay network design, interfaces are associated with VPNs that translate to VRFs. The interfaces that participate in a VPN are configured and enabled in that VPN. Each interface can be present only in a single VPN.

**Note** Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. When you complete the configuration on Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

The overlay network has the following types of VPNs/VRFs:

- **VPN 0**: **Transport VPN**, that carries control traffic using the configured WAN transport interfaces. Initially, VPN 0 contains all the interfaces on a device except for the management interface, and all the interfaces are disabled. This is the global VRF on Cisco IOS XE Catalyst SD-WAN software.
- **VPN 512**: **Management VPN**, that carries out-of-band network management traffic among the Cisco Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco Catalyst SD-WAN devices. For controller devices, by default, VPN 512 is not configured. On Cisco IOS XE Catalyst SD-WAN devices, the management VPN is converted to VRF Mgmt-Intf.

For each network interface, you can configure a number of interface-specific properties, such as DHCP clients and servers, VRRP, interface MTU and speed, and Point-to-Point Protocol over Ethernet (PPPoE). At a high level, for an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

### Management and Monitoring Options

There are various ways in which you can manage and monitor a router. Management interfaces provide access to devices in the Cisco Catalyst SD-WAN overlay network, allowing you to collect information from the devices in an out-of-band fashion and to perform operations on the devices, such as configuring and rebooting them.

The following management interfaces are available:

- CLI
- IP Flow Information Export (IPFIX)

- RESTful API
- SNMP
- System logging (syslog) messages
- Cisco SD-WAN Manager

### CLI

You can access a CLI on each device, and from the CLI, you configure overlay network features on the local device and gather operational status and information regarding that device. Using an available CLI, we strongly recommend that you configure and monitor all the Cisco Catalyst SD-WAN network devices from Cisco SD-WAN Manager, which provides views of network-wide operations and device status, including detailed operational and status data. In addition, Cisco SD-WAN Manager provides straightforward tools for bringing up and configuring overlay network devices, including bulk operations for setting up multiple devices simultaneously.

You can access the CLI by establishing an SSH session to a Cisco Catalyst SD-WAN device.

For a Cisco Catalyst SD-WAN device that is being managed by Cisco SD-WAN Manager, if you create or modify the configuration from the CLI, the changes are overwritten by the configuration that is stored in the Cisco SD-WAN Manager configuration database.

### IPFIX

The IP Flow Information Export (IPFIX) protocol, also called cflowd, is a tool for monitoring the traffic flowing through Cisco Catalyst SD-WAN devices in the overlay network and exporting information about the traffic to a flow collector. The exported information is sent in template reports, that contain both information about the flow and the data extracted from the IP headers of the packets in the flow.

Cisco Catalyst SD-WAN cflowd performs 1:1 traffic sampling. Information about all the flows is aggregated in the cflowd records; flows are not sampled.

**Note** Cisco Catalyst SD-WAN devices do not cache any of the records that are exported to a collector.

The Cisco Catalyst SD-WAN cflowd software implements cflowd Version 10, as specified in RFC 7011 and RFC 7012.

For a list of elements exported by IPFIX, see Traffic Flow Monitoring with Cflowd.

To enable the collection of traffic flow information, you must create data policies that identify the traffic of interest, and then direct that traffic to a cflowd collector. For more information, see Traffic Flow Monitoring with Cflowd.

You can also enable cflowd visibility directly on Cisco Catalyst SD-WAN devices without configuring a data policy, so that you can perform traffic flow monitoring on the traffic coming to the device from all the VPNs in the LAN. You can then monitor the traffic from Cisco SD-WAN Manager or from the device's CLI.

### RESTful API

The Cisco Catalyst SD-WAN software provides a RESTful API, which is a programmatic interface for controlling, configuring, and monitoring the Cisco Catalyst SD-WAN devices in an overlay network. You can access the RESTful API through Cisco SD-WAN Manager.

The Cisco Catalyst SD-WAN RESTful API calls expose the functionality of the Cisco Catalyst SD-WAN software and hardware to an application program. Such functionality includes the normal operations you perform to maintain the devices and the overlay network itself.

### SNMP

The Simple Network Management Protocol (SNMP) allows you to manage all the Cisco Catalyst SD-WAN devices in the overlay network. The Cisco Catalyst SD-WAN software supports SNMP v2c.

You can configure basic SNMP properties—device name, location, contact, and community—that allow the device to be monitored by an SNMP Network Management System (NMS).

You can configure trap groups and SNMP servers to receive traps.

The object identifier (OID) for the internet port of the SNMP MIB is 1.3.6.1.

SNMP traps are asynchronous notifications that a Cisco Catalyst SD-WAN device sends to an SNMP management server. Traps notify the management server of events, whether normal or significant, that occur on the Cisco Catalyst SD-WAN device. By default, SNMP traps are not sent to an SNMP server. Note that for SNMPv3, the PDU type for notifications, is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

### Syslog Messages

System logging operations use a mechanism that is similar to the UNIX **syslog** command to record system-wide, high-level operations that occur on the Cisco Catalyst SD-WAN devices in the overlay network. The log levels (priorities) of the messages are the same as those in standard UNIX commands, and you can configure the priority of the syslog messages that should be logged. Messages can be logged to files on the Cisco Catalyst SD-WAN device or to a remote host.

### Cisco SD-WAN Manager

Cisco SD-WAN Manager is a centralized network management system that allows configuration and management of all the Cisco Catalyst SD-WAN devices in the overlay network, and provides a dashboard displaying the operations of the entire network and of individual devices in the network. Three or more Cisco SD-WAN Manager servers are consolidated into a Cisco SD-WAN Manager cluster to provide scalability and management support for up to 6,000 Cisco Catalyst SD-WAN devices, to distribute Cisco SD-WAN Manager functions across multiple devices, and to provide redundancy of network management operations.

# Basic Settings for Cisco SD-WAN Manager

The System template is used to configure system-level Cisco SD-WAN Manager workflows.

Use the Settings screen to view the current settings and configure the setting for Cisco SD-WAN Manager parameters, including the organization name, Cisco SD-WAN Validators DNS name or IP address, certificate settings, and statistics collection.

The current setting for each item is displayed in the bar for each item, immediately following the name.

## Configure Organization Name

Before you can generate a Certificate Signing Request (CSR), you must configure the name of your organization. The organization name is included in the CSR.

In public key infrastructure (PKI) systems, a CSR is sent to a certificate authority to apply for a digital identity certificate.

To configure the organization name:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Organization Name**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.)
3. In **Organization Name**, enter the name of your organization. The organization name must be identical to the name that is configured on the Cisco SD-WAN Validator.
4. In **Confirm Organization Name**, re-enter and confirm your organization name.
5. Click **Save**.

**Note** technology-guides

After the control connections are up and running, the organization name bar is no longer editable.

# Configure Cisco SD-WAN Validator DNS Name or IP Address

1. From **Validator**, click **Edit** .
2. In **Validator DNS/IP Address: Port**, enter the DNS name that points to the Cisco SD-WAN Validator or the IP address of the Cisco SD-WAN Validator and the port number to use to connect to it.
3. Click **Save**.

**Note** The DNS cache timeout should be proportional to the number of Cisco Catalyst SD-WAN Validator IP addresses that DNS has to resolve, otherwise the control connection for Cisco SD-WAN Manager might not come up during a link failure. This is because, when there are more than six IP addresses (this is the recommended number since the default DNS cache timeout is currently two minutes) to check, the DNS cache timer expires even as the highest preferred interface tries all Cisco SD-WAN Validator IP addresses, before failing over to a different color. For instance, it takes about 20 seconds to attempt to connect to one IP address. So, if there are eight IP addresses to be resolved, the DNS cache timeout should be 20*8=160 seconds or three minutes.

# 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**.

# 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. Click **Enforce Software Version (ZTP)**.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, locate **Enforce Software Version (ZTP)** and click **Edit**.)
4. For a specific platform, enable enforcing the software version.
5. Do one of the following:

   • Use an image on a local server:

   a. In the **Image Location** field, choose **Local Server**.

   b. In the **Version/Image Name** field, choose an image.

   • Use an image on a remote server:

   a. In the **Image Location** field, choose **Remote Server**.

   b. In the **Remote Server Name** field, choose a server.

   c. In the **Image Filename** field, choose an image.

6. Click **Save**.

# Banner

Use the Banner template for Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Managers, Cisco Catalyst SD-WAN Controllers, s, and Cisco IOS XE Catalyst SD-WAN devices.

- To configure the banner text for login screens using Cisco SD-WAN Manager templates, create a Banner feature template to configure PIM parameters, as described in this topic.
- To configure a login banner for the Cisco SD-WAN Manager system, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

### Configure a Banner

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 device for which you are creating the template.
5. Click **Additional Templates** or scroll to the **Additional Templates** section.
6. From the **Banner** drop-down list, click **Create Template**. The **Banner** template form is displayed. This form contains fields for naming the template, and the fields for defining Banner parameters.
7. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In **Template Description**, 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.
9. To set a banner, configure the following parameters:

   ***Table 2: Parameters to be configured while setting a banner:***

| Parameter Name | Description |
|---|---|
| MOTD Banner | On a Cisco IOS XE Catalyst SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type **\n**. |
| Login Banner | Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type **\n**. |

10. To save the feature template, click **Save.**

*CLI equivalent:*

```
banner{login login-string | motd motd-string}
```

# Create a Custom Banner

To create a custom banner that is displayed after you log in to the Cisco SD-WAN Manager:

1. From **Banner**, click **Edit**.
2. In **Enable Banner**, click **Enabled**.
3. In **Banner Info**, enter the text string for the login banner or click **Select a File** to download a file that contains the text string.
4. Click **Save**.

# Collect Device Statistics

Enable or disable the collection of statistics for devices in the overlay network. By default, the collection of statistics is enabled for all the devices in the overlay network.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. To modify the settings for collecting device statistics, click **Statistics Database Configuration**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Statistics Setting** and **Edit**.

   By default, for every group of statistics (such as **Aggregated SAIE** and **AppHosting**), collection of statistics is enabled for all devices.
3. To enable the collection of a group of statistics for all devices, click **Enable All** for the particular group.
4. To disable the collection of a group of statistics for all devices, click **Disable All** for the particular group.
5. To enable the collection of a group of statistics for all devices only for consumption by Cisco SD-WAN Analytics, click **vAnalytics only** for the particular group.
6. To enable or disable the collection of a group of statistics for specific devices in the overlay network, click **Custom** for the particular group.

   In the **Select Devices** dialog box, depending on whether statistics collection is enabled or disabled for a device, the device is listed among **Enabled Devices** or **Disabled Devices** respectively.

   a. To enable statistics collection for one or more devices, choose the devices from **Disabled Devices** and move them to **Enabled Devices**.

**Tip** To choose all **Disabled Devices**, click **Select All**.

   b. To disable statistics collection for one or more devices, choose the devices from **Enabled Devices** and move them to **Disabled Devices**.

**Tip** To choose all **Enabled Devices**, click **Select All**.

   c. To save your selections, click **Done**.

      To discard your selections, click **Cancel**.
7. To apply the modified settings, click **Save**.

   To discard your changes, click **Cancel**.

   To revert to the default settings, click **Restore Factory Default**.

### Configure the Time Interval to Collect Device Statistics

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. To modify the time interval at which device statistics are collected, click **Statistics Configuration**.
3. Enter the desired **Collection Interval** in minutes.

- Default value: 30 minutes
- Minimum value: 5 minutes
- Maximum value: 180 minutes

4. To apply the modified settings, click **Save**.

   To discard your changes, click **Cancel**.

   To revert to the default settings, click **Restore Factory Default**.

# 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. Click **Maintenance Window**. (If you are using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier, click **Maintenance Window** and then click **Edit**.)

   To cancel the maintenance window, click **Cancel**.
3. Click the **Start Date** and **Start Time** drop-down list. Select the date and time when the **Maintenance Window** will start.
4. Click the **End Date** and **EndTime** drop-down list. 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 Basic System Parameters

Use the System template for all Cisco Catalyst SD-WAN devices.

To configure system-wide parameters using Cisco SD-WAN Manager templates:

1. Create a **System** feature template to configure system parameters.
2. Create an **NTP** feature template to configure NTP servers and authentication.
3. Configure the organization name and Cisco Catalyst SD-WAN Validator IP address on the Cisco SD-WAN Manager. These settings are appended to the device templates when the templates are pushed to devices.

### Create System 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 device for which you are creating the template.
5. To create a custom template for System, select the **Factory_Default_System_Template** and click **Create Template**.

   The System template form is displayed. This form contains fields for naming the template, and fields for defining the System parameters.
6. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In **Template Description**, 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 to the left of the parameter field and select one of the following:

***Table 3:***

| 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 Catalyst SD-WAN device to a device template.<br>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 Catalyst SD-WAN device to a device template.<br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Basic System-Wide Configuration

To set up system-wide functionality on a Cisco Catalyst SD-WAN device, select the **Basic Configuration** tab and then configure the following parameters. Parameters marked with an asterisk are required.

*Table 4:*

| Parameter Field | Description |
|---|---|
| Site ID* (on routers, Cisco SD-WAN Manager instances, and Cisco SD-WAN Controller) | Enter the identifier of the site in the Cisco Catalyst SD-WAN overlay network domain in which the device resides, such as a branch, campus, or data center. The site ID must be the same for all Cisco Catalyst SD-WAN devices that reside in the same site.*Range:* 1 through 4294967295 ($2^{32} – 1$) |
| System IP* | Enter the system IP address for the Cisco Catalyst SD-WAN device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0. |
| Timezone* | Select the timezone to use on the device. |
| Hostname | Enter a name for the Cisco Catalyst SD-WAN device. It can be up to 32 characters. |
| Location | Enter a description of the location of the device. It can be up to 128 characters. |
| Device Groups | Enter the names of one or more groups to which the device belongs, separated by commas. |
| Controller Groups | List the Cisco Catalyst SD-WAN Controller groups to which the router belongs. |
| Description | Enter any additional descriptive information about the device. |
| Console Baud Rate | Select the baud rate of the console connection on the router. *Values:* 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps).<br>Starting from Cisco vManage Release 20.3.1, the default value is 9600 on Cisco IOS XE Catalyst SD-WAN devices. |
| Maximum OMP Sessions | Set the maximum number of OMP sessions that a router can establish to a Cisco Catalyst SD-WAN Controller. *Range*: 0 through 100. *Default:* 2 |

To save the feature template, click **Save**.

To configure the DNS name or IP address of the Cisco Catalyst SD-WAN Validator in your overlay network, go to **Administration** > **Settings** screen and click **Validator**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **vBond**.)

### Configure the GPS Location

To configure a device location, select the **GPS** tab and configure the following parameters. This location is used to place the device on the Cisco SD-WAN Manager network map. Setting the location also allows Cisco SD-WAN Manager to send a notification if the device is moved to another location.

*Table 5:*

| Parameter Field | Description |
|---|---|
| Latitude | Enter the latitude of the device, in the format *decimal-degrees*. |
| Longitude | Enter the longitude of the device, in the format *decimal-degrees*. |

To save the feature template, click **Save**.

### Configure Interface Trackers for NAT Direct Internet Access

The DIA tracker helps determine if the internet or external network becomes unavailable. This feature is useful when NAT is enabled on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet.

If the internet or external network becomes unavailable, the router continues to forward traffic based on the NAT route in the service VPN. Traffic that is forwarded to the internet gets dropped. To prevent the internet-bound traffic from being dropped, configure the DIA tracker on the edge router to track the status of the transport interface. The tracker periodically probes the interface IP address of the end point of the tunnel interface to determine the status of the transport interface. The tracker determines the status of the internet and returns the data to the attach points that are associated with the tracker.

When the tracker is configured on the transport interface, the interface IP address is used as a source IP address for probe packets.

IP SLA monitors the status of probes and measures the round trip time of these probe packets and compares the values with the configured latency in the probe. When the latency exceeds the configured threshold value, the tracker considers the network as unavailable.

If the tracker determines that the local internet is unavailable, the router withdraws the NAT route and reroutes the traffic based on the local routing configuration to overlay.

The local router continues to periodically check the status of the path to the interface. When it detects that the path is functioning again, the router reinstalls the NAT route to the internet.

For more information on NAT DIA tracker for Cisco IOS XE Catalyst SD-WAN devices, see the NAT DIA Tracker section of the *Cisco Catalyst SD-WAN NAT Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

### Configure NAT DIA Tracker

To track the status of transport interfaces that connect to the internet (Network Address Translation Direct Internet Access (NAT DIA)), click **Tracker** > **Add New Tracker** and configure the following parameters:

*Table 6:*

| Parameter Field | Description |
|---|---|
| Name | Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers. |
| Tracker Type | Choose an interface, static route. |

| Parameter Field | Description |
|---|---|
| Threshold | How long to wait for the probe to return a response before declaring that the transport interface is down. *Range:* 100 through 1000 milliseconds. *Default:* 300 milliseconds. |
| Interval | How often probes are sent to determine the status of the transport interface. *Range:* 10 through 600 seconds. *Default:* 60 seconds (1 minute) |
| Multiplier | Number of times to resend probes before declaring that the transport interface is down. *Range:* 1 through 10. *Default:* 3 |
| End Point Type: IP Address | IP address of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.<br>**Note** In Cisco SD-WAN Release 20.5.1 and later releases, if the tracker receives an HTTP response status code, which is less than 400, the endpoint is reachable.<br>Prior to Cisco SD-WAN Release 20.5.1, the endpoint is reachable if the tracker receives an HTTP response status code of 200. |
| End Point Type: DNS Name | DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. |

To save a tracker, click **Add**.

To save the feature template, click **Save**.

### Configure NAT DIA Tracker Using the CLI

Configure NAT DIA tracker

```
Device(config)# endpoint-tracker tracker1
    Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
    Device(config-endpoint-tracker)# threshold 100
    Device(config-endpoint-tracker)# multiplier 5
    Device(config-endpoint-tracker)# interval 10

Device(config)# endpoint-tracker tracker1
    Device(config-endpoint-tracker)# endpoint-api-url https://ip-address:8443/apidocs
    Device(config-endpoint-tracker)# threshold 100
    Device(config-endpoint-tracker)# multiplier 5
    Device(config-endpoint-tracker)# interval 10
```

### Apply Tracker to an Interface

To apply a tracker to an interface, configure it in the **VPN Interface Cellular**, **VPN Interface Ethernet**, **VPN Interface NAT Pool**, or **VPN Interface PPP** configuration templates. You can apply only one tracker to an interface.

### Monitor NAT DIA Endpoint Tracker 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 **Endpoint Tracker Info**.

### Configure Advanced Options

To configure additional system parameters, click **Advanced**:

***Table 7:***

| Parameter Name | Description |
|---|---|
| Control Session Policer Rate | Specify a maximum rate of DTLS control session traffic, to police the flow of control traffic. *Range:* 1 through 65535 pps. *Default:* 300 pps |
| Port Hopping | Click **On** to enable port hopping, or click **Off** to disable it. When a Cisco Catalyst SD-WAN device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other Cisco Catalyst SD-WAN devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. To disable port hopping on an individual TLOC (tunnel interface), use the VPN Interface Ethernet configuration template. *Default:* Enabled (on routers); disabled (on Cisco SD-WAN Manager devices and Cisco Catalyst SD-WAN Controllers). |
| Port Offset | Enter a number by which to offset the base port number. Configure this option when multiple Cisco Catalyst SD-WAN devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. *Values:* 0 through 19 |
| Track Transport | Click **On** to regularly check whether the DTLS connection between the device and a Cisco Catalyst SD-WAN Validator is up. Click **Off** to disable checking. By default, transport checking is enabled. |
| Track Interface | Set the tag string to include in routes associated with a network that is connected to a non-operational interface. *Range:* 1 through 4294967295 |
| Gateway Tracking | Click **On** to enable or click **Off** to Disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the device's route table. *Default:* Enabled |
| Collect Admin Tech on Reboot | Click **On** to collect admin-tech information when the device reboots. |
| Idle Timeout | Set how long the CLI is inactive on a device before the user is logged out. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires. *Range:* 0 through 300 seconds. *Default:* CLI session does not time out. |

To save the feature template, click **Save**.

*CLI equivalent:*

```
system
   admin-tech-on-failure  allow-same-site-tunnels
   control-session-pps rate eco-friendly-mode
   host-policer-pps rate

   icmp-error-pps rate

   idle-timeout seconds multicast-buffer-percent percentage

   port-hop  port-offset number
   system-tunnel-mtu bytes timer
    dns-cache-timeout minutes track-default-gateway
    track-interface-tag number

   track-transport  upgrade-confirm minutes
```

# Configure Global Parameters

***Table 8: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Configure Global Parameters | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | This feature lets you configure HTTP and Telnet server settings, and several other device settings, from Cisco SD-WAN Manager. |

Use the Global Settings template to configure a variety of global parameters for all Cisco IOS XE Catalyst SD-WAN devices, including:

- Various services, such as HTTP and Telnet
- NAT64 timeouts
- HTTP authentication mode
- TCP keepalive
- TCP and UDP small servers
- Console logging
- IP source routing
- VTY line logging
- SNMP IFINDEX persistence
- BOOTP server

Before applying the global parameters to a device, you can view the current configuration of the device and view the differences between the parameter values that you have set in the Global Settings template and the current values on a device.

To configure global settings using Cisco SD-WAN Manager:

1. Create a feature template to configure global settings.
2. Create a device template and include the Global Settings feature template.
3. (Recommended) Before applying the device template to a device, use the Preview Device Configuration and View Configuration Differences, on page 202 feature to review the differences between the configuration currently on the device and the configuration to be sent to the device. This step is recommended because applying the device template overwrites the existing configuration on a device.

### Limitations

Cisco Catalyst SD-WAN can apply the global settings feature template only to devices running Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x or later.

# Create Global Settings 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. In the left pane, select a device type.
5. Select the **Global Settings** template.
6. Provide a name and description for the template.
7. For each of the parameters, use the default or set custom values as desired.

| Parameter | Description |
|---|---|
| **Services** | |
| HTTP Server | Enable or disable HTTP server. |
| HTTPS Server | Enable or disable secure HTTPS server. |
| Passive FTP | Enable or disable passive FTP. |
| IP Domain-Lookup | Enable or disable domain name server (DNS) lookup. |
| Arp Proxy | Enable or disable proxy ARP. |
| RSH/RCP | Enable or disable remote shell (RSH) and remote copy (RCP) on the device. |
| Telnet (Outbound) | Enable or disable outbound telnet. |

| Parameter | Description |
|---|---|
| CDP | Enable or disable Cisco Discovery Protocol. Starting from Cisco SD-WAN 17.3 release, CDP on interfaces is enabled when the **cdp run** command is executed globally on Cisco ASR 1000 series devices. |
| **Other Settings** | |
| TCP Keepalives (In) | Enable or disable generation of keepalive timers when incoming network connections are idle. |
| TCP Keepalives (Out) | Enable or disable generation of keepalive timers when outgoing network connections are idle. |
| TCP Small Servers | Enable or disable small TCP servers (for example, ECHO). |
| UDP Small Servers | Enable or disable small UDP servers (for example, ECHO). |
| Console Logging | Enable or disable console logging. By default, the router sends all log messages to its console port. |
| IP Source Routing | Enable or disable IP source routing. IP source routing is a feature that enables the originator of a packet to specify the path for the packet to use to get to the destination. |
| VTY Line Logging | Enable or disable the device to display log messages to a VTY session in real time. |
| SNMP IFINDEX Persist | Enable or disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots. |
| Ignore BOOTP | Enable or disable BOOTP server. When enabled, the device listens for the bootp packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets. |
| **NAT64** | |
| UDP Timeout | NAT64 translation timeout for UDP<br>Range: 1 to 65536 (seconds)<br>Default: 300 seconds (5 minutes)<br>**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default UDP Timeout value for NAT64 has been changed to 300 seconds (5 minutes). |
| TCP Timeout | NAT64 translation timeout for TCP<br>Range: 1 to 65536 (seconds)<br>Default: 3600 seconds (1 hour)<br>**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default TCP Timeout value for NAT64 has been changed to 3600 seconds (1 hour). |

| Parameter | Description |
|---|---|
| **HTTP Authentication** | |
| HTTP Authentication | HTTP authentication mode<br>Accepted values: Local, AAA<br>Default: Local |
| **SSH Version** | |
| SSH version | Specify an SSH version.<br>Default value: Version 2 |

8. Enter a name for the template and click **Save**.

# CLI Equivalent

Services (enable):

```
system
    ip http server
    ip http secure-server
    ip ftp passive
    ip domain lookup
    ip arp proxy disable
    ip rcmd rsh-enable
    ip rcmd rcp-enable
    cdp run enable
```

**Note** Starting from Cisco SD-WAN 17.3 release, CDP on interfaces is enabled when the **cdp run** command is executed globally on Cisco ASR 1000 series devices.

Telnet outbound enable:

```
system
    line vty 0 4
        transport input telnet ssh
```

Services (disable):

```
system
    no ip http server
    no ip http secure-server
    no ip ftp passive
    no ip domain lookup
    no ip arp proxy disable
    no ip rcmd rsh-enable
    no ip rcmd rcp-enable
    no cdp run enable
```

Telnet outbound disable:

```
system
    line vty 0 4
        transport input ssh
```

Other settings (enable):

```
system
    service tcp-keepalives-in
    service tcp-keepalives-out
    service tcp-small-servers
    service udp-small-server
    logging console
    ip source-route
    logging monitor
    snmp-server ifindex persist
    ip bootp server
```

Other settings (disable):

```
system
    no service tcp-keepalives-in
    no service tcp-keepalives-out
    no service tcp-small-servers
    no service udp-small-server
    no logging console
    no ip source-route
    no logging monitor
    no snmp-server ifindex persist
    no ip bootp server
```

NAT 64:

```
system
    nat64 translation timeout udp timeout
    nat64 translation timeout tcp timeout
```

HTTP Authentication:

```
system
    ip http authentication {local | aaa}
```

# Configure NTP Servers Using Cisco SD-WAN Manager

Configure NTP servers on your devices in order to synchronize time across all the devices in the Cisco overlay network. You can configure up to four NTP servers, and they must all be located or reachable in the same VPN.

Other devices are allowed to ask a Cisco Catalyst SD-WAN device for the time, but no devices are allowed to use a Cisco Catalyst SD-WAN device as an NTP server.

**Note** For the NTP to properly function when using Global VRF on the Cisco IOS XE Catalyst SD-WAN devices, you must configure **allow-service ntp** for the tunnel interface on the Cisco VPN Interface Ethernet template.

To configure an NTP server using Cisco SD-WAN Manager templates:

1. Create an NTP feature template to configure NTP parameters, as described in this section.
2. Configure the timezone in the System template.

### 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. 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 wish to create the template.
5. Click **Basic Information**.
6. From **Additional Cisco System Templates**, click **NTP**.
7. From the **NTP** drop-down list, choose **Create Template**.

   The **Cisco NTP** template form is displayed. This form contains fields for naming the template, and fields for defining NTP parameters.
8. In **Template Name**, enter a name for the template.

   The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, 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 value 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 9: Setting Parameter Scope***

| 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.<br><br>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 Create a Template Variables Spreadsheet.<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Configure an NTP Server

To configure an NTP server, click **Server**, and click **Add New Server**, and configure the following parameters. Parameters marked with an asterisk are required to configure an NTP server.

*Table 10: Parameters for Configuring an NTP Server*

| Parameter Name | Description |
|---|---|
| **Hostname/IP Address*** | Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server. |
| **Authentication Key ID*** | Specify the MD5 authentication key associated with the NTP server, to enable authentication. For the key to work, you must mark it as trusted in the **Trusted Keys** field, under **Authentication**.<br>**Note** From Cisco Catalyst SD-WAN Control Components Release 20.14.1, you can use CMAC-AES authentication when configuring NTP servers for Cisco SD-WAN Control Components. This requires configuration using a CLI template. |
| **VPN ID*** | Enter the number of the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN.<br>The valid range is from 0 through 65530. |
| **Version*** | Enter the version number of the NTP protocol software. The range is from 1 through 4. The default is 4. |
| **Source Interface** | Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored. |
| **Prefer** | Click **On** if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one at the highest stratum level. |

To add an NTP server, click **Add**.

To add another NTP server, click **Add New Server**. You can configure up to four NTP servers. The Cisco Catalyst SD-WAN software uses the server at the highest stratum level.

To edit an NTP server, click the pencil icon to the right of the entry.

To delete an NTP server, click the trash icon to the right of the entry.

To save the feature template, click **Save**.

### Configure NTP Authentication Keys

To configure the authentication keys used to authenticate NTP servers, click **Authentication**, and then the **Authentication Key**. Then click **New Authentication Key**, and configure the following parameters. Parameters marked with an asterisk are required to configure the authentication keys.

*Table 11: Parameters for Configuring NTP Authentication Keys*

| Parameter Name | Description |
|---|---|
| **Authentication Key ID*** | Enter the following values:<br>• Authentication Key: Enter an authentication key ID. Valid range is from 1 to 65535.<br>• Authentication Value: Enter either a cleartext key or an AES-encrypted key. |
| **Authentication Value*** | Enter an authentication key. For this key to be used, you must designate it as trusted. To associate a key with a server, enter the same value that you entered in the **Authentication Key ID** field under **Server**. |

To configure the trusted keys used to authenticate NTP servers, under **Authentication**, click **Trusted Key**, and configure the following parameters.

*Table 12: Parameters for Configuring Trusted Keys*

| Parameter Name | Description |
|---|---|
| **Trusted Keys*** | Enter the authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value that you entered for the **Authentication Key ID** field under **Server**. |

# Configure a Router as an NTP Primary

*Table 13: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Configuring a Router as an NTP Primary | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | This feature lets you configure a supported router as an NTP primary router. Other nodes in a Cisco Catalyst SD-WAN deployment synchronize their clocks to the NTP primary router. This configuration is useful if you do not have an NTP server in your deployment. |

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 NTP Servers for Cisco SD-WAN Control Components

### Configure NTP Servers Using CLI Commands

### Before You Begin

For information about using a CLI template, see CLI Templates.

By default, CLI templates execute commands in global configuration mode.

### Configure NTP Servers for Cisco SD-WAN Control Components

1. Enter system configuration mode.

   **system**

2. Enter NTP configuration mode.

   **ntp**

3. Enter keys configuration mode.

   **keys**

4. Configure an authentication type to use for an NTP server. Assign a key for the authentication type, and assign one of the following authentication methods: MD5, CMAC-AES-128. Using multiple instances of the **authentication** command, you can configure authentication for multiple NTP servers.

   **authentication** *authentication-key-id* {**md5** *md5-authentication-key* | **cmac-aes-128** *cmac-authentication-key*}

**Note** The CMAC-AES option is available from Cisco Catalyst SD-WAN Control Components Release 20.14.1.

5. Designate an authentication type as trusted. Optionally, you can include multiple authentication key IDs.

   **trusted** *authentication-key-id* {*authentication-key-id*}[*authentication-key-id*]

6. Exit keys configuration mode.

   **exit**

7. Configure an NTP server, including the VPN and version, and optionally an authentication key. You can configure multiple NTP servers.

   **server** {*server-ip* | *fully-qualified-domain-name*}
   **key** *authentication-key*
   **vpn** *vpn-id*
   **version** *version-id*
   **exit**

### Example

Here is an example for configuring two authentication types and three NTP servers. Two servers are trusted and use an authentication key, and one server is generic. Authentication key 1001 uses MD5 and key 1002 uses CMAC-AES-128.

```
system ntp
  keys
    authentication 1001 md5 password1
    authentication 1002 cmac-aes-128 password2
    trusted 1001 1002
  !
  server 192.168.10.1
    key 1001
    vpn 512
    version 4
  exit
  server 192.168.10.2
    key 1002
    vpn 512
    version 4
  server us.pool.ntp.org
    vpn 512
    version 4
  exit
  !
!
```

**Note** The passwords above are in plain text. When using a CLI template, you can encrypt passwords.

# Configure Time using CLI

You can set the time locally on your without using NTP if you do not need to ensure that time is synchronized across an entire network of devices. You can also set the time locally on any device as it is joining the network, in addition to configuring an NTP server. The local time gets overwritten by the official NTP time once the device contacts the NTP server.

```
clock set 12:00:00 31 May 2019
```

# 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 14:***

| Parameter Name | Description |
|---|---|
| GPS | Click **On** to enable the GPS feature on the router. |
| GPS Mode | Select the GPS mode:<br>• **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.<br>• **Standalone**—Use satellite information when determining position.<br>**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.<br>**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.<br>**Note** This option is not used for configuring geofencing. |

| Parameter Name | Description |
|---|---|
| Destination Port | (Optional) Enter the number of the port to use to send NMEA data to the server.<br>**Note** This option is not used for configuring geofencing. |

To save the feature template, click **Save**.

# Configure Automatic Bandwidth Detection

*Table 15: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Day 0 WAN Interface Automatic Bandwidth Detection | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>Cisco vManage Release 20.5.1 | This feature enables 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 System Logging Using CLI

Use the following command to configure system logging on Cisco SDWAN.

```
config-transaction [IP address | description | alarm | buffered | buginf | console |
discriminator
 esm | event | facility | file | history | host | origin-id | persistent | rate-limit |
snmp-authfail | snmp-trap | source-interface
 trap | userinfo]
```

# SSH Terminal

Use the SSH Terminal screen to establish an SSH session to a router. From an SSH session, you can issue CLI commands on a router.

### Establish an SSH Session to a Device

To establish an SSH session to a device:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Select the device on which you wish to collect statistics:
   a. Select the device group to which the device belongs.
   b. If needed, sort the device list by its status, hostname, system IP, site ID, or device type.
   c. Click the device to select it.
3. Enter the username and password to log in to the device.

You can now issue CLI commands to monitor or configure the device.

# HTTP/HTTPS Proxy Server for Cisco SD-WAN Manager Communication with External Servers

*Table 16: 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<br>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. |
| Cisco SD-WAN Manager HTTP/HTTPS Proxy Server Support Over IPv6 | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a<br>Cisco Catalyst SD-WAN Manager Release 20.13.1 | You can now configure an IPv6 address when configuring an HTTP/HTTPs proxy server. |

The following are some instances in which Cisco SD-WAN Manager uses an HTTP/HTTPS connection to an external server:

- Certificate request or renewal
- Cisco Plug and Play integration
- Smart Licensing Using Policy
- Cloud OnRamp
- Software image download
- Data upload to Cisco SD-WAN Analytics

In Cisco vManage Release 20.4.1 and earlier releases, you must permit this HTTP/HTTPS communication in the firewall configured on your on-premises Cisco SD-WAN Manager instance. Beginning Cisco vManage Release 20.5.1, you can channel the HTTP/HTTPS communication via an HTTP/HTTPS proxy server. With the HTTP/HTTPS proxy server configured, you can restrict HTTP/HTTPS communication with external servers while configuring the firewall and secure the system further.

Traffic is directed through the HTTP/HTTPS proxy server in the following cases:

- HTTPS connection for Symantec or Cisco automated certificate request or renewal
- REST API calls to URLs of the following domains:
    - cisco.com
    - amazonaws.com
    - microsoft.com
    - office.com

- microsoftonline.com

Once every 24 hours, Cisco SD-WAN Manager checks whether the configured HTTP/HTTPS proxy server is reachable. If the proxy server is unreachable, Cisco SD-WAN Manager raises the alarm `HTTPS proxy server {IP} not reachable`.

### Restrictions

- When configured to communicate with external servers via an HTTP/HTTPS proxy server, Cisco SD-WAN Manager resolves FQDNs locally or through configured DNS servers, bypassing the proxy server. Cisco SD-WAN Manager then sends the HTTP/HTTPS connections resulting from the resolution to the proxy server. DNS queries for the resolution of external server FQDNs must be successful before Cisco SD-WAN Manager can send resulting HTTP/HTTPS connections to the HTTP/HTTPS proxy server.
- Use of the HTTP/HTTPS proxy server is not supported for communication between the SD-AVC container in Cisco SD-WAN Manager and external services.

# Configure HTTP/HTTPS Proxy Server

### Prerequisites

Enable out of band interface on single node using **Administration** > **Cluster Management** before configuring proxy server.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Open **HTTP/HTTPS Proxy**.
3. For the **Enable HTTP/HTTPS Proxy** setting, click **Enabled**.
4. Enter the **HTTP/HTTPS Proxy IP Address** and **Port** number.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. For releases from Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
5. Enter a **Non Proxy Host/IP List**.

   This list is a pipe (|) separated list of IP addresses or hostnames that are not to be proxied.
6. 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.

# Bulk API Rate Limit for a Cisco SD-WAN Manager Cluster

*Table 17: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Bulk API Rate Limit for a Cisco SD-WAN Manager Cluster | Cisco vManage Release 20.10.1 | For a Cisco SD-WAN Manager cluster, the rate limit for bulk APIs equals (rate-limit per node) * (number of nodes in the cluster). Cisco SD-WAN Manager distributes bulk API requests among the nodes in the cluster. With these changes, you can retrieve data faster from a Cisco SD-WAN Manager cluster through bulk APIs. |

In Cisco vManage Release 20.9.x and earlier releases, you send bulk API requests to a node in the Cisco SD-WAN Manager cluster. The bulk API throughput is constrained by the rate-limit per node. To increase the throughput, you must send separate bulk API requests to each node in the cluster and the collate the API responses.

From Cisco vManage Release 20.10.1, send bulk API requests to the Cisco SD-WAN Manager cluster. Cisco SD-WAN Manager distributes the API requests among the clusters in the node. This distribution increases the rate limit to (rate-limit per node) * (number of nodes in the cluster), allowing you to retrieve more data in a shorter duration compared to a bulk API request addressed to a single node. With the distribution, you need not send separate bulk API requests to two or more nodes in the cluster or collate the API responses.

## Configure Bulk API Rate Limit

1. Log in to one of the Cisco SD-WAN Manager nodes in the Cisco SD-WAN Manager cluster and configure the following command:

   vManage# **request nms server-proxy set ratelimit**

2. The command-line displays the following prompt about the rate limit for non-bulk APIs:

   ```
   Do you want to reconfigure rate limit for URL non bulk api [y/n] :
   ```

   Enter **n**.

3. The command-line displays the following prompt about the rate limit for bulk APIs:

   ```
   Do you want to reconfigure rate limit for URL bulk api /dataservice/data/device/statistics
    [y/n] :
   ```

   Enter **y**.

4. Enter the per-node rate limit in response to a prompt similar to the following:

   ```
   Enter the PER NODE rate limit for URL bulk api /dataservice/data/device/statistics [144
    load balanced across all nodes at present] :
   ```

This prompt is from a three-node Cisco SD-WAN Manager cluster, with the bulk API rate limit configured to the default value of 48 requests per node. Across all the three nodes, the bulk API rate limit is (rate-limit/node) * 3, which is 144 requests.

Before you enter the rate limit, consider its effect on Cisco SD-WAN Manager resources.

5. Enter the unit time for which the rate limit applies in response to a prompt similar to the following.

   You can apply a rate limit per second, minute, hour, or day. The default unit is minute.

   ```
   Enter the rate limit unit (second, minute, hour, day) for URL bulk api
   /dataservice/data/device/statistics [minute] :
   ```

   Cisco vMange applies the rate limit on all the Cisco SD-WAN Manager instances in the cluster. The command line displays the following message:

   ```
   Propagating rate limit update across all nodes. Please wait.
   ```

   After the rate limit is applied, Cisco SD-WAN Manager prompts you to restart the server-proxy on all nodes and the command line returns to the privileged EXEC mode:

   ```
   Done. Please restart server-proxy on all nodes using "request nms server-proxy restart"
    command.
   vManage#
   ```

6. Restart the server-proxy using the following command:

   vManage# **request nms server-proxy restart**

7. Log in to the other Cisco SD-WAN Manager nodes in the cluster and restart the server-proxy using the **request nms server-proxy restart** command.

In the following example, the bulk API rate limit per node is set to 50 requests per minute.

```
vManage# request nms server-proxy set ratelimit
Do you want to reconfigure rate limit for URL non bulk api [y/n] : n
Do you want to reconfigure rate limit for URL bulk api /dataservice/data/device/statistics
 [y/n] : y
Enter the PER NODE rate limit for URL bulk api /dataservice/data/device/statistics [144
load balanced across all nodes at present] : 50
Enter the rate limit unit (second, minute, hour, day) for URL bulk api
/dataservice/data/device/statistics [minute] : minute
Propagating rate limit update across all nodes. Please wait.
Done. Please restart server-proxy on all nodes using "request nms server-proxy restart"
command.
vManage# request nms server-proxy restart
```

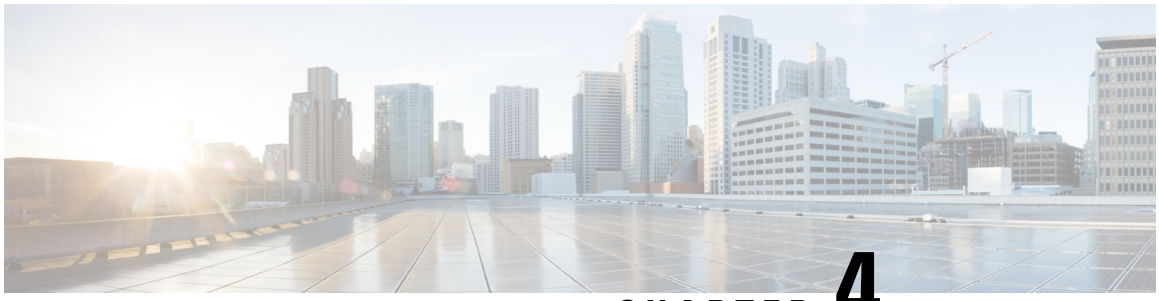
# View Bulk API Rate Limit

To view the bulk API rate limit, log in to any node in the Cisco SD-WAN Manager cluster and use the **show nms server-proxy ratelimit** command.

The following is a sample command output:

```
vManage# show nms server-proxy ratelimit
Non Bulk API: 100/second (per node)
Bulk API: 150/minute (across cluster)
```

This sample output is from three-node Cisco SD-WAN Manager cluster with the bulk API rate limit per node configured to 50 requests per minute. Therefore, the bulk API rate limit for the cluster is 50*3 = 150 requests per minute.



CHAPTER 4

# Configure System Logging

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 18: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Ability to Send Syslog Messages over TLS | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | This feature allows you to transport syslog messages to external configured hosts by establishing a Transport Layer Security (TLS) connection. Using the TLS protocol enables the content of syslog messages to remain confidential, secure, and untampered or unaltered during each hop. |
| Remote Logging Over TCP and TLS in Cisco Catalyst SD-WAN Control Components | Cisco Catalyst SD-WAN Control Components Release 20.13.1 | The feature allows remote logging of syslog messages through TCP and TLS. This feature is now available on Cisco Catalyst SD-WAN Control Components (Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Manager) in addition to Cisco IOS XE Catalyst SD-WAN devices. |


- System Logging, on page 44
- Syslog Message Format, Syslog Message Levels, and System Log Files, on page 44
- Benefits of Using TLS for Sending Syslog Messages, on page 48
- Configure Logging in Server Authentication for TLS, on page 48
- Configure Logging in Mutual Authentication for TLS, on page 48
- Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication , on page 49

- Install Root Certificate Authority on Syslog Server for Server Authentication, on page 51
- Install Syslog Root Certificate on Cisco IOS XE Catalyst SD-WAN Device for Mutual Authentication, on page 51
- Configure Logging Feature Template Using Cisco SD-WAN Manager, on page 52
- Generate Feature Certificate Signing Request and Install Feature Certificates, on page 58
- Verify Trustpoint Configuration on Cisco IOS XE Catalyst SD-WAN Device, on page 59
- Export Cisco SD-WAN Manager NMS Audit Log to Syslog Server, on page 60
- Remote Logging Over TCP and TLS in Cisco Catalyst SD- WAN Control Components, on page 62


# System Logging

System logging operations use a mechanism similar to the UNIX syslog command to record system-wide, high-level operations that occur on Cisco Catalyst SD-WAN devices in the overlay network. The log levels (priorities) of the messages are the same as standard UNIX commands, and you can configure the priority of syslog messages. Cisco Catalyst SD-WAN devices can send log messages to a UNIX-style syslog service.

Cisco IOS XE Catalyst SD-WAN devices send syslog messages to syslog servers on configured external hosts using TCP and UDP. When these devices are sending the syslog messages, the messages might transit several hops to reach the output destination. The intermediate networks during the hops might not be trustworthy, be in a different domain, or have a different security level. Therefore, Cisco IOS XE Catalyst SD-WAN devices now support sending secure syslog messages over the Transport Layer Security (TLS) as per RFC5425. To secure the syslog message content from potential tampering, the TLS protocol is used for certificate exchange, mutual authentication, and ciphers negotiation.

Cisco IOS XE Catalyst SD-WAN devices supports both mutual and server authentication for sending syslog messages over TLS.

# Syslog Message Format, Syslog Message Levels, and System Log Files

### Syslog Message Format

Syslog messages begin with a percent sign (%) and following are the syslog message formats:

- Syslog message format

  *seq no:timestamp: %facility-severity-MENEMONIC:description (hostname-n)*
- Syslog message format based on RFC5424

  *<pri>ver timestamp hostname appname procid msgid structured data description/msg*

**Note** In the syslog message format based on RFC5424, the optional fields such as, hostname, appname, procId, msgId, structured data are specified with a -.

The field descriptions of syslog messages are:

*Table 19: Field Descriptions of Syslog Message Format*

| Field | Description |
|---|---|
| facility | Sets the logging facility to a value other than 20, which UNIX systems expect. |
| severity | The importance or severity of the message is categorized by the numerical code from 0 through 7. A lower number in this range indicates greater severity of the system condition. |
| msg or description | A text string that describes the condition of syslog server. This portion of the syslog message sometimes includes IP addresses, interface names, port numbers, or usernames.<br>In syslog message formats based on RFC5424, the description represents: *%facility-severity-MENEMONIC:description* |

Usually, the syslog messages are preceded by extra text.

- The following is an example of a system logging message preceded by a priority value, sequence number, and time stamp:

  *<45>10: polaris-user1: *Jun 21 10:76:84.100: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down*
- Based on RFC5424, the following is an example of a system logging message preceded by a priority value, version of syslog protocol specification, and time stamp:

  *<45>1 2003-10-11T22:14:15.003Z 10.64.48.125 polaris-user1 - - - %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down*

**Note** The time stamp formats are not the same in both the syslog message formats. In the message format based on RFC5424, T, and Z are mandatory where T represents a separator and Z represents zero timezone.

### Syslog Message Levels

All syslog messages are associated with priority levels that indicate the severity of syslog messages to save. The default priority value is "informational", so by default, all syslog messages are recorded. The priority level can be one of the following in order of decreasing severity:

- Emergency—System is unusable (corresponds to syslog severity 0).
- Alert—Ensure that you act immediately (corresponds to syslog severity 1).
- Critical—A serious condition (corresponds to syslog severity 2).
- Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3).
- Warning—A minor error condition (corresponds to syslog severity 4).
- Notice—A normal, but significant condition (corresponds to syslog severity 5).

- Informational—Routine condition (the default) (corresponds to syslog severity 6).
- Debug—Issues debug messages that correspond to syslog severity 7.

### System Log Files

All syslog messages that are at or above the default or configured priority value are recorded in a number of files in the `/var/log` directory on the local device of the syslog server. The following are the contents of the log files:

- auth.log—Login, logout, and superuser access events, and usage of authorization systems
- kern.log—Kernel messages
- messages.log—Consolidated log file that contains syslog messages from all sources.
- vconfd.log—All configuration-related syslog messages
- vdebug.log—All debug messages for modules whose debugging is turned on and all syslog messages that are above the default priority value. The debug log messages support various levels of logging based on the module. The different modules implement the logging levels differently. For example, the system manager (sysmgr) has two logging levels (on and off), while the chassis manager (chmgr) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. Therefore, to enable debugging, use the **debug** operational command.
- vsyslog.log—All syslog messages from Cisco Catalyst SD-WAN processes (daemons) that are above the configured priority value. The default priority value is "informational", so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages are saved.
- vmanage-syslog.log—Cisco SD-WAN Manager NMS Audit log messages

The following are the standard LINUX files that Cisco Catalyst SD-WAN does not use and are available in the `/var/log` directory.

- cron.log
- debug.log
- lpr.log
- mail.log
- syslog

The messages sent to syslog files are not rate-limited and consequently:

- A storage limit of 10 log files with a capacity of up to 16 MB size is set for each syslog file.
  - When the storage capacity exceeds the 16 MB size limit, the log file is saved as a .GZ file along with the date appended to it.
  - When the storage limit exceeds 10 log files, the oldest log file is dropped.
- If many syslog messages are generated in a short span of time, the overflowing messages are buffered and queued to be stored in the syslog file.

For repeating syslog messages or identical messages that occur multiple times in succession, only one copy of the message is placed in the syslog file. The message is annotated to indicate the number of times the message occurred.

The maximum length of a log message is 1024 bytes. The longer messages are truncated.

The maximum length of a log message for Cisco SD-WAN Manager NMS audit logs is 1024 bytes. The longer messages are truncated into smaller fragments and each of these fragments are indicated by an identifier. The identifiers are, fragment 1/2, fragment 2/2, and so on. For example, a long audit log message when truncated into smaller fragments appears as:

```
local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-1/2: {"logid":
"d9ed576a-43ae-49ce-921b-a51c1ed40698", "entry_time":
1576605512190, "statcycletime" 34542398334245, "logmodule":"maintenance", "logfeature":
"upgrade", "loguser": "admin", "logusersrcip":
"10.0.1.1", "logmessage": "Device validation Upgrade to version — Validation success",
"logdeviceid":"Validation", "auditdetails" :
["[18-Oct-2020 17:42:08 UTC] Published messages to vmanage(s)", "auditdetails":["[18-Oct-2020
 17:42:07 UTC] Software image: vmanage-99.99.999-
x86_64.tar.gz", "Software image download may take up to 60}
```

```
local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-2/2: { minutes", "logprocessid":
 "software_install-7de0ec44-d290-4429-b24532435324", "tenant":, "default"}
```

The syslog messages related to AAA authentication and Netconf CLI access and usage are placed in the auth.log and messages.log files. Each time a Cisco SD-WAN Manager NMS logs into a router to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. So, over time, these messages can fill the log files. To prevent these messages from filling the log files, you can disable the logging of AAA and Netconf syslog messages by using the following commands from Cisco SD-WAN Manager NMS:

**Note** For information about available syslog messages on Cisco SD-WAN Manager, see Syslog Messages.

### Disable logging of AAA and Netconf Syslog Messages

1. `vManage# config`

   Enters the configuration mode terminal

2. `vManage(config)# system aaa logs`

   Configures the logging of AAA and Netconf system logging (syslog) messages

3. `vManage(config-logs)# audit-disable`

   Disable logging of AAA events

4. `vManage(config-logs)# netconf-disable`

   Disable logging of Netconf events

5. `vManage(config-logs)# commit`

   Commit complete.

# Benefits of Using TLS for Sending Syslog Messages

The benefits of using TLS for sending syslog messages are:

- Confidentiality of message content where each TLS session begins with a handshake between the Cisco IOS XE Catalyst SD-WAN device and the syslog server. The Cisco IOS XE Catalyst SD-WAN device and syslog server agree on the specific security key and the encryption algorithms to be used for that session. The TLS session opposes any disclosure of the contents of the syslog message.
- Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.
- Mutual authentication between the Cisco IOS XE Catalyst SD-WAN device and syslog server ensures that the syslog server accepts log messages only from authorized clients through certificate exchange.

# Configure Logging in Server Authentication for TLS

In server authentication, Cisco IOS XE Catalyst SD-WAN devices verify the identity of the syslog server. If the syslog server and the certificate are legitimate entities, the device establishes a TLS connection with the server. For implementing server authentication, the syslog server shares the public certificate with the Cisco IOS XE Catalyst SD-WAN devices.

**Prerequisite**

Ensure that Cisco IOS XE Catalyst SD-WAN devices have preinstalled Root Certificate Authority (CA), which you configure using cryptographic module CLIs. See Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication .

To configure TLS profile for syslog server, perform the following steps:

1. Configure Logging Feature Template Using Cisco SD-WAN Manager.
   a. Configure Logging Attributes to Local Disk.
   b. Configure Logging to Remote Severs.
2. Create a device template from logging feature template.

# Configure Logging in Mutual Authentication for TLS

In mutual authentication, both the syslog server and Cisco IOS XE Catalyst SD-WAN device authenticate each other at the same time. Cisco IOS XE Catalyst SD-WAN devices must have root or identity certificates for mutual authentication of the TLS session. To configure TLS profile for syslog server, perform the following steps:

1. Install Syslog Root Certificate on Cisco IOS XE Catalyst SD-WAN Device for Mutual Authentication.
2. Configure Logging Feature Template Using Cisco SD-WAN Manager.
   a. Configure Logging Attributes to Local Disk.

b. Generate Feature Certificate Signing Request and Install Feature Certificates, on page 58

c. Configure Logging to Remote Severs.

3. Create a device template from logging feature template.
4. Generate Feature Certificate Signing Request and Install Feature Certificates, on page 58.
5. Verify Trustpoint Configuration on Cisco IOS XE Catalyst SD-WAN Device.

# Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication

**Before you begin**

Ensure that you generate the encoded CA certificate on the syslog server. See Install Root Certificate Authority on Syslog Server for Server Authentication, on page 51.

**Step 1** To configure PKI trustpoint for Certificate Authority, use these commands for authorizing and revocation of certificates in PKI.

a) **enable**

Enables privileged EXEC mode.

**Example:**

```
Cisco XE SD-WAN> enable
```

b) **config-transaction**

Enters the configuration mode.

**Example:**

```
Cisco XE SD-WAN# config-transaction
```

c) **crypto pki trustpoint** *name*

Declares the trustpoint and a given name and enters CA-trustpoint configuration mode.

**Example:**

```
Cisco XE SD-WAN  (config)# crypto pki trustpoint Syslog-signing-CA
```

d) **enrollment [mode] [retry period** *minutes*] [**retry count** *number*] **url** url [**pem**]

Specifies the enrollment parameters of the CA.

**Example:**

```
Cisco XE SD-WAN(ca-trustpoint)# enrollment terminal
```

e) **chain-validation [{stop | continue}[parent-trustpoint]]**

Configures the level to which a certificate chain is processed on all certificates.

**Example:**

```
Cisco XE SD-WAN(ca-trustpoint)# chain-validation stop
```

f) **revocation-check method**

(Optional) Checks the revocation status of a certificate.

**Example:**

```
Cisco XE SD-WAN(ca-trustpoint)# revocation-check none
```

g) **exit**

Returns to global configuration mode.

**Example:**

```
Cisco XE SD-WAN(ca-trustpoint)# exit
```

**Step 2** Retrieve and authenticate the Root CA before the Cisco IOS XE Catalyst SD-WAN device can be issued a certificate and certificate enrollment occurs.

To authenticate the CA, use the **crypto pki authenticate** command.

**Example:**

```
Cisco XE SD-WAN(config)# crypto pki authenticate root
```

**Step 3** Copy the block of text containing the base 64 encoded CA certificate and paste it at the prompt.

To generate and copy the text containing the encoded CA certificate, see Install Root Certificate Authority on Syslog Server for Server Authentication, on page 51.

**Example:**

A sample base 64 encoded CA certificate:

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswCQYD
VQQGEwJJTjESMBAGA1UECAwJS2FybmF0YWthMRIwEAYDVQQHDAlCYW5nYWxvcmUx
DjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANDU0cxGzAZBgNVBAMMEmVtYmQtbG54
LmNpc2NvLmNvbTEdMBsGCSqGSIb3DQEJARYOYW5idkBjaXNjby5jb20wHhcNMTkw
OTIwMTQ1NjAxWhcNMjIwOTE5MTQ1NjAxWjCBjzELMAkGA1UEBhMCSU4xEjAQBgNV
BAgMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMQ4wDAYDVQQKDAVDaXNj
bzEMMAoGA1UECwwDQ1NHMRswGQYDVQQDDBJlbWJkLWxueC5jaXNjby5jb20xHTAb
BgkqhkiG9w0BCQEWDmFuYnZAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuof+Dh8EdAQ7bHJPdnXhy9ibTLAQ+OpQrMBoOqeAsU/Jru8y
3ht2Eqci35aNjlDcsTUlZyUHBNAMtL69t1HxTRVCOghOZmipzOS+q8rFykHa+bcA
FqmHyqxNwdQcW3cQFZ6rvWTFD9O46ONX3xewpdCR+s+0KFOHDd+RxpAb2NyDWIvn
/1/xwq2a4ZlwgM2d0G8sit0i0D/+6FbZuJjAf+PRTypo4IJyQjcOHpZuslLzPztM
HxLI7pOmR+8+WcInT0l0dyGdpKKHXi6lEbeiyubIym0z0Des5OckDYFejXgXpJDx
9jCVkz+r0bijqbT5PMpSAYYcjdnQ0kdH43sykwIDAQABo1MwUTAdBgNVHQ4EFgQU
OcOmN72TyBqD/Ud2qBLUwId1Yv0wHwYDVR0jBBgwFoAUOcOmN72TyBqD/Ud2qBLU
wId1Yv0wDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAUVVWJHWo
rKxfFV2w7jR7mLZSlVtEvZueMXWPvyYP+Qt09MrRqwNDUJEvggTxU7lvLwtnITPM
l/dOmpoer8GhDtnxUnjsVeVWGIR74SJCS0GU/03bEJ2sto/eAJEOzI7wDg7Fubgy
Pc3RHbk4JWTWs4JF8+E64p2UzJMuu0eLDPQWxl7p2wd3sr4DBHB3qlfbg31T3VHr
PCcuzJmOEdeZYGL1/LFvPx7NZS8lwFAohe6h8ptm3ENg7dzIeyZFZVfcq11Q1rer
+3RcM0VqjScIOZhp97dqfBlHEdqUE/QfKlBt12KU+0sj8yJJC+cuKlHQj5JGmGLI
Y6r7bMcn99Y6Rw==
-----END CERTIFICATE-----
```

**Step 4** Type **yes** to confirm the acceptance of the certificate.

---

The Root CA certificate is successfully imported.

### What to do next

Configure Logging Feature Template Using Cisco SD-WAN Manager, on page 52

# Install Root Certificate Authority on Syslog Server for Server Authentication

In this document, the following steps describe the procedure to set up syslog-ng server that supports TLS.

**Step 1** To install syslog-ng on the server, use the following command:

**Example:**

```
# apt-get install syslog-ng openssl
```

**Step 2** To change the directory to syslog-ng folder and create folders to store the root certificates, use the following commands:

**Example:**

```
# cd /etc/syslog-ng
# mkdir cert.d
# mkdir key.d
# mkdir ca.d
# cd cert.d
# openssl req -new -x509 -out cacert.pem -days 1095 -nodes
# mv privkey.pem ../key.d
```

After using the **openssl** command, an encoded root certificate is available in `cacert.pem` file. The file is located in the `cd/etc/syslog-ng/cert.d` directory.

**Step 3** Copy the content from the `cacert.pem` file when installing root certificate on Cisco IOS XE Catalyst SD-WAN Device. See Step 3 of Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication , on page 49.

### What to do next

Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication , on page 49

# Install Syslog Root Certificate on Cisco IOS XE Catalyst SD-WAN Device for Mutual Authentication

To configure Cisco IOS XE Catalyst SD-WAN devices with Transport Layer Security (TLS) syslog protocol, the devices must have root or identity certificates for mutual authentication of TLS session. You can either use a third-party Certificate Authority (CA) to get public key infrastructure (PKI) services, or Microsoft Active Directory Certificate Services (AD CS). AD CS allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your requirement.

**Step 1** Generate the enterprise root certificate using a third party CA or Microsoft Active Directory Certificate Services.

**Step 2** Download the root CA in base 64 format, select and copy the content of root CA.

**Step 3** From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

**Step 4** Click **Enterprise Feature Certificate Authorization**.

**Step 5** Paste the root CA content in the **Enterprise Root Certificate** box.

**Step 6** (Optional) if you want to generate a Certificate Signing Request (CSR), check the **Set CSR Properties** check box.

**Step 7** Click **Close**.

The root CA is uploaded to Cisco SD-WAN Manager, and Cisco SD-WAN Manager saves the root certificate to the Cisco IOS XE Catalyst SD-WAN device.

### What to do next

Configure Logging Feature Template Using Cisco SD-WAN Manager, on page 52

# Configure Logging Feature Template Using Cisco SD-WAN Manager

On Cisco IOS XE Catalyst SD-WAN device , you can log event notification system log (syslog) messages to files on the local device, or you can log them to files on a remote host using Cisco SD-WAN Manager.

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

**Step 2** Click **Feature Templates**, and click **Add Template**.

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

**Step 3** From **Select Devices**, choose the device for which you wish to create a template.

**Step 4** To create a template for logging, select **Cisco Logging**.

The Cisco Logging template form appears. This form contains fields for naming the template, and fields for defining the Logging parameters. Click a tab or the plus sign (+) to display other fields.

When you first open a feature template, the scope is set to **Default** for those parameters that have a default value. The default setting or value appears next to a parameter. To change the default or to enter a value, click the **Scope** drop-down list to the left of the parameter field.

**Step 5** In **Template Name**, enter a name for the template.

The name may contain up to 128 alphanumeric characters.

**Step 6** In **Template Description**, enter a description of the template.

The description may contain up to 2048 alphanumeric characters.

### What to do next

Configure Logging Attributes to Local Disk, on page 52

# Configure Logging Attributes to Local Disk

1. Click **Disk** and configure the following parameters:

*Table 20: Parameter Information*

| Parameter | Description |
|---|---|
| Enable Disk | To save syslog messages in a file on the local hard disk, click **On** or **Off** to disallow saving. By default, logging to a local disk file is enabled on all devices. |
| Maximum File Size | Enter the maximum size of syslog files. The syslog files are rotated on an hourly basis based on the file size. When the file size exceeds configured value, the file is rotated and the *syslogd* process is notified.<br>Range: 1-20 MB<br>Default: 10 MB |
| Rotations | Enter the number of syslog files to create before discarding the earliest created files.<br>Range: 1-10 MB<br>Default: 10 MB |

2. To save the feature template, click **Save**.
3. To associate the feature template with a device template, see Create a Device Template from Feature Templates.

**What to Do Next**

Configure TLS Profile for Server Authentication, on page 53 or Configure TLS Profile for Mutual Authentication, on page 55

# Configure TLS Profile for Server Authentication

1. Click **TLS Profile**.
2. Click **New Profile**, and configure the following parameters:

*Table 21: Parameter Information*

| Parameter Name | Description |
|---|---|
| Profile Name | Enter the TLS profile name |
| TLS Version | Choose TLS versions v1.1 or v1.2 |
| Authentication Type | Choose authentication types as **Server**. |

| Parameter Name | Description |
|---|---|
| Ciphersuites | Choose groups of cipher suites (encryption algorithm) based on the TLS version.<br>The following are the list of cipher suites.<br>• aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha<br>• aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha<br>• dhe-aes-128-cbc-sha Encryption type tls_dhe_rsa_with_aes_128_cbc_sha<br>• dhe-aes-cbc-sha2 Encryption typetls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)<br>• dhe-aes-gcm-sha2 Encryption typetls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)<br>• ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2(TLS1.2 & above) SuiteB<br>• ecdhe-rsa-aes-128-cbc-sha Encryption type tls_ecdhe_rsa_with_aes_128_cbc_sha<br>• ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2& above)<br>• ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2& above)<br>• rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)<br>• rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above) |

You can use the following cipher suites for each TLS version:

*TLS v1.1*

```
aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha
```

*TLS v1.2 and later*

```
dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)

ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
```

```
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)

rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

The TLS profiles appear in a table.

3. To create another profile, click **Add**.
4. To edit or delete a TLS profile information, click or under **Action**.
5. To save the feature template, click **Save**.
6. To associate the feature template with a device template, see Create a Device Template from Feature Templates.

When you choose the authentication type as **Server**, all information about TLS profiles, except the trustpoint information, is saved.

**What to Do Next**

Configure Logging to Remote Severs, on page 57

# Configure TLS Profile for Mutual Authentication

1. Click **TLS Profile**.
2. Click **New Profile**, and configure the following parameters:

***Table 22: Parameter Information***

| Parameter Name | Description |
|---|---|
| Profile Name | Enter the TLS profile name |
| TLS Version | Choose TLS versions v1.1 or v1.2 |
| Authentication Type | Choose authentication types as **Mutual**. |

| Parameter Name | Description |
|---|---|
| Ciphersuites | Choose groups of cipher suites (encryption algorithm) based on the TLS version that must be used for encryption.<br>The following are the list of cipher suites.<br>• aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha<br>• aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha<br>• dhe-aes-128-cbc-sha Encryption type tls_dhe_rsa_with_aes_128_cbc_sha<br>• dhe-aes-cbc-sha2 Encryption typetls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)<br>• dhe-aes-gcm-sha2 Encryption typetls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)<br>• ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2(TLS1.2 & above) SuiteB<br>• ecdhe-rsa-aes-128-cbc-sha Encryption type tls_ecdhe_rsa_with_aes_128_cbc_sha<br>• ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2& above)<br>• ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2& above)<br>• rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)<br>• rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above) |

You can use the following cipher suites for each TLS version:

*TLS v1.1*

```
aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha
```

*TLS v1.2 and later*

```
dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

```
ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)

rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

The TLS profiles appear in a table.

3. To create another profile, click **Add**.
4. To edit or delete a TLS profile information, click or under **Action**.
5. To save the feature template, click **Save**.
6. Associate the feature template with a device template. See Create a Device Template from Feature Templates.

The mutually authenticated feature template is saved on the Cisco IOS XE Catalyst SD-WAN devices, and trustpoint such as, SYSLOG-SIGNING-CA certificate is saved on the device. Cisco SD-WAN Manager can now install the certificate from Cisco IOS XE Catalyst SD-WAN devices.

**What to Do Next**

Configure Logging to Remote Severs, on page 57

# Configure Logging to Remote Severs

To include the TLS profile in IPV6 or IPV4 server configuration and configure logging of event notification system log messages to a remote server,

1. Click **Server**.
2. Click **Add New Server**, and configure the following parameters for IPv4 or IPv6:

***Table 23: Parameter Information***

| Parameter Name | Description |
|---|---|
| Hostname/IP Address | Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages.<br>To add another syslog server, click +.<br>To delete a syslog server, click . |
| VPN ID | Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached.<br>VPN ID Range: 0-65530 |

| Parameter Name | Description |
|---|---|
| Source Interface | Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration of syslog servers is ignored. If you configure multiple syslog servers, the source interface must be same for all of them. |
| Priority | Choose a severity of the syslog message to be saved. The severity indicates the seriousness of the event that generated the syslog message. See Syslog Message Levels. |
| TLS | For Cisco IOS XE Catalyst SD-WAN devices, click **On** to enable syslog over TLS. |
| Custom Profile | For Cisco IOS XE Catalyst SD-WAN devices, click **On** to enable choosing a TLS profile, or click **Off** to disable choosing a TLS profile. |
| TLS Profile | For Cisco IOS XE Catalyst SD-WAN devices, choose a TLS profile that you have created for server or mutual authentication in IPv4 or IPv6 server configuration. |

The server entries appear in a table.

3. To create another entry for a server, click **Add**.
4. To edit a logging server, click .
5. To remove a logging server, click .
6. To save the feature template, click **Save**.
7. To associate the feature template with a device template, see Create a Device Template from Feature Templates.

# Generate Feature Certificate Signing Request and Install Feature Certificates

To validate and authenticate Cisco IOS XE Catalyst SD-WAN devices and syslog server, perform the following operation on the Cisco SD-WAN Manager Certificates screen. See Cisco Catalyst SD-WAN Getting Started Guide for information about enterprise certificates.

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

**Step 2** From **Certificates**, choose a Cisco IOS XE Catalyst SD-WAN device.

a) Generate Feature Certificate Signing Request (CSR).

After you generate the Feature CSR, the **View Feature CSR** and **Install Feature certificate** options are available.

b) View Feature CSR.

c) To download the feature CSR, click **Download**.

**Step 3** To sign the certificate, send the certificate to a third-party signing authority.

**Step 4** To import the certificate into Cisco IOS XE Catalyst SD-WAN devices, Install feature certificate.

The Install Feature Certificate screen uses the signed certificate and installs it on Cisco IOS XE Catalyst SD-WAN devices.

---

After the feature certificate installation is successful, the Revoke Feature Certificate and View Feature Certificate options are available on Cisco SD-WAN Manager.

### What to do next

Verify Trustpoint Configuration on Cisco IOS XE Catalyst SD-WAN Device, on page 59

# Verify Trustpoint Configuration on Cisco IOS XE Catalyst SD-WAN Device

To display the contents of syslog file with trustpoint information for Cisco IOS XE Catalyst SD-WAN device, use the **show crypto pki trustpoints status** command.

### Examples

Server authentication

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

Mutual authentication

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  rsakeypair SYSLOG-SIGNING-CA 2048
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

Verify trustpoints on a device for a Syslog-signing-CA certificate

```
Cisco XE SD-WAN# show crypto pki trustpoints SYSLOG-SIGNING-CA status
```

```
Trustpoint SYSLOG-SIGNING-CA:

 Issuing CA certificate not configured.

State:

Keys generated ..... No

 Issuing CA authenticated ..... No

  Certificate request(s) ..... None
```

# Export Cisco SD-WAN Manager NMS Audit Log to Syslog Server

*Table 24: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Export Cisco SD-WAN Manager Audit Log as Syslog | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | The Cisco SD-WAN Manager exports audit logs in syslog message format to a configured external syslog server. This feature allows you to consolidate and store network activity logs in a central location. |

On Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices, you can log event notification system log (syslog) messages to files on a local device, or to files on a remote host using CLI. These event notification logs are converted to system log files and exported to the syslog server. You can then retrieve system log information from the syslog server.

# Configure System Logging Using CLI

## Log Syslog Messages to a Local Device

By default, a priority level of "information" is enabled when you log syslog messages to a file on a local device. Use the following commands:

1. **logging disk**

   Logs syslog messages on a hard disk

   **Example:**

   ```
   vm01(config-system)# logging disk
   ```

2. **enable**

   Enables logging to a disk

   **Example:**

   ```
   vm01(config-logging-disk)# enable
   ```

3. **file size** *size*

Specifies the size of syslog files in megabytes (MB) By default, the syslog files are 10 MB. You can configure the size of syslog files to be 1–20 MB.

**Example:**

```
vm01(config-logging-disk)# file size 3
```

4. **file rotate** *number*

   Rotates syslog files on an hourly basis based on the size of the file By default, 10 syslog files are created. You can configure the rotate command to be a number from 1 through 10.

   **Example:**

   ```
   vm01(config-logging-disk)# file rotate 3
   ```

For more information about logging disk commands, see the logging disk command.

## Log Syslog Messages to a Remote Device

To log event notification system log (syslog) messages to a remote host, use the following commands:

1. **logging server**

   Logs syslog messages to a remote host or syslog server You can configure the name of the server by DNS name, hostname, or IP address. You can configure up to four syslog servers.

   **Example:**

   ```
   vm01(config-system)# logging server 192.168.0.1
   ```

2. (Optional) **vpn** *vpn-id*

   Specifies the VPN ID of the syslog server

3. (Optional) **source interface** *interface-name*

   Specifies the source interface to reach the syslog server. The interface name can be a physical interface or a sub-interface (a VLAN-tagged interface). Ensure that the interface is located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

   **Example:**

   ```
   vm01(config-server-192.168.0.1)# source interface eth0
   ```

4. **priority** *priority*

   Specifies the severity of the syslog message to be saved. The default priority value is "informational" and by default, all syslog messages are recorded.

   **Example:**

   In the following example, set the syslog priority to log alert conditions.

   ```
   vm01(config-server-192.168.0.1)# priority alert
   ```

If the syslog server is unreachable, the system suspends sending syslog messages for 180 seconds. When the server becomes reachable, logging resumes. For more information about logging server commands, see the logging server command.

## View System Logging Information

To view system log settings after logging syslog messages to a remote host, use the **show logging** command. For example:

```
vm01(config-server-192.168.0.1)# show logging

System logging
    server 192.168.0.1
    source interface eth0
    exit
!
!
```

To view the contents of the syslog file, use the **show log** command. For example:

```
vm01(config-server-192.168.0.1)# show log nms/vmanage-syslog.log tail 10
```

To view the configured system logging settings from Cisco SD-WAN Manager, see Audit Log.

To view device-specific syslog files from Cisco SD-WAN Manager, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**, and ensure that you enable **Data Stream**.
2. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a Cisco IOS XE Catalyst SD-WAN device

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**, and choose a Cisco IOS XE Catalyst SD-WAN device.
3. Click **Troubleshooting**.
4. From **Logs**, click **Debug Log**.
5. From **Log Files**, select a name of the log file to view the log information.

# Remote Logging Over TCP and TLS in Cisco Catalyst SD- WAN Control Components

## Information About Remote Logging Over TCP and TLS

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, support for remote logging of syslog messages has been enhanced to include TCP and TLS transport methods in addition to UDP. This enhancement applies to Cisco Catalyst SD-WAN Control Components including Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Manager.

By default, UDP is enabled as the default transport type for remote logging. However, users now have the additional option to select either TCP or TLS as their transport method for remote logging.

For more information, see System Logging, on page 44

# Benefits of Remote Logging Over TCP and TLS

- Syslog over TCP and TLS supports large-scale network environments. While TCP can handle large volumes of data, TLS can ensure that the log data is securely sent and protected from unauthorized access or tampering.
- You can configure up to four separate remote syslog servers with the option to assign each server a unique transport protocol such as UDP, TLS, or TCP. Alternatively, you can choose to use the same transport protocol for all four servers.
- For remote logging over TLS, a TLS profile supports TLS version 1.2. Also, various cipher suites can be accommodated within the TLS profile, depending on the TLS version.

# Configure Remote Logging Over TCP and TLS

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.
4. In the left pane, from **Select Devices**, choose a a Cisco Catalyst SD-WAN control component.
5. Under **OTHER TEMPLATES**, click **Logging** 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. Configure Logging Attributes to Local Disk.
   a. Click **Disk** and configure the following parameters:

   ***Table 25: Parameter Information***

| Parameter | Description |
|---|---|
| Enable Disk | To save syslog messages in a file on the local hard disk, click **On** or **Off** to disallow saving. By default, logging to a local disk file is enabled on all devices. |
| Maximum File Size | Enter the maximum size of syslog files. The syslog files are rotated on an hourly basis based on the file size. When the file size exceeds the configured value, the file is rotated and the *syslogd* process is notified.<br>Range: 1 to 20 MB<br>Default: 10 MB |

| Parameter | Description |
|---|---|
| Rotations | Enter the number of syslog files to create before discarding the earliest created files.<br>Range: 1 to 10 MB<br>Default: 10 MB |

b. To save the feature template, click **Save**.

c. To associate the feature template with a device template, see Create a Device Template from Feature Templates.

## Configure TLS Profile for Server Authentication

1. From the **TLS Profile** section, click **New Profile** to configure a TLS profile.

*Table 26: TLS Profile Parameters*

| Parameter Name | Description |
|---|---|
| Profile Name | Enter the TLS profile name |
| TLS Version | Choose TLS v1.2. |

| Parameter Name | Description |
|---|---|
| Ciphersuites | Choose one or more ciphersuites based on the TLS version.<br>The following ciphersuites are supported:<br>• ECDHE-ECDSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES256-GCM-SHA384<br>• DHE-RSA-AES256-GCM-SHA384<br>• ECDHE-ECDSA-AES128-GCM-SHA256<br>• ECDHE-RSA-AES128-GCM-SHA256<br>• DHE-RSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES256-SHA384<br>• ECDHE-RSA-AES256-SHA384<br>• DHE-RSA-AES256-SHA256<br>• ECDHE-ECDSA-AES128-SHA256<br>• ECDHE-RSA-AES128-SHA256<br>• DHE-RSA-AES128-SHA256<br>• RSA-PSK-AES256-GCM-SHA384<br>• DHE-PSK-AES256-GCM-SHA384<br>• AES256-GCM-SHA384<br>• PSK-AES256-GCM-SHA384<br>• RSA-PSK-AES128-GCM-SHA256<br>• DHE-PSK-AES128-GCM-SHA256<br>• AES128-GCM-SHA256<br>• PSK-AES128-GCM-SHA256<br>• AES256-SHA256<br>• AES128-SHA256 |

2. (Optional) Click **Add** to create another profile.

## Configure Syslog Servers for TLS/TCP/UDP

1. From the **Server** section, click **New Server** to configure syslog servers.

*Table 27: Syslog Servers Parameters*

| Parameter Name | Description |
|---|---|
| Hostname/IP Address | Enter the DNS name, hostname, IPv4 or IPv6 address of the server on which to store syslog messages.<br>To add another syslog server and its details, click **Add**. |
| VPN ID | Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached.<br>Range is 0 to 65530 |
| Source Interface | Enter the specific interface to use for outgoing system log messages. |
| Priority | Choose a logging level for syslog messages that you want to log on the server. The logging level indicates the type of event that generated the syslog message. See Syslog Message Levels. |
| Transport for messages logged to remote host | Choose either TCP, UDP, or TLS as the transport type for forwarding syslog messages to a remote server. |
| Port for transport (default 514) | Specify the port number for the transport type. |
| TLS Profile | This field displays if you have chosen the transport type as TLS. Choose a TLS profile to attach a TLS profile. See Configure TLS Profile for Server Authentication, on page 64 |

2. (Optional) Click **Add** to create another entry for a server.
3. Click **Save** to save the feature template

## Apply the Logging Feature Template to a Device

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.
3. From the **Create Template** drop-down list, choose **From Feature Template**
4. From the **Device Model** drop-down list, choose one of the devices.
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 device template.

This field is mandatory, and it can contain all characters and spaces.

7. From the **Cisco Logging** drop-down list, choose the template that you created for remote logging.
8. Click **Create** to apply the template to a device.
9. From the list of device templates, click **…** next to the device template that you created.
10. Click **Attach Devices**.
11. Choose the devices to which you want to attach the device template.
12. Click **Attach** to the template to the devices.

# Configure Remote Logging Over TCP and TLS

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

This section provides sample CLI configurations to configure a remote server for logging with transport type as TCP and TLS.

### Configure Remote Server with Transport Type as TCP

Configure Remote Server with Transport Type as TCP.

```
system
 logging
  server <server-ip-address>
  transport tcp port 514
```

### Configure Remote Server with Transport Type as TLS

Configuring a remote server for logging with Transport type as TLS is a three-step process.

1. Manage Certificate

   To manage the Certificate Authority (CA) certificate from the syslog server, use the following commands below to install, list, and uninstall the certificates.

   - Install a Certificate

     A certificate can be installed from either a local directory, such as /home/admin, or remotely using secure copy (scp), HTTP, or FTP.

     ```
     request logging ca-cert
      install new syslog-ng ca
     ```

   - List All Installed Certificates

     ```
     show logging cacert
     ```

   - Uninstall a Certificate

```
request logging ca-cert uninstall <cert-name>
```

2. Create a TLS Profile

   Creating a TLS profile involves specifying the protocols and cipher suites that a device will use for secure communication. You can configure up to four TLS profiles.

   Use the following configuration to create a TLS profile:

```
system
 logging
 tls-profile <profile-name>
  tls-version TLSv1.2
  ciphersuite <ciphersuite1> <ciphersuite2>
```

3. Attach a TLS Profile to a Remote Logging Server

   Use the following configuration to attach a TLS profile to the remote logging servers:

```
server<server-ip-address>
 vpn <vpn-instance-of-logging-server>
 source-interface <interface-num>
 transport tls
 tls-profile <tls-profile-name>
```

# Verify Remote Logging Over TCP and TLS

The following is a sample output from the **show logging cacert** command to view installed certificates.

```
Device# show logging cacert
INDEX  NAME      VALIDITY
-----------------------------------------
0      cert.pem  Fri Jun 21 20:35:10 2024
```

# Configuration Example for Support for Syslog over TCP and TLS

### Configuration Example for Logging Over TLS

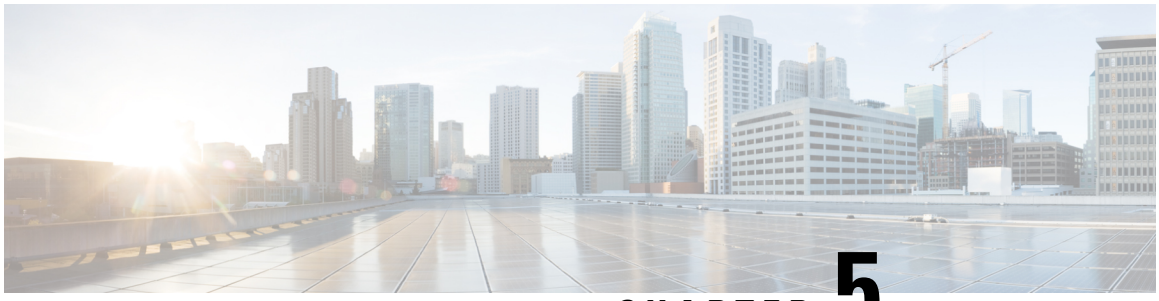
This example shows the configuration for logging over TLS.

```
system
logging
  disk
   enable
  !
  tls-profile profile1
   version     TLSv1.2
   ciphersuite ECDHE-ECDSA-AES128-SHA256 AES256-GCM-SHA384 PSK-AES256-GCM-SHA384
PSK-AES128-GCM-SHA256 AES256-SHA256
  exit
  server 10.0.1.55
   source interface 10.1.1.12
   transport   tls
   tls-profile profile1
  exit
!
!
```

### Configuration Example for Logging Over TCP

This example shows the configuration for logging over TCP.

```
system
logging
  disk
   enable
  !
  server 10.0.1.56
   transport tcp
  exit
!
!
```



CHAPTER 5

# Configure User Access and Authentication

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Use the **Manage Users** screen to add, edit, or delete users and user groups from Cisco SD-WAN Manager.

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.


- Configure Hardened Passwords , on page 72
- Configure User Login Options, on page 75
- Manage Users, on page 80
- Configure Users Using CLI, on page 81
- Manage a User Group, on page 82
- Creating Groups Using CLI, on page 83
- Ciscotac User Access, on page 84
- Configure Sessions in Cisco SD-WAN Manager, on page 85
- Configuring RADIUS Authentication Using CLI, on page 86
- Configure SSH Authentication, on page 88
- Configure the Authentication Order, on page 89
- Role-Based Access with AAA, on page 90
- Configuring AAA using Cisco SD-WAN Manager Template, on page 100
- Configure IEEE 802.1X Authentication, on page 108
- Posture Assessment Support, on page 114
- Type 6 Passwords on Cisco IOS XE SD-WAN Routers, on page 117

# Configure Hardened Passwords

*Table 28: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Hardened Passwords | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | This feature enables password policy rules in Cisco SD-WAN Manager. After password policy rules are enabled, Cisco SD-WAN Manager enforces the use of strong passwords. |
| | Cisco IOS XE Catalyst SD-WAN Release 17.9.1a<br>Cisco vManage Release 20.9.1 | This feature lets you configure Cisco SD-WAN Manager to enforce predefined-medium security or high-security password criteria. |

## 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. IClick **Password Policy**.
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. Click **Save**.

### Password Requirements

Cisco SD-WAN Manager enforces the following password requirements after you have enabled the password policy rules:

- The following password requirements apply to releases before Cisco vManage Release 20.9.1:
  - Must contain a minimum of eight characters, and a maximum of 32 characters.

- Must contain at least one uppercase character.
- Must contain at least one lowercase character.
- Must contain at least one numeric character.
- Must contain at least one of the following special characters: # ? ! @ $ % ^ & * -.
- Must not contain the full name or username of the user.
- Must not reuse a previously used password.
- Must contain different characters in at least four positions in the password.

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

| Password Criteria | Requirements |
|---|---|
| Medium Security | • Must contain a minimum of 8 characters<br>• Must contain no more than 32 characters<br>• Must contain at least 1 lowercase character<br>• Must contain at least 1 uppercase character<br>• Must contain at least 1 numeric character<br>• Must contain at least 1 of the following special characters: # ? ! @ $ % ^ & * -<br>• Must not be identical to any of the last 5 passwords used<br>• Must not contain the full name or username of the user |
| High Security | • Must contain a minimum of 15 characters<br>• Must contain no more than 32 characters<br>• Must contain at least 1 lowercase character<br>• Must contain at least 1 uppercase character<br>• Must contain at least 1 numeric character<br>• Must contain at least 1 of the following special characters: # ? ! @ $ % ^ & * -<br>• Must not be identical to any of the last 5 passwords used<br>• Must not contain the full name or username of the user<br>• Must have at least eight characters that are not in the same position they were in the old password |

## Password Attempts Allowed

You are allowed five consecutive password attempts before your account is locked. After six failed password attempts, you are locked out for 15 minutes. If you enter an incorrect password on the seventh attempt, you are not allowed to log in, and the 15-minute lock timer starts again.

If your account is locked, wait for 15 minutes for the account to automatically be unlocked. Alternatively, reach out to an administrator to reset the password, or have an administrator unlock your account.

**Note** Your account gets locked even if no password is entered multiple times. When you do not enter anything in the password field, it is considered as invalid or wrong password.

## Password Change Policy

**Note** You must have enabled password policy rules first for strong passwords to take effect. For more information, see Enforce Strong Passwords, on page 72.

When resetting your password, you must set a new password. You cannot reset a password using an old password.

**Note** In Cisco vManage Release 20.6.4, Cisco vManage Release 20.9.1 and later releases, a user that is logged out, or a user whose password has been changed locally or on the remote TACACS server cannot log in using their old password. The user can log in only using their new password.

## 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.

## Reset a Locked User Using the CLI

You can reset a locked user using the CLI as follows:

1. Log in to the device as an `admin` user.
2. Run the following command:

   ```
   Device# request aaa unlock-user username
   ```
3. When prompted, enter a new password for the user.

# Configure User Login Options

***Table 29: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Inactivity Lockout | Cisco Catalyst SD-WAN Manager Release 20.12.1 | This feature lets you configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days. |
| Unsuccessful Login Attempts Lockout | Cisco Catalyst SD-WAN Manager Release 20.12.1 | This feature lets you configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period. |
| Duo Multifactor Authentication Support | Cisco Catalyst SD-WAN Manager Release 20.12.1 | This feature lets you configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager. |

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, a netadmin user can enable the following Cisco SD-WAN Manager user login features:

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can access Cisco SD-WAN Manager with basic privileges even if TACACS user is not mapped to a group. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the access to Cisco SD-WAN Manager was denied.

- Inactivity lockout: You can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days. Locked out users cannot log in to Cisco SD-WAN Manager until an administrator unlocks their accounts.

  See Configure Account Lockout , on page 76.

- Unsuccessful login lockout: You can configure Cisco SD-WAN Manager to prevent users who make a designated number of consecutive unsuccessful login attempts within a designated time period from

logging in to Cisco SD-WAN Manager until a configured amount of time passes or an administrator unlocks their user accounts.

By default, Cisco SD-WAN Manager locks out users for 15 minutes after five consecutive unsuccessful login attempts within 15 minutes. After a lockout period expires, a user can log in with the correct user name and password.

See Configure Unsuccessful Login Attempts Lockout, on page 77.

- Duo multifactor authentication: You can configure Cisco SD-WAN Manager to require the use of Duo multifactor authentication to verify identity before users can log in. Users must confirm a login attempt by using Duo multifactor authentication on their mobile devices.

  See Configure Duo Multifactor Authentication, on page 79.

# Configure Account Lockout

### Before You Begin

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.

Cisco SD-WAN Manager marks locked out users as inactive, and they cannot log in again until an administrator unlocks their accounts in Cisco SD-WAN Manager.

**Note** To unlock a user account, see Reset a Locked User.

### Configure Account Lockout

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Account Lockout** and enable the **Inactive days before locked out** option.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x, locate the **Account Lockout**, click **Edit**, and enable **Inactive days before locked out**.)
3. Configure the following options:

| Field | Description |
|---|---|
| **Inactive days before account locked out** | Enable this option and enter the number of consecutive inactive days after which Cisco SD-WAN Manager locks out a user.<br><br>An inactive day is defined as a day on which a user does not log in to Cisco SD-WAN Manager.<br><br>Valid values are 2 through 90. |

| Field | Description |
|---|---|
| **Number of failed login attempts before lockout** | Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user.<br>Possible values: 1 through 3600<br>Default: 3600 |
| **Duration within which the failed attempts are counted (minutes)** | Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts.<br>For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes.<br>Possibe values: 1 through 60<br>Default: 60 |
| **Cooldown or Lockout period** | This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts.<br>This option is enabled by default. If you disable it, an administrator must manually unlocks the account of a locked-out user.<br>**a.** Click **Enabled** adjacent to **Cooldown or Lockout period**.<br>**b.** In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user.<br>Possible values: 1 through 60<br>Default: 15 |

4. Click **Save**.

# Configure Unsuccessful Login Attempts Lockout

### Before You Begin

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

**Note** From Cisco Catalyst SD-WAN Manager Release 20.13.1 or later, use the procedure described in Configure Account Lockout , on page 76.

You can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a period of time.

Cisco SD-WAN Manager prevents locked out users from logging in again until a configured amount of time has passed or an administrator unlocks their accounts in Cisco SD-WAN Manager.

**Note** To unlock a user account, see Reset a Locked User.

### Configure Unsuccessful Login Attempts Lockout

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Account Lockout**
3. In the **Lockout on failed login attempts** row, click **Edit**.
4. Configure the following options:

| Field | Description |
|---|---|
| **Number of failed login attempts before lockout** | Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user.<br>Possible values: 1 through 3600<br>Default: 3600 |
| **Duration within which the failed attempts are counted (minutes)** | Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts.<br>For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes.<br>Possibe values: 1 through 60<br>Default: 60 |

| Field | Description |
|---|---|
| **Cooldown or Lockout period** | This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts.<br>This option is enabled by default. If you disable it, an administrator must manually unlocks the account of a locked-out user.<br>**a.** Click **Enabled** adjacent to **Cooldown or Lockout period**.<br>**b.** In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user.<br>Possible values: 1 through 60<br>Default: 15 |

5. Click **Save**.

# Configure Duo Multifactor Authentication

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager and other controllers. When you configure this feature, users are prompted on their mobile devices to authenticate with Duo after they enter a username and password and click **Log In** on the Cisco SD-WAN Manager **Login** screen.

This feature requires that you have a Duo account with local users created on that account.

**Note**

- Duo MFA does not apply to the admin user by default. To enable Duo MFA for the admin user, enable the**DUO MFA Configuration** option, and then enter the admin-auth-order command from the CLI.
- Users do not see a message in Cisco SD-WAN Manager that an MFA request has been sent to a mobile device.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **DUO MFA Configuration**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.
3. Click **Enabled**.
4. Configure the following options:

| Field | Description |
|---|---|
| **Integration Key** | Enter the integration key (Ikey) for your Duo account. |
| **Secret Key** | Enter the secret key (Skey) for your Duo account. |
| **API Hostname** | Enter the API hostname (api-hostname) for your Duo account. |
| **Server proxy** | (Read only) Shows the server proxy that is used to access the Duo server if Cisco SD-WAN Manager is behind a firewall. Set this server proxy with the **system http proxy** or the **system https proxy** command.<br>**Note** If Cisco SD-WAN Manager is deployed on a cloud that can be reached by an external network, a server proxy should not be set. |

5. Click **Save**.
6. If a Cisco SD-WAN Validator or a Cisco SD-WAN Controller does not have internet access, use the following commands in the CLI or the device template of the device to provide access to the Duo MFA feature.

   These commands configure the device with proxy information about the device on which Duo MFA is enabled.

```
vm# config
vm(config)# system aaa
vm(config-aaa)# multi-factor-auth
vm(config-multi-factor-auth)# duo
vm(config-duo)# api-hostname name
vm(config-duo)# secret-key key
vm(config-duo)# integration-key key
vm(config-duo)# proxy proxy_url
vm(config-duo)# commit
```

# 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 30: 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 |

# Configure Users Using CLI

You can use the CLI to configure user credentials on each device. This way, you can create additional users and give them access to specific devices. The credentials that you create for a user by using the CLI can be different from the Cisco SD-WAN Manager credentials for the user. In addition, you can create different credentials for a user on each device. All Cisco IOS XE Catalyst SD-WAN device users with the **netadmin** privilege can create a new user.

To create a user account, configure the username and password, and place the user in a group:

This example, shows the addition of user, Bob, to an existing group:

```
Device(config)# system aaa user bob group basic
```

This example, shows the addition of user, Alice, to a new group `test-group`:

```
Device(config)# system aaa user test-group
Device(config)# system aaa user alice group test-group
```

The Username can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. Because some usernames are reserved, you cannot configure them. For a list of reserved usernames, see the **aaa** configuration command in the Cisco Catalyst SD-WAN Command Reference Guide.

The Password is the password for a user. Each username must have a password, and users are allowed to change their own password. The CLI immediately encrypts the string and does not display a readable version of the password. When a user logs in to a Cisco IOS XE Catalyst SD-WAN device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and must wait for 15 minutes before attempting to log in again.

**Note** Enclose any user passwords that contain the special character ! in double quotation marks (“ “). If a double quotation is not included for the entire password, the config database (?) treats the special character as a space and ignores the rest of the password.

For example, if the password is C!sc0, use “C!sc0”.

Group name is the name of a standard Cisco Catalyst SD-WAN group (**basic**, **netadmin**, or **operator**) or of a group configured with the **usergroup** command (discussed below). If an admin user changes the permission 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.

The factory-default password for the admin username is admin. We strongly recommend that you modify this password the first time you configure a Cisco IOS XE Catalyst SD-WAN device:

```
Device(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

Configure the password as an ASCII string. The CLI immediately encrypts the string and does not display a readable version of the password, for example:

```
Device# show run | sec username
username admin privilege 15 secret 9
$9$3F2M2l2G2/UM3U$TGe2kqoIibdIRDEj4cOVKbVFP/o4vnlFAwWnmzx1rRE
username appnav privilege 15 secret 9
$9$3l2L2V.F2VIM1k$p3MBAyBtGxKf/yBGnUSHQ1g/ae1QhfIbieg28buJJGI
username eft secret 9 $9$3FMJ3/UD2VEL2E$d.kE4.an41v7wEhrQc6k5wIfE9M9WkNAJxUvbbempS.
username lab privilege 15 secret 9
$9$3l.J3FUD2F.E2.$/AiVn9PmLCpgr6ExVrE7dH979Wu8nbdtAfbzUtfysg.
username test secret 9 $9$1l2J3l6D3/QL3k$7PZOXJAJOI1os5UI763G3XcpVhXlqcwJ.qEmgmx4X9g
username vbonagir privilege 15 secret 9
$9$3/2K2UwF2lQF3U$VbdQ5bq18590rRthF/NnNnOsw.dw1/EViMTFZ5.ctus
Device#
```

If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to verify the password:

```
Device(config)#  radius server tag
```

The tag is a string that you defined with the **radius server tag** command, as described in the Cisco Catalyst SD-WAN Command Reference Guide.

# 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.

# Creating Groups Using CLI

The Cisco Catalyst SD-WAN software provides default user groups: **basic**, **netadmin**, **operator**, **network_operations**, and **security_operations**. The username **admin** is automatically placed in the **netadmin** usergroup.

If needed, you can create additional custom groups and configure privilege roles that the group members have. To create a custom group with specific authorization, configure the group name and privileges:

```
Device(config)# aaa authentication login user1 group radius enable
Device(config)# aaa authentication login user2 group radius enable
Device(config)# aaa authentication login user3 group radius enable
Device(config)#
```

*group-name* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any

uppercase letters Some group names are reserved, so you cannot configure them. For a list of them, see the aaa configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the user group **basic**. If a remote server validates authentication and specifies a user group (say, X) using VSA Cisco SD-WAN-Group-Name, the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

In the **task** option, list the privilege roles that the group members have. The role can be one or more of the following: **interface**, **policy**, **routing**, **security**, and **system**.

# Ciscotac User Access

The Cisco Edge software provides two users—**ciscotacro** and **ciscotacrw**—that are for use only by the Cisco Support team. These users are available for both cloud and on-premises installations. They operate on a consent-token challenge and token response authentication in which a new token is required for every new login session. The ciscotacro and ciscotacrw users can use this token to log in to Cisco SD-WAN Manager web server as well as the SSH Terminal on Cisco SD-WAN Manager. These users can also access Cisco SD-WAN Validator, Cisco SD-WAN Controllers, and Cisco vEdge devices using the SSH Terminal on Cisco SD-WAN Manager.

The default CLI templates include the ciscotacro and ciscotacrw user configuration. These users are enabled by default. However, a customer can disable these users, if needed.

- **ciscotacro User:** This user is part of the operator user group with only read-only privileges. This user can only monitor a configuration but cannot perform any operation that will modify the configuration of the network.
- **ciscotacrw User:** This user is part of the netadmin user group with read-write privileges. This user can modify a network configuration. In addition, only this user can access the root shell using a consent token.

Use the **tools consent-token** command to authenticate the network administrator of an organization to access system shell. Starting Cisco Catalyst SD-WAN Control Components Release 20.12.x, the **request support ciscotac** command is deprecated.

### Limitations

- Only 16 concurrent sessions are supported for the ciscotacro and ciscotacrw users.
- The session duration is restricted to four hours. It is not configurable.
- The inactivity timer functionality closes user sessions that have been idle for a specified period of time. This feature is enabled by default and the timeout value is 30 minutes. However, the user configuration includes the option of extending the inactivity timer.
- A customer can remove these two users. If removed, the customer can open a case and share temporary login credentials or share the screen with the Cisco Support team for troubleshooting an issue.

# Configure Sessions in Cisco SD-WAN Manager

*Table 31: Feature History*

| Feature History | Release Information | Description |
|---|---|---|
| Configure Sessions in Cisco SD-WAN Manager | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>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 **User Sessions**.
3. Under **Client Session Timeout**, click **Session Timeout**.
4. Specify the timeout value, in minutes.
5. 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 **User Sessions**.
3. In the **SessionLifeTime Timeout (minutes) field**, specify the session timeout value, in minutes, from the drop-down list.
4. 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 **User Sessions**.
3. In **Server Session Timeout Timeout(minutes)** field, specify the timeout value, in minutes.
4. 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. In Max Session Per User, click **Session**.
3. In the **Max Sessions Per User** field, specify a value for the maximum number of user sessions.
4. Click **Save**.

# Configuring RADIUS Authentication Using CLI

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication

requests to a central RADIUS server, which contains all user authentication and network service access information.

To have a Cisco IOS XE Catalyst SD-WAN device use RADIUS servers for user authentication, configure one or up to 8 servers:

```
Deviceconfig-transaction
Device(config)# radius server test address ipv4 10.1.1.55 acct-port 110
Device(config-radius-server)# key 33
Device(config-radius-server)# exit
Device(config)# radius server test address ipv4 10.1.1.55 auth-port 330
Device(config-radius-server)# key 55
Device(config-radius-server)#
```

For each RADIUS server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear text string up to 31 characters long or as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server. To configure more than one RADIUS server, include the **server** and **secret-key** commands for each server.

The remaining RADIUS configuration parameters are optional.

To set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

By default, the Cisco IOS XE Catalyst SD-WAN device uses port 1812 for authentication connections to the RADIUS server and port 1813 for accounting connections. To change these port numbers, use the **auth-port** and **acct-port** commands.

If the RADIUS server is reachable via a specific interface, configure that interface with the **source-interface** command.

You can tag RADIUS servers so that a specific server or servers can be used for AAA, IEEE 802.1X, and IEEE 802.11i authentication and accounting. Define the tag here, with a string from 4 to 16 characters long. Then associate the tag with the **radius-servers** command when you configure AAA, and when you configure interfaces for 802.1X and 802.11i.

If the RADIUS server is located in a different VPN from the Cisco IOS XE Catalyst SD-WAN device, configure the server's VPN number so that the Cisco IOS XE Catalyst SD-WAN device can locate it. If you configure multiple RADIUS servers, they must all be in the same VPN.

When waiting for a reply from the RADIUS server, a Cisco IOS XE Catalyst SD-WAN device waits 3 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Device# config-transaction
 Device(config)# aaa group server radius server-10.99.144.201
 Device(config-sg-radius)# server-private 10.99.144.201 auth-port 1812 timeout 5 retransmit
 3
```

# Configure SSH Authentication

*Table 32: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Secure Shell Authentication Using RSA Keys | Cisco IOS XE Catalyst SD-WAN Release 16.12.1b | This feature helps configure RSA keys by securing communication between a client and a Cisco Catalyst SD-WAN server. |

The Secure Shell (SSH) protocol provides secure remote access connection to network devices.

SSH supports user authentication using public and private keys. To enable SSH authentication, public keys of the users are stored in the home directory of authenticating user in the following location:

```
~<user>/.ssh/authorized_keys
```

A new key is generated on the client machine which owns the private-key. Any message encrypted using the public key of the SSH server is decrypted using the private key of the client.

### Restrictions for SSH Authentication on Cisco Catalyst SD-WAN

- The range of SSH RSA key size supported by Cisco IOS XE Catalyst SD-WAN devices is from 2048 to 4096. SSH RSA key size of 1024and 8192 are not supported.
- A maximum of two keys per user are allowed on Cisco IOS XE Catalyst SD-WAN devices.

## SSH Authentication using Cisco SD-WAN Manager on Cisco IOS XE Catalyst SD-WAN Devices

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. From **Select Devices**, select the type of device for which you are creating the template.
4. From **Basic Information**, choose **CISCO AAA** template.
5. From **Local**, click **New User** and enter the details.
6. Enter **SSH RSA Key**.

**Note** You must enter the complete public key from the id_rsa.pub file in **SSH RSA Key**.

# Configure SSH Authentication using CLI on Cisco IOS XE Catalyst SD-WAN Devices

SSH key based login is supported on IOS. Per user a maximum of 2 keys can be supported. Also, IOS only supports RSA based keys.

Traditional IOS CLI, allow support for:

• Key-string

• Key-hash – The key-string is base64 decoded and MD5 hash is run on it.

However, the transaction yang model has provision to only copy the key-hash (instead of the entire key-string). Cisco SD-WAN Manager does this conversion and pushes the configuration to the device.

### Public Keys supported on Cisco IOS XE Catalyst SD-WAN Devices

- SSH-RSA

# Configure the Authentication Order

The authentication order dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port. The default authentication order is **local**, then **radius**, and then **tacacs**. With the default authentication order, the authentication process occurs in the following sequence:

- The authentication process first checks whether a username and matching password are present in the running configuration on the local device.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, the user is authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.
- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Cisco IOS XE Catalyst SD-WAN device device is denied.

To modify the default order, use the **auth-order** command:

Specify one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be **local**.

To have the "admin" user use the authentication order configured in the **auth-order** command, use the following command:

```
Device(config-system-aaa)# admin-auth-order
```

If you do not include this command, the "admin" user is always authenticated locally.

You can configure authentication to fall back to a secondary or tertiary authentication mechanism when the higher-priority authentication method fails to authenticate a user, either because the user has entered invalid credentials or because the authentication server is unreachable (or all the servers are unreachable):

- If the authentication order is configured as **radius local**:
  - With the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
- If the authentication order is configured as **local radius**:
  - With the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
- If the authentication order is configured as **radius tacacs local**:
  - With the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.

If a remote server validates authentication but does not specify a user group, the user is placed into the user group **basic**.

If a remote server validates authentication and specifies a user group (say, X), the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

If a remote server validates authentication and that user is not configured locally, the user is logged in to the vshell as the user **basic**, with a home directory of /home/basic.

If a remote server validates authentication and that user is configured locally, the user is logged in to the vshell under their local username (say, eve) with a home direction of /home/*username* (so, /home/eve).

**Note** Tags are used for grouping, describing, or finding devices. You can tag RADIUS and TACAC servers for authentication and accounting. You can add more than one tag to a device. Starting from Cisco vManage Release 20.9.1, following new tags are used in authentication:

- Viptela-User-Group: for user group definitions instead of Viptela-Group-Name.
- Viptela-Resource-Group: for resource group definitions.

# Role-Based Access with AAA

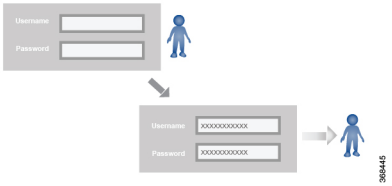
The Cisco Catalyst SD-WAN AAA software implements role-based access to control the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices. Role-based access consists of three components:

- Users are those who are allowed to log in to a Cisco IOS XE Catalyst SD-WAN device.
- User groups are collections of users.

- Privileges are associated with each group. They define the commands that the group's users are authorized to issue.

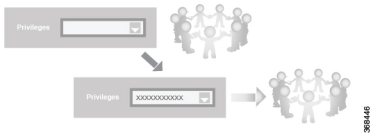
### Users and User Groups

All users who are permitted to perform operations on a Cisco IOS XE Catalyst SD-WAN device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on each device that a user is allowed to access.




The Cisco Catalyst SD-WAN software provides one standard username, **admin**, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the **admin** username password is **admin**. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE Catalyst SD-WAN device. As part of configuring the login account information, you specify which user group or groups that user is a member of. You do not need to specify a group for the **admin** user, because this user is automatically in the user group **netadmin** and is permitted to perform all operations on the Cisco IOS XE Catalyst SD-WAN device.




The user group itself is where you configure the privileges associated with that group. These privileges correspond to the specific commands that the user is permitted to execute, effectively defining the role-based access to the Cisco Catalyst SD-WAN software elements.

The Cisco Catalyst SD-WAN software provides the following standard user groups:

- **basic**: The basic group is a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission to both view and modify information on the device.
- **operator**: The operator group is also a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission only to view information.
- **netadmin**: The netadmin group is a non-configurable group. By default, this group includes the **admin** user. You can add other users to this group. Users in this group are permitted to perform all operations on the device.
- Minimum supported release: Cisco vManage Release 20.9.1

**network_operations**: The **network_operations** group is a non-configurable group. Users in this group can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as application aware routing policy or CFlowD policy.

- Minimum supported release: Cisco vManage Release 20.9.1

**security_operations**: The **security_operations** group is a non-configurable group. Users in this group can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** group are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** group require **network_operations** users to intervene on day-0 to deploy security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.

**Note** Only admin users can view running and local configuration. Users associated with predefined operator user group do not have access to the running and local configurations. The predefined user group operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new user group with the selected features from the features list with both read and write access and associate the group with the custom user.

### Privileges for Role-Based Access

Role-based access privileges are arranged into five categories, which are called *tasks:*

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy—Privileges for controlling control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.
- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.
- System—General systemwide privileges.

The tables in the following sections detail the AAA authorization rules for users and user groups. These authorization rules apply to commands issued from the CLI and to those issued from Netconf.

### User Authorization Rules for Operational Commands

The user authorization rules for operational commands are based simply on the username. Any user who is allowed to log in to the Cisco IOS XE Catalyst SD-WAN device can execute most operational commands. However, only the **admin** user can issue commands that affect the fundamental operation of the device, such as installing and upgrading the software and shutting down the device.

Note that any user can issue the **config** command to enter configuration mode, and once in configuration mode, they are allowed to issue any general configuration command. Also, any user is allowed to configure their password by issuing the **system aaa user** *self* **password** *password* command and then committing that

configuration change. For the actual commands that configure device operation, authorization is defined according to user group membership. See User Group Authorization Rules for Configuration Commands.

The following tables lists the AAA authorization rules for general CLI commands. All the commands are operational commands except as noted. Also, some commands available to the "admin" user are available only if that user is in the "netadmin" user group.

| CLI Command | Any User | Admin User |
|---|---|---|
| clear history | X | X |
| commit confirm | X | X |
| complete-on-space | X | X |
| config | X | X |
| exit | X | X |
| file | X | X |
| help | X | X |
| [no] history | X | X |
| idle-timeout | X | X |
| job | X | X |
| logout | — | X (users in netadmin group only) |
| monitor | X | X |
| nslookup | X | X |
| paginate | X | X |
| ping | X (users in netadmin group only) | X (users in netadmin group only) |
| poweroff | — | X(users in netadmin group only) |
| prompt1 | X | X |
| prompt2 | X | X |
| quit | X | X |
| reboot | — | X (users in netadmin group only) |
| request aaa request admin-tech request firmware request interface-reset request nms request reset request software | — | X (users in netadmin group only) |
| request execute request download request upload | X | X |

| CLI Command | Any User | Admin User |
|---|---|---|
| request (everything else) | — | X |
| rollback (configuration mode command) | — | X (users in netadmin group only) |
| screen-length | X | X |
| screen-width | X | X |
| show cli | X | X |
| show configuration commit list | X | X |
| show history | X | X |
| show jobs | X | X |
| show parser dump | X | X |
| show running-config | X | X |
| show users | X | X |
| system aaa user *self* password *password* (configuration mode command) (Note: A user cannot delete themselves) | | |
| tcpdump | X | X |
| timestamp | X | X |
| tools ip-route | X | X |
| tools netstat | X | X |
| tools nping | X | X |
| traceroute | X | X |
| vshell | X<br>(Only available in Cisco vManage Release 20.11.1 and earlier releases) | X<br>(From Cisco Catalyst SD-WAN Manager Release 20.12.1, vshell AAA authorized access is limited only to netadmin users) |

### User Group Authorization Rules for Operational Commands

The following table lists the user group authorization roles for operational commands.

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| clear app | | X | | | |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| clear app-route | | X | | | |
| clear arp | X | | | | |
| clear bfd | | | X | | X |
| clear bgp | | | X | | X |
| clear bridge | X | | | | |
| clear cellular | X | | | | |
| clear control | | | | X | |
| clear crash | | | | | X |
| clear dhcp | | | | | X |
| clear dns | | | | | X |
| clear igmp | | | X | | |
| clear installed-certificates | | | | X | |
| clear interface | X | | | | |
| clear ip | | | X | | |
| clear notification | | | | | X |
| clear omp | | | X | | |
| clear orchestrator | | | | X | |
| clear ospf | | | X | | |
| clear pim | | | X | | |
| clear policy | | X | | | |
| clear pppoe | X | | | | |
| clear system | | | | | X |
| clear tunnel | | | | X | |
| clear wlan | X | | | | |
| clear ztp | | | | X | X |
| clock | | | | | X |
| debug bgp | | | X | | |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| debug cellular | X | | | | |
| debug cflowd | | X | | | |
| debug chmgr | | | | | X |
| debug config-mgr | | | | | X |
| debug dhcp-client | | | | | X |
| debug dhcp-helper | | | | | X |
| debug dhcp-server | | | | | X |
| debug fpm | | X | | | |
| debug ftm | | | | | X |
| debug igmp | | | X | | |
| debug netconf | | | | | X |
| debug omp | | | X | | |
| debug ospf | | | X | | |
| debug pim | | | X | | |
| debug resolver | | | X | | |
| debug snmp | | | | | X |
| debug sysmgr | | | | | X |
| debug transport | | | | | X |
| debug ttm | | | | | X |
| debug vdaemon | | | | X | X |
| debug vrrp | | | | X | |
| debug wlan | X | | | | |
| request certificate | | | | X | |
| request control-tunnel | | | | X | |
| request controller | | | | X | |
| request controller-upload | | | | X | |
| request csr | | | | X | |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| request device | | | | X | |
| request device-upload | | | | X | |
| request on-vbond-controller | | | | X | |
| request port-hop | | | | X | |
| request root-cert-chain | | | | X | |
| request security | | | | X | |
| request vedge | | | | X | |
| request vedge-upload | | | | X | |
| request vsmart-upload | | | | X | |
| show aaa | | | | | X |
| show app | | X | | | |
| show app-route | | X | | | |
| show arp | X | | | | |
| show bfd | | | X | | X |
| show bgp | | | X | | |
| show boot-partition | | | | | X |
| show bridge | X | | | | |
| show cellular | X | | | | |
| show certificate | | | | X | |
| show clock | | | | | X |
| show control | | | | X | X |
| show crash | | | | | X |
| show debugs—same as debug commands | | | | | |
| show dhcp | | | | | X |
| show external-nat | | | | X | X |
| show hardware | | | | | X |
| show igmp | | | X | | |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| show interface | X | | | | |
| show ip | | | X | | X |
| show ipsec | | | | X | |
| show licenses | | | | | X |
| show logging | | | | | X |
| show multicast | | | X | | |
| show nms-server | | | | | X |
| show notification | | | | | X |
| show ntp | | | | | X |
| show omp | | X | X | | X |
| show orchestrator | | | | X | |
| show ospf | | | X | | |
| show pim | | | X | | |
| show policer | | X | | | |
| show policy | | X | | | |
| show ppp | X | | | | |
| show pppoe | X | | | | |
| show reboot | | | | | X |
| show security-info | | | | X | |
| show software | | | | | X |
| show system | | | | | X |
| show transport | | | | | X |
| show tunnel | | | | X | |
| show uptime | | | | | X |
| show users | | | | | X |
| show version | | | | | X |
| show vrrp | X | | | | |
| show wlan | X | | | | |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| show ztp | | | | X | |

### User Group Authorization Rules for Configuration Commands

The following table lists the user group authorization rules for configuration commands.

| Configuration Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| apply-policy | | X | | | |
| banner | | | | | X |
| bfd | | | X | | X |
| bridge | X | | | | |
| omp | | X | X | | X |
| policy | | X | | | |
| security | | | | X | X |
| snmp | | | | | X |
| system | | | | | X |
| vpn interface | X | | | | |
| vpn ip | | | X | | |
| vpn router | | | X | | |
| vpn service | | | X | | |
| vpn (everything else, including creating, deleting, and naming) | | | | | X |
| wlan | X | | | | |

# Configuring AAA using Cisco SD-WAN Manager Template

*Table 33: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Authorization and Accounting | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>Cisco vManage Release 20.5.1 | This feature provides for the configuration of authorization, which authorizes commands that a user enters on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device. |

Configuring AAA by using the Cisco SD-WAN Manager template lets you make configuration setting inCisco SD-WAN Manager and then push the configuration to selected devices of the same type. This procedure is a convenient way to configure several of the same type of devices at one time.

Use the AAA template for Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Controllers, and Cisco IOS XE Catalyst SD-WAN devices.

Cisco IOS XE Catalyst SD-WAN devices support configuration of authentication, authorization, and accounting (AAA) in combination with RADIUS and TACACS+.

**Note** You must configure a local user with a secret key via the template if you are using PPP or using MLPPP with CHAP.

## 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 34:***

| 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 .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

# Configuring Local Access for Users and User Groups

You can configure local access to a device for users and user groups. Local access provides access to a device if RADIUS or TACACS+ authentication fails.

To configure local access for individual users, select **Local**.

To add a new user, from **Local** click **+ New User**, and configure the following parameters:

***Table 35:***

| Parameter Name | Description |
|---|---|
| Name | Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.<br><br>The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved. |

| Parameter Name | Description |
|---|---|
| Password | Enter a password for the user.<br>Each username must have a password. Users are allowed to change their own passwords.<br>The default password for the admin user is admin. We strongly recommended that you change this password.<br>**Note** When configuring local users using a Cisco SD-WAN Manager AAA template, Cisco SD-WAN Manager uses a Cisco type 9 password type. The Cisco type 9 password type uses the scrypt algorithm for hashing the passwords of local users. The Cisco SD-WAN Manager AAA template uses only the Cisco type 9 password type for hashing of local user passwords.<br>If you configure local users using a device CLI template or a CLI add-on template, you can choose other Cisco password types for hashing of local user passwords. For more information, see Configure Type 6 Passwords Using CLI Add-On Template. |
| Privilege Level 1 OR 15 | Select between privilege level 1 or 15.<br>• **Level 1**: User EXEC mode. Read-only, and access to limited commands, such as the `ping` command.<br>• **Level 15**: Privileged EXEC mode. Full Access to all commands, such as the `reload` command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1 |
| SSH RSA Key(s) | Add SSH RSA Keys by clicking the **+ Add** button. A new field is displayed in which you can paste your SSH RSA key. To remove a key, click the - button.<br>Devices support a maximum of 2 SSH RSA keys. |

Click **Add** to add the new user. Click **+ New User** again to add additional users.

To configure local access for user groups, you first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups. To make this configuration, from **Local** select **User Group**.

Click **+ New User Group**, and configure the following parameters:

*Table 36:*

| Parameter Name | Description |
|---|---|
| Name | Name of an authentication group. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The Cisco Catalyst SD-WAN software provides three standard user groups, basic, netadmin, and operator. The user admin is automatically placed in the group netadmin and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group basic. All users in the basic group have the same permissions to perform tasks, as do all users in the operator group. The following groups names are reserved, so you cannot configure them: adm, audio, backup, bin, cdrom, dialout, dip, disk, fax, floppy, games, gnats, input, irc, kmem, list, lp, mail, man, news, nogroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, utmp, video, voice, and www-data. Also, group names that start with the string viptela-reserved are reserved. |
| Feature Type | Click **Preset** to display a list of preset roles for the user group. Click **Custom** to display a list of authorization tasks that have been configured. |
| Feature | The feature table lists the roles for the user group. These roles are Interface, Policy, Routing, Security, and System. Each role allows the user group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Click the appropriate boxes for Read, Write, and None to assign privileges to the group for each role. |

Click **Add** to add the new user group.

To add another user group, click **+ New User Group** again.

To delete a user group, click the trash icon at the right side of the entry. You cannot delete the three standard user groups, basic, netadmin, and operator.

# Configuring RADIUS Authentication

Configure RADIUS authentication if you are using RADIUS in your deployment.

To configure a connection to a RADIUS server, from **RADIUS**, click **+ New Radius Server**, and configure the following parameters:

*Table 37:*

| Parameter Name | Description |
|---|---|
| Address | Enter the IP address of the RADIUS server host. |
| 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. *Default:* Port 1812 |
| Accounting Port | Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. *Range:* 0 through 65535. *Default:* 1813. |

| Parameter Name | Description |
|---|---|
| Timeout | Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request.<br>*Default:* 5 seconds.<br>*Range:* 1 through 1000 |
| Retransmit Count | Enter the number of times the device transmits each RADIUS request to the server before giving up. *Default:* 5 seconds. |
| Key (Deprecated) | Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can type 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. |

Click **Add** to add the new RADIUS server.

To add another RADIUS server, click **+ New RADIUS Server** again.

To remove a server, click the trash icon.

*CLI equivalent:*

```
Device(config)# radius server 10.99.144.201
Device1(config-radius-server)# retransmit 5
Device(config-radius-server)# timeout 10
```

# Configuring TACACS+ Authentication

Configure TACACS+ authentication if you are using TACACS+ in your deployment.

To configure a connection to a TACACS+ server, from **TACACS**, click **+ New TACACS Server**, and configure the following parameters:

***Table 38:***

| Parameter Name | Description |
|---|---|
| Address | Enter the IP address of the TACACS+ server host. |
| Port | Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0.<br>*Default:* Port 49 |
| Timeout | Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. *Default:* 5 seconds. *Range:* 1 through 1000 |
| Key | Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type 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 TACACS+ server. |

Click **Add** to add the new TACACS server.

To add another TACACS server, click **+ New TACACS Server** again.

To remove a server, click the trash icon.

# Configuring 8021X

For information on configuring 802.1X, see Configure IEEE 802.1X Authentication, on page 108.

# Configuring Authentication Order

You can configure the authentication order for devices. The authentication order specifies the order in which the system attempts to authenticate user, and provides a way to proceed with authentication if the current authentication method is unavailable.

To configure AAA authentication order on a Cisco IOS XE Catalyst SD-WAN device, select the Authentication tab and configure the following parameters:

***Table 39:***

| Parameter Name | Description |
|---|---|
| Server Group Order | Configuring a device to use AAA server groups provides a way to group existing server hosts. Grouping existing server hosts allows you to select a subset of the configured server hosts and use them for a particular service<br><br>To change the default order of authentication methods that the software tries when verifying user access to a Cisco IOS XE Catalyst SD-WAN device:<br><br>**1.** Click the ServerGroups priority order field to display the drop-down list of server groups. The list displays groups from local, RADIUS, and TACACS authentication methods.<br><br>**2.** From the list, select the groups in the order that you want the software to verify a user trying to access a Cisco IOS XE Catalyst SD-WAN device.<br><br>You must select at least one group from the list. |

# Configure Authorization and Accounting

***Table 40: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Authorization and Accounting | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br><br>Cisco vManage Release 20.5.1 | This feature provides for the configuration of authorization, which authorizes commands that a user enters on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device. |

# 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. |
| 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 41:***

| 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 IEEE 802.1X Authentication

*Table 42: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| 802.1X Support for SD-WAN | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | This feature lets you enable the IEEE 802.1X authentication on Cisco IOS XE Catalyst SD-WAN devices. To be able to configure this feature using Cisco SD-WAN Manager, ensure that Cisco SD-WAN Manager is running Cisco SD-WAN Release 20.1.1. |

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, IEEE 802.1X is supported based on Identity-Based Networking Services (IBNS)1.0 IOS-XE CLIs. This feature is supported on both LAN and WAN interfaces.

### IEEE 802.1X Open Authentication and Host Modes

Any of the four host modes (single-host mode, multiple-host mode, multi-domain authentication mode, and multiauthentication mode) may be configured to allow a device to gain network access before authentication.

Open authentication is enabled by entering the **authentication open** command after host mode configuration, and acts as an extension to the configured host mode. For example, if open authentication is enabled with single-host mode, then the port will allow only one MAC address. When preauthentication open access is enabled, initial traffic on the port is restricted and independent of 802.1X is configured on the port. If no access restriction other than 802.1X is configured on the port, then a client device will have a full access on the configured VLAN. You can configure open authentication using CLI template only. You cannot configure open authentication using dot1x feature template on Cisco SD-WAN Manager.

### Prerequisites

- Enable RADIUS authentication servers to authenticate IEEE 802.1x services.
- Enable IEEE 802.1X configuration on switch-port interface.
- Enable the following VLAN configurations for authenticated and unauthenticated clients:
  - Restricted VLAN (or authentication rejected VLAN)
  - Guest VLAN
  - Critical VLAN (or authentication failed VLAN)
  - Critical Voice VLAN
- Enable one of the following host-mode authentication:
  - Single-host mode
  - Multiple-host mode
  - Multiple-authentication mode

- Multi-domain mode

- Configure RADIUS Accounting attributes.
- IEEE 802.1X Authentication event using VLAN ID has to be enabled in the Add-on template, if required.

### Restrictions

- IEEE 802.1X Authentication, Authorization, and Accounting (AAA) is not supported on multiple groups.
- Authentication order IEEE 802.1X MAB CLI cannot be disabled through Cisco SD-WAN Manager. The presence of this authentication order CLI results in a 60 second delay in MAB authentication when MAB client is online.
- Authentication open is not supported in feature templates but can be deployed with a CLI add on template.

# Configure IEEE 802.1X Authentication using Cisco SD-WAN Manager

IEEE 802.1X is a port-based network access control (PNAC) protocol that prevents unauthorized network devices from gaining access to wired networks by providing authentication for devices that want to connect to a wired network.

A RADIUS authentication server must authenticate each client connected to a port before that client can access any services offered by network.

To configure IEEE 802.1X authentication on the interface, first create a **Cisco AAA** feature template:

1. In Cisco SD-WAN Manager, select **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 titled **Feature**.

3. Select your device from the list on the left panel.
4. Select the **Cisco AAA** template.
5. Enter the **Template Name** and **Description.**
6. Select the **RADIUS** tab and under **RADIUS SERVER** click on **New RADIUS Server.**
7. Configure the following parameters:

| Parameter Name | Description |
|---|---|
| Mark as Optional Row | Check the **Mark as Optional Row** check box to mark your configuration as device-specific. |
| Address | Enter IP Address of the RADIUS server. |

| Parameter Name | Description |
|---|---|
| Authentication Port | Click **Authentication**, then click Add New Authentication Entry to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session.<br>To save the entry, click **Add**. |
| Accounting Port | Click **Accounting**, then click **Add New Accounting Entry** to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session.<br>To save the entry, click **Add**. |
| Timeout | Configure how long to wait for replies from the RADIUS server. |
| Retransmit Count | Configure how many times this RADIUS server is contacted. |
| Key | Enter the RADIUS server shared key. |

8. Click **Add.**
9. Select **RADIUS GROUP** and click on **New RADIUS Group** to configure these parameters:

| Parameter Name | Description |
|---|---|
| VPN-ID | Enter the VPN through which the RADIUS or other authentication server is reachable. |
| Source Interface | Enter the interface that will be used to reach the RADIUS server. |
| Radius Server | Configure the Radius server. |

10. Click **Add.**
11. Select the **802.1X** tab and enter these parameters:

| Parameter Name | Description |
|---|---|
| Authentication Param | Click On to enable authentication parameters. |
| Accounting Param | Click On to enable accounting parameters. |

12. To save this feature template, click **Save**.
13. To enable this feature on your device, ensure to add these feature templates to your device template.

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

Next create a **Switch Port** template that can be used for the Switch Port device:

1. To create a **Switch Port** template, repeat steps 1 to 3 from above.
2. Select the **Switch Port** template.

3. Enter the **Template Name** and **Description.**
4. Select the **Interface** tab click on **New Interface.**
5. Configure the following parameters:

| Parameter Name | Description |
|---|---|
| Interface name | Enter the interface name. |
| Speed | Enter the interface speed. |
| VLAN Name | Enter the VLAN name. |
| VLAN ID | Enter the VLAN identifier associated with the bridging domain. |
| 802.1X | Enable IEEE 802.1X authentication on this interface. Select "On".<br>This will provide a further set of parameters listed below. |
| Interface PAE Type | Enter the IEEE 802.1x Interface PAE type. |
| Control Direction | Enter unidirectional or bidirectional authorization mode. |
| Host Mode | Select whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients):<br>• Multi Auth—Grant access to one host on a voice VLAN and multiple hosts on data VLANs.<br>• Multi Host—Grant access to multiple hosts<br>• Single Host—Grant access only to the first authenticated host. This is the default.<br>• Multi-Domain—Grant access to both a host and a voice device, such as an IP phone on the same switch port.<br>**Note** These options are available only in the 'Global' Host Mode settings. |
| Periodic Reauthentication | Enter how often to reauthenticate IEEE 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request.<br>Range: 0 to 1440 minutes |

6. Click on **Advanced Options** and enter the following:

| Parameter Name | Description |
|---|---|
| Authentication Order | Enter the order of authentication methods to use when authenticating devices for connection to the IEEE 802.1X interface. The default authentication order is RADIUS, then MAC authentication bypass (MAB). |
| MAC Authentication Bypass | Select to enable MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-IEEE 802.1X–compliant clients using a RADIUS server. |

| Parameter Name | Description |
|---|---|
| Port Control Mode | Enter the port control mode to enable IEEE 802.1X port-based authentication on the interface.<br>Auto- Configure this to enable IEEE 802.1X authentication and start the port in unauthorized state. This allows only EAPOL frames to be sent and received through the port. |
| Voice VLAN ID | Configure the Voice VLAN ID. |
| Critical VLAN | Enter the critical VLAN (or authentication failed VLAN) for IEEE 802.1x-compliant clients. Configure network access when RADIUS authentication or the RADIUS server fails. |
| Critical Voice VLAN | Enable the critical voice VLAN. |
| Guest VLAN | Configure guest VLAN to drop non-IEEE 802.1X enabled clients, if the client is not in the MAB list. |
| Restricted VLAN | Enter the restricted VLAN (or authentication failed VLAN) for IEEE 802.1x-compliant clients. Configure limited services to IEEE 802.1X–compliant clients that failed RADIUS authentication. |

7. Click on **Add.**
8. To save this feature template, click **Save**.
9. To enable this feature on your device, ensure to add these feature templates to your device template.

# Configure IEEE 802.1X Open Authentication

You can configure IEEE 802.1X open authentication using the CLI add-on template.

```
Device# config-transaction
Device(config)# interface GigabitEthernet2
Device(config-if)# authentication open
```

# Configure IEEE 802.1X Authentication using CLIs

### Configuration

For this feature, two sets of configurations are required-

1. **Configure the Global AAA commands:**
   a. Enable or disable IEEE 802.1X globally

```
Device(config)# aaa authentication dot1x default group radius-0
Device(config)# aaa authorization network default group radius-0
Device(config)# dot1x system-auth-control
Device(config)# radius-server dead-criteria time 10 tries 3
Device(config)# radius-server deadtime 15
```

   b. Enable accounting

```
Device(config)# aaa accounting dot1x default start-stop group radius-0
```

2. **Configure the Interface Level commands:**

   **a.** Enable or disable IEEE 802.1X on port-basis

   ```
   Device(config-if)# dot1x pae authenticator
   Device(config-if)# authentication port-control auto
   ```

   **b.** Enable or disable MAB on port-basis

   ```
   Device(config-if)# mab
   ```

   **c.** Select host-mode

   ```
   Device(config-if)# authentication host-mode  <multi-auth | multi-domain | multi-host
    | single-host>
   ```

   **d.** Configure voice vlan

   ```
   Device(config-if)# switchport voice vlan <vlan-id>
   ```

   **e.** Select IEEE 802.1X control direction

   ```
   Device(config-if)# authentication control-direction <both | in>
   ```

   **f.** Enable periodic re-authentication and corresponding re-authentication interval and inactivity timeout time

   ```
   Device(config-if)# authentication periodic
   Device(config-if)# authentication timer reauthenticate <internal-in-sec>
   Device(config-if)# authentication timer inactivity <timeout-in-sec>
   ```

   **g.** Configurable authentication orders on per-port basis

   ```
   Device(config-if)# authentication order dot1x mab
   ```

   **h.** Specify the restricted VLAN

   ```
   Device(config-if)#  authentication event fail action authorize vlan <vlan-id>
   ```

   **i.** Specify the guest VLAN

   ```
   Device(config-if)# authentication event no-response action authorize vlan <vlan-id>
   ```

   **j.** Specify the critical VLAN

   ```
   Device(config-if)# authentication event server dead action authorize vlan <vlan-id>
   ```

   **k.** Enable the critical voice VLAN feature

   ```
   Device(config-if)# authentication event server dead action authorize voice
   ```

# Posture Assessment Support

*Table 43: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Posture Assessment Support | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | This feature enables you to utilize Posture Assessment capabilites to validate the compliance of endpoints according to security policies of your enterprise. Identity Services Engine (ISE) Posture functions are integrated into Cisco 1100 Integrated Services Routers. This feature can only be configured using the Add-On feature template in Cisco SD-WAN Manager. |

In a network, endpoint validation is necessary to ensure compliance with security policies of the company and posture assessment enables you to validate this. The posture module enforces security policies on endpoints that are connected to a network. For a connection between the endpoints of Cisco 1100 Integrated Services Router and ISE (Identity Services Engine), authentication interaction between them is required. IEEE 802.1X is the recommended standard authentication process for posture assessment, MAC Authentication Bypass (MAB) can be used as well.

The posture agent software used for this is Cisco AnyConnect Posture Assessment. The Cisco AnyConnect software is installed on the endpoint and has a module called posture. Cisco AnyConnect downloads security policies from ISE server and then checks the conditions (anti-malware condition, anti-spyware condition, anti-virus condition, application condition, USB condition) of the endpoints. If all conditions are met, Cisco AnyConnect gives a ‘Compliant’ result to the ISE server. If not, Cisco AnyConnect gives a ‘NonCompliant’ result. After authorization and authentication of the endpoints by authenticantion and redirect Access Control Lists (ACL), Cisco AnyConnect posture module on the client end initiates posture assessment with the posture-policy server.

After posture assessment is completed and authenticated, the RADIUS CoA (Change of Authorization) process is initiated by a policy set on ISE, from RADIUS servers to re-authenticate or re-authorize new policies. Once posture assessment is successful, access to the entire network is pushed down to the Cisco ISR 1100 router and to the client, through CoA re-authentication command.

## Prerequisites for Posture Assessment

- Basic IEEE 802.1x authentication process should be functional.
- Change of Authorization (CoA) should be supported.
- Redirect ACL, downloadable ACL (dACL) and critical ACL should be available.
- Device tracking policy (for identity) should be supported.
- URL redirect should be supported.

# Restrictions for Posture Assessment

- Only 8 port Cisco 1100 Integrated Services Routers support ACL functions such as dACL and redirect ACL.
- ACL and Access Control Entry (ACE) rules do not support compare operations, such as >, <, >=, <=
- Up to 120 dACL ACEs are supported, and 64 Redirect ACL ACEs are supported.
- Port ACL and IPv6 ACL are not supported.
- IP option and IP fragment ACL are not supported.
- Per-VLAN device-tracking is not supported.
- Only limited per-port device tracking policy options such as glean and address tracking are allowed.

# Configuring Posture Assessment on Cisco Catalyst SD-WAN

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.

# Type 6 Passwords on Cisco IOS XE SD-WAN Routers

*Table 44: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Type 6 Passwords on Cisco IOS XE SD-WAN Routers | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a<br>Cisco vManage Release 20.4.1 | This feature allows you to use type 6 passwords that use secure reversible encryption. This encryption provides enhanced security by using more secure algorithms to encrypt your passwords. These passwords are supported for the templates detailed in Supported Templates, on page 118. |

## Overview of Type 6 Passwords

The Type 6 Passwords feature enables secure reversible encryption for authentication, authorization, and accounting (AAA) and Simple Network Management Protocol (SNMP) configurations based on the advanced encryption scheme (AES) algorithm.

Reversible encryption is the process by which a password is encrypted with a reversible, symmetric encryption algorithm. To check if the password entered by the user is valid, the password is decrypted and compared to the user-input password. To perform this encryption, the symmetric encryption algorithm requires a key which you can provide. The encryption algorithm used is advanced encryption scheme (AES) algorithm in Cipher Block Chaining (CBC) mode with a PKCS#5 padding. This algorithm is used for AAA features such as RADIUS, TACACS+, SNMP, and TrustSec.

When you create a supported template in Cisco vManage Release 20.4.1 and later releases, by default type 6 passwords are used. Cisco SD-WAN Manager encrypts the passwords and sends the passwords to the router over a secure tunnel. The router then encrypts the passwords into the type 6 format and stores the password on the device. The Type 6 Passwords feature is not supported on Viptela software.

**Note** Cisco SD-WAN Manager encrypted passwords show up as either $6$ or $8$. Where as, Cisco IOS XE devices have encryption streams defined as type 0, type 5, type 6, type 8, and so on. On the other hand, Cisco SD-WAN Manager runs on Viptela OS which is based on Linux. Linux uses hashing and encryption schemes. Encrypted passwords on Cisco SD-WAN Manager starting with $6$ refer to sha512-crypt. Passwords beginning with $8$ represent aes-cfb 128 encryption.

**Note** On Cisco IOS XE Catalyst SD-WAN devices, an admin user with privilege 15 is created by default during day-0 bringup of the device. It is recommended that users don't delete this admin user.

**Note** We recommend using type 6 passwords to reduce the vulnerability of a malicious attack against password integrity. On upgrading your device to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, all AAA, RADIUS key, and TACACS+ keys are encrypted to type 6.

# Supported Platforms

Cisco IOS XE Catalyst SD-WAN devices.

# Supported Templates

The following templates support Type 6 passwords:

- RADIUS and TACACS authentication using the Cisco AAA template.
- SNMP template.
- CLI add-on template.

# Restrictions

- For SNMP templates, the community name is encrypted by default. Therefore, to upgrade existing SNMP templates to type 6 passwords, delete and re-create the community and trap target.
- When using type 6 passwords with the **keychain key-string** command, the maximum password length for a clear text is 38 characters.

# Configure Type 6 Passwords Using Cisco SD-WAN Manager

## 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.

## 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**.

# Verify Type 6 Passwords

To verify that your passwords are upgraded to type 6 passwords, you can do one of the following:

- On Cisco SD-WAN Manager, when you attach a configuration that supports type 6 passwords to your device the configuration preview displays the encrypted password. For example:

  ```
  snmp-server community 0 $CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==
   ro
  ```

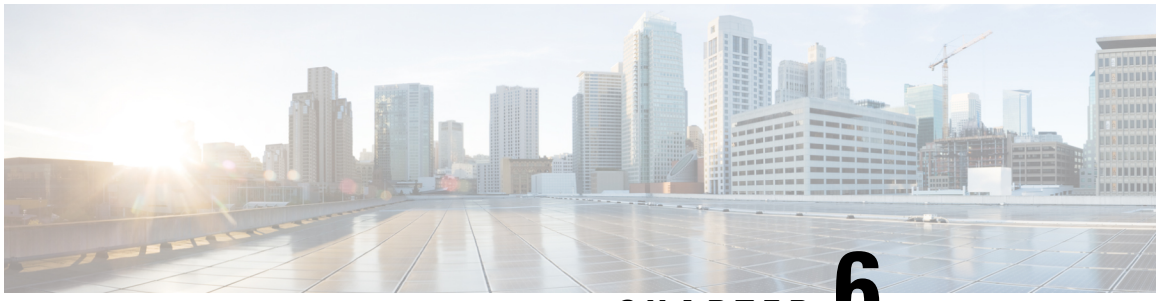
  Despite the command displaying the type as `0`, the `$CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==` string represents your encrypted password. If your password is encrypted, it will begin with `$CRYPT_CLUSTER$`.

- On your device, you can run the following command to display your encrypted passwords:

  ```
  Device#show run | sec aaa
  aaa new-model
  aaa group server tacacs+ tacacs-0
  ```

```
server-private 10.0.0.1 key 6 BibgKcVeWF]^aK[XfEIICXMCbdScBYAAB
aaa group server radius radius-0
server-private 10.0.0.2 timeout 5 retransmit 3 key 6 CHd_VK[]NHEdcVCWGCaENGINQHLBEhDBe
```

The output displays that the password is type 6 and also displays your encrypted password.



CHAPTER 6

# Role Based Access Control

*Table 45: Feature History*

| Feature Name | Release Information | Feature Description |
|---|---|---|
| Co-Management: Granular Role-Based Access Control | Cisco Catalyst SD-WAN Manager Release 20.13.1 | This feature introduces role-based access control (RBAC) based on sites, scope, or roles. It is a method of authorizing system access for users based on a combination of role and scope of a user.<br>You can create scope, users and roles with required read and write permissions for Cisco SD-WAN Manager policies. RBAC prevents unauthorized access and reduces the risk of data breaches and other security incidents. |
| Canadian French Language Support on Cisco Catalyst SD-WAN Manager | Cisco Catalyst SD-WAN Manager Release 20.13.1 | Added support for using Canadian French for the Cisco Catalyst SD-WAN Manager user interface. |


- Information About Role Based Access Control, on page 121
- Restriction for Role Based Access Control, on page 123
- Configure Role Based Access Control, on page 123


# Information About Role Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and scope. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and scopes. A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access.

**User**: is the entity that performs different actions in Cisco SD-WAN Manager. A user belongs to a role.

**Roles**: define the permissions (Read, Write or Deny) allowed for a user for different APIs or functionalities.

**Scope**: define the set of objects (sites, devices or templates) on which a user can perform actions.

When **Read** or **Write** is selected, the user can view and make changes for the selected features. When **Read** is selected, the user can only view information. When **Deny** is selected, the user can neither view or make changes to the Cisco IOS XE Catalyst SD-WAN.

System default roles cannot be changed or modified. The Cisco IOS XE Catalyst SD-WAN software provides the following system default roles:

- **basic**: The basic role is a system default role and is pre-built-in Cisco SD-WAN Manager. You cannot modify or delete. If you want to modify the role, you must make a copy of it and then modify it as a new customer role.
- **operator**: The operator role is also a configurable role and can be used for any users and privilege levels. This role is designed to include users who have permission only to view information.
- **netadmin**: The netadmin role is a non-configurable role. By default, this role includes the **admin** user. You can add other users to this role. Users with this role are permitted to perform all operations on the device.
- **network_operations**: The **network_operations** role is a non-configurable role. Users in this role can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as an application aware routing policy or Cflowd policy.
- **security_operations**: The **security_operations** role is a non-configurable role. Users in this role can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** role are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** role require **network_operations** users to intervene on day-0 to deploy a security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.

**Note** Only netadmin users can view the running and local configuration. Users associated with a predefined operator role do not have access to the running and local configurations. The predefined role operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new role with the selected features from the features list with both read and write access and associate the role with the custom user.

### Privileges for Role-Based Access

Role-based access privileges are arranged into five categories, which are called *tasks:*

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy—Privileges for controlling the control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.
- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.

- System—General system-wide privileges.

# Restriction for Role Based Access Control

- In Cisco Catalyst SD-WAN Manager Release 20.13.1, you can only configure one role and one scope per user.

# Configure Role Based Access Control

## Configure Scope

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

   By default **Scope** menu is selected. The table displays the list of scopes configured in the device.
2. Click **Add Scope**.
3. Enter **Scope Name** and **Description**.
4. Click **Add Nodes**.
5. Choose the required **Nodes** and click **Save**.

   (Optional) Click **Edit Nodes** to update the existing nodes in the list.
6. (Optional) In the **Associations** pane, click **Add Users** to associate users.
7. In the **Add Users** pop-up window, choose the users that you want to add.
8. Click **Save**.

   The selected users are associated to a scope.
9. (Optional) In the **Configurations** tab, click **Add Configurations** to add configurations.
10. In the **Add Configurations** page, choose the available configurations from the following tabs:
    a. **Configuration Group**
    b. **Device Template**
    c. **Feature Template**
    d. **Feature Profile**
    e. **Security Policy**
    f. **Localized Policy**
11. Click **Save**.

    A new scope with nodes, users and required configurations is created.

# Configure Roles

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

   By default **Roles** menu is selected. The table displays the list of scopes configured in the device.
2. Click **Add Role**.
3. Enter **Custom Role Name** in the **Add Custom Role** page.
4. Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to assign a role.
5. Click **Add**.
6. You can view the new role in the table in the **Roles** page.

### Copy Custom Role

1. In the list of roles, for the role you wish to copy, click **...**, and click **Copy**.

   The **Copy Custom Role** page is displayed.
2. Enter **Custom Role Name**.
3. Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.
4. Click **Copy**.
5. You can view the new role in the table in the **Roles** page.

### Edit Custom Role

1. In the list of roles, for the role you wish to copy, click **...**, and click **Edit**.

   The **Edit Custom Role** page is displayed.
2. Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.
3. Click **Update**.
4. You can view the updated role in the table in the **Roles** page.

### Delete a Role

You can delete a role when it is no longer needed. For example, you might delete a role that you created for a specific project when that project ends.

1. Choose the role you wish to delete, click **...**, and click **delete**.

   The **Warning** page is displayed.
2. To confirm the deletion of the role, click **Delete**.

# Configure Users

### Add User

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.
2. Click **Users**.
3. Click **Add User**.
4. Configure the following:

| Field | Description |
|---|---|
| **Full Name** | Enter the full name of the user. |
| **User Name** | Enter the user name. |
| **Password** | Enter a password. |
| **Remote User** | Enable the **Remote User** option for remote users. If you enable this option, enter an email for the user. |
| **Roles** | Choose roles for the user. |
| **Scope** | Choose the scope for the user. |
| **Select Locale** | (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose a locale to set the language for the Cisco SD-WAN Manager user interface. |

**Note** In Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier releases, Cisco SD-WAN Manager only supported the English language on the user interface. From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cisco SD-WAN Manager user interface supports Canadian French.

5. Click **Add** to add the user.

### Edit User

1. In the **Users** page, for the user you wish to edit, click **...**, and click **Edit**.

   The **Edit User** page is displayed.
2. Enter **Full Name**, **User Name**.
3. Choose the role from the **Roles** drop-down list.
4. Choose the scope from the **Scope** drop-down list.
5. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose the locale from the **Select Locale** drop-down list.

6. Click **Update**.

### Copy User

1. For the user you wish to copy, click **...**, and click **Copy**.

   The **Copy User** page is displayed.

2. Enter **Full Name**, **User Name**.
3. Enter the password in the **Password** and **Confirm Password**fields.
4. Choose the role from the **Roles** drop-down list.
5. Choose the scope from the **Scope** drop-down list.
6. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose the locale from the **Select Locale** drop-down list.
7. Click **Copy**.

### Delete User

If a user no longer needs access to devices, you can delete the user. Deleting a user does not log out the user if the user is logged in.

1. For the user you wish to delete, click **...**, and click **Delete**.
2. To confirm the deletion of the user, click **OK**.

### Change User Password

1. For the user you wish to change the password, click **...** and click **Change Password**.
2. Enter the **Current User Password**.
3. Enter the new password in the **Password** field.
4. Enter the new password again in the **Confirm Password** field.
5. Click **Update**.

### Reset Locked User

1. For the user you wish to reset the lock, click **...** and click **Reset Locked User**.
2. In the **Reset Locked User** pop-up menu, click **Yes**.

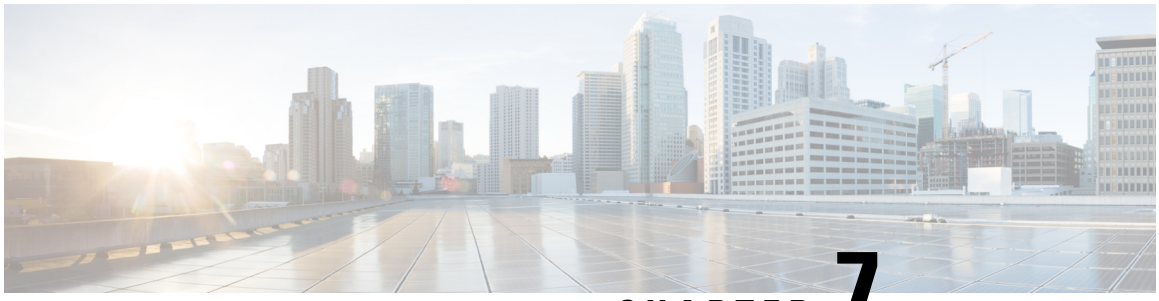
### Administrative Lock

1. For the user you wish to reset the lock, click **...** and click **Administrative Lock**.
2. In the **Lock User** pop-up menu, click **Yes**.

# Configure User Sessions

User Sessions page shows a list of all the active HTTP sessions within Cisco SD-WAN Manager, including username, domain, source IP address, and so on.

To remove a user session, choose the session from the list, and click **Remove Session**.



CHAPTER 7

# Role-Based Access Control (Cisco IOS XE Catalyst SD-WAN Release 17.12.x and Earlier)

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 46: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Role-Based Access Control By Resource Group | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>Cisco vManage Release 20.5.1 | This feature introduces role-based access control (RBAC) based on sites or resource groups. It is a method of authorizing system access for users based on a combination of user groups and resource groups.<br>For large Cisco Catalyst SD-WAN deployments across multiple geographical locations, this feature helps you to split the network administration among different regional administrators. |
| RBAC for Policies | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1 | This feature allows you to create users and user groups with required read and write permissions for Cisco SD-WAN Manager policies. RBAC for policies provides users with the access to all the details of policies to help maximize the operational efficiency. It makes it easier to meet configuration requirements and guarantees that authorized users on the system are only given access to what they need. |

| Feature Name | Release Information | Description |
|---|---|---|
| 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.<br>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:<br>• network_operations user group for non-security policies<br>• security_operations user group for security policies<br>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.<br>This feature introduces new permission options for the following configuration groups and feature profiles.<br>• AppQoE under other feature profile<br>• GPS under transport feature profile<br>• Cisco VPN Interface GRE under WAN/LAN profile.<br>• Cisco VPN Interface IPsec under WAN profile.<br>• Cisco Multicast under LAN profile.<br>• UCSE under other feature profile.<br>• IPv4 Tracker and Tracker Group under transport and service feature profiles.<br>• 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. |

• Information About RBAC, on page 131
• Restrictions for RBAC, on page 145
• Use Cases for RBAC, on page 146
• Configure RBAC, on page 146
• Configure RBAC Using the CLI, on page 179
• Verify RBAC, on page 181
• Monitor RBAC, on page 181

# Information About RBAC

## Role-Based Access Control by VPN

Role-based access control (RBAC) is the process of restricting user access to network configurations and resources. In RBAC, users are assigned roles depending on the resources they need access to. The RBAC by

VPN feature helps you to manage and control access to your network based on the VPNs. It involves setting permissions and privileges to enable access to authorized users.

# RBAC by VPN

Role-based access by VPN allows a network administrator to define VPN groups with one or more network segments. The network administrator can associate a user with a VPN group that restricts user access to devices in the network and features of Cisco SD-WAN Manager.

RBAC by VPN provides the following restricted access to users configured with a VPN group:

- Access to VPN Dashboard
- Monitor devices, network, and application status via VPN dashboard
- VPN dashboard information restricted to devices with segments in the VPN group
- Monitor option restricted to devices with segments in the VPN group
- Interface monitoring on each device restricted to interfaces of segments in the VPN group

# VPN Dashboard Overview

Users configured with VPN group can access only the VPN Dashboard, and it is read-only access. User with Admin access can create the VPN groups and has access to both Admin Dashboard and VPN Dashboard(s). Admin user can access these dashboards by choosing **Dashboard** from the Cisco SD-WAN Manager menu.

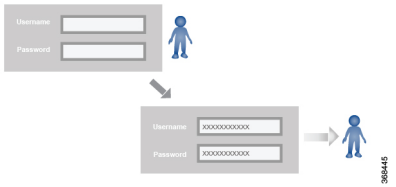
# Role-Based Access with AAA

The Cisco Catalyst SD-WAN AAA software implements role-based access to control the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices. Role-based access consists of three components:

- Users are those who are allowed to log in to a Cisco IOS XE Catalyst SD-WAN device.
- User groups are collections of users.
- Privileges are associated with each group. They define the commands that the group's users are authorized to issue.

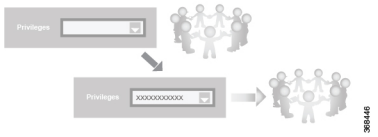
### Users and User Groups

All users who are permitted to perform operations on a Cisco IOS XE Catalyst SD-WAN device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on each device that a user is allowed to access.

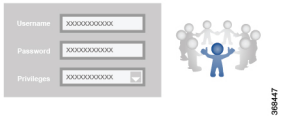


The Cisco Catalyst SD-WAN software provides one standard username, **admin**, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the **admin** username password is **admin**. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE Catalyst SD-WAN device. As part of configuring the login account information, you specify which user group or groups that user is a member of. You do not need to specify a group for the **admin** user, because this user is automatically in the user group **netadmin** and is permitted to perform all operations on the Cisco IOS XE Catalyst SD-WAN device.




The user group itself is where you configure the privileges associated with that group. These privileges correspond to the specific commands that the user is permitted to execute, effectively defining the role-based access to the Cisco Catalyst SD-WAN software elements.




The Cisco Catalyst SD-WAN software provides the following standard user groups:

- **basic**: The basic group is a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission to both view and modify information on the device.
- **operator**: The operator group is also a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission only to view information.
- **netadmin**: The netadmin group is a non-configurable group. By default, this group includes the **admin** user. You can add other users to this group. Users in this group are permitted to perform all operations on the device.
- Minimum supported release: Cisco vManage Release 20.9.1

  **network_operations**: The **network_operations** group is a non-configurable group. Users in this group can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as application aware routing policy or CFlowD policy.
- Minimum supported release: Cisco vManage Release 20.9.1

  **security_operations**: The **security_operations** group is a non-configurable group. Users in this group can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** group are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** group require **network_operations** users to intervene on day-0 to deploy security policy on a device and on day-N to remove a deployed security policy.

However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.

**Note** Only admin users can view running and local configuration. Users associated with predefined operator user group do not have access to the running and local configurations. The predefined user group operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new user group with the selected features from the features list with both read and write access and associate the group with the custom user.

### Privileges for Role-Based Access

Role-based access privileges are arranged into five categories, which are called *tasks:*

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy—Privileges for controlling control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.
- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.
- System—General systemwide privileges.

The tables in the following sections detail the AAA authorization rules for users and user groups. These authorization rules apply to commands issued from the CLI and to those issued from Netconf.

### User Authorization Rules for Operational Commands

The user authorization rules for operational commands are based simply on the username. Any user who is allowed to log in to the Cisco IOS XE Catalyst SD-WAN device can execute most operational commands. However, only the **admin** user can issue commands that affect the fundamental operation of the device, such as installing and upgrading the software and shutting down the device.

Note that any user can issue the **config** command to enter configuration mode, and once in configuration mode, they are allowed to issue any general configuration command. Also, any user is allowed to configure their password by issuing the **system aaa user** *self* **password** *password* command and then committing that configuration change. For the actual commands that configure device operation, authorization is defined according to user group membership. See User Group Authorization Rules for Configuration Commands.

The following tables lists the AAA authorization rules for general CLI commands. All the commands are operational commands except as noted. Also, some commands available to the "admin" user are available only if that user is in the "netadmin" user group.

| CLI Command | Any User | Admin User |
|---|---|---|
| clear history | X | X |
| commit confirm | X | X |
| complete-on-space | X | X |
| config | X | X |

| CLI Command | Any User | Admin User |
|---|---|---|
| exit | X | X |
| file | X | X |
| help | X | X |
| [no] history | X | X |
| idle-timeout | X | X |
| job | X | X |
| logout | — | X (users in netadmin group only) |
| monitor | X | X |
| nslookup | X | X |
| paginate | X | X |
| ping | X (users in netadmin group only) | X (users in netadmin group only) |
| poweroff | — | X(users in netadmin group only) |
| prompt1 | X | X |
| prompt2 | X | X |
| quit | X | X |
| reboot | — | X (users in netadmin group only) |
| request aaa request admin-tech request firmware request interface-reset request nms request reset request software | — | X (users in netadmin group only) |
| request execute request download request upload | X | X |
| request (everything else) | — | X |
| rollback (configuration mode command) | — | X (users in netadmin group only) |
| screen-length | X | X |
| screen-width | X | X |
| show cli | X | X |
| show configuration commit list | X | X |

| CLI Command | Any User | Admin User |
|---|---|---|
| show history | X | X |
| show jobs | X | X |
| show parser dump | X | X |
| show running-config | X | X |
| show users | X | X |
| system aaa user *self* password *password* (configuration mode command) (Note: A user cannot delete themselves) | | |
| tcpdump | X | X |
| timestamp | X | X |
| tools ip-route | X | X |
| tools netstat | X | X |
| tools nping | X | X |
| traceroute | X | X |
| vshell | X<br>(Only available in Cisco vManage Release 20.11.1 and earlier releases) | X<br>(From Cisco Catalyst SD-WAN Manager Release 20.12.1, vshell AAA authorized access is limited only to netadmin users) |

### User Group Authorization Rules for Operational Commands

The following table lists the user group authorization roles for operational commands.

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| clear app | | X | | | |
| clear app-route | | X | | | |
| clear arp | X | | | | |
| clear bfd | | | X | | X |
| clear bgp | | | X | | X |
| clear bridge | X | | | | |
| clear cellular | X | | | | |
| clear control | | | | X | |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| clear crash | | | | | X |
| clear dhcp | | | | | X |
| clear dns | | | | | X |
| clear igmp | | | X | | |
| clear installed-certificates | | | | X | |
| clear interface | X | | | | |
| clear ip | | | X | | |
| clear notification | | | | | X |
| clear omp | | | X | | |
| clear orchestrator | | | | X | |
| clear ospf | | | X | | |
| clear pim | | | X | | |
| clear policy | | X | | | |
| clear pppoe | X | | | | |
| clear system | | | | | X |
| clear tunnel | | | | X | |
| clear wlan | X | | | | |
| clear ztp | | | | X | X |
| clock | | | | | X |
| debug bgp | | | X | | |
| debug cellular | X | | | | |
| debug cflowd | | X | | | |
| debug chmgr | | | | | X |
| debug config-mgr | | | | | X |
| debug dhcp-client | | | | | X |
| debug dhcp-helper | | | | | X |
| debug dhcp-server | | | | | X |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| debug fpm | | X | | | |
| debug ftm | | | | | X |
| debug igmp | | | X | | |
| debug netconf | | | | | X |
| debug omp | | | X | | |
| debug ospf | | | X | | |
| debug pim | | | X | | |
| debug resolver | | | X | | |
| debug snmp | | | | | X |
| debug sysmgr | | | | | X |
| debug transport | | | | | X |
| debug ttm | | | | | X |
| debug vdaemon | | | | X | X |
| debug vrrp | | | | X | |
| debug wlan | X | | | | |
| request certificate | | | | X | |
| request control-tunnel | | | | X | |
| request controller | | | | X | |
| request controller-upload | | | | X | |
| request csr | | | | X | |
| request device | | | | X | |
| request device-upload | | | | X | |
| request on-vbond-controller | | | | X | |
| request port-hop | | | | X | |
| request root-cert-chain | | | | X | |
| request security | | | | X | |
| request vedge | | | | X | |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| request vedge-upload | | | | X | |
| request vsmart-upload | | | | X | |
| show aaa | | | | | X |
| show app | | X | | | |
| show app-route | | X | | | |
| show arp | X | | | | |
| show bfd | | | X | | X |
| show bgp | | | X | | |
| show boot-partition | | | | | X |
| show bridge | X | | | | |
| show cellular | X | | | | |
| show certificate | | | | X | |
| show clock | | | | | X |
| show control | | | | X | X |
| show crash | | | | | X |
| show debugs—same as debug commands | | | | | |
| show dhcp | | | | | X |
| show external-nat | | | | X | X |
| show hardware | | | | | X |
| show igmp | | | X | | |
| show interface | X | | | | |
| show ip | | | X | | X |
| show ipsec | | | | X | |
| show licenses | | | | | X |
| show logging | | | | | X |
| show multicast | | | X | | |
| show nms-server | | | | | X |

| Operational Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| show notification | | | | | X |
| show ntp | | | | | X |
| show omp | | X | X | | X |
| show orchestrator | | | | X | |
| show ospf | | | X | | |
| show pim | | | X | | |
| show policer | | X | | | |
| show policy | | X | | | |
| show ppp | X | | | | |
| show pppoe | X | | | | |
| show reboot | | | | | X |
| show security-info | | | | X | |
| show software | | | | | X |
| show system | | | | | X |
| show transport | | | | | X |
| show tunnel | | | | X | |
| show uptime | | | | | X |
| show users | | | | | X |
| show version | | | | | X |
| show vrrp | X | | | | |
| show wlan | X | | | | |
| show ztp | | | | X | |

### User Group Authorization Rules for Configuration Commands

The following table lists the user group authorization rules for configuration commands.

| Configuration Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| apply-policy | | X | | | |
| banner | | | | | X |

| Configuration Command | Interface | Policy | Routing | Security | System |
|---|---|---|---|---|---|
| bfd | | | X | | X |
| bridge | X | | | | |
| omp | | X | X | | X |
| policy | | X | | | |
| security | | | | X | X |
| snmp | | | | | X |
| system | | | | | X |
| vpn interface | X | | | | |
| vpn ip | | | X | | |
| vpn router | | | X | | |
| vpn service | | | X | | |
| vpn (everything else, including creating, deleting, and naming) | | | | | X |
| wlan | X | | | | |

# RBAC By Resource Group Overview

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1

RBAC by resource groups is a method of restricting or authorizing system access for users based on user groups and resource groups. A user group defines the privileges of a user in the system and the resource group defines the organizations (domains) to which a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate user and resource groups.

For large Cisco Catalyst SD-WAN deployments across multiple geographical locations, you can split the network administration among different regional adminstrators.

Based on the user groups and resources groups to which network administrators are assigned, we can broadly classify them as Global Administrators and Regional Administrators. Global administrators have access to resources in every resource group and have full read-write privileges for all the features. Regional Administrators group have full read-write privileges for all the features, but the resources they can access is controlled by the resource groups to which they are assigned.

### Global Admin

User accounts in the global resource group have access to all resources. A global admin is responsible for overseeing the entire network, but not involved in the operations of the individual devices on a daily basis.

The global admin can assign devices to their corresponding regions, assign the regional admin accounts, manage the controllers, maintain sharable and centralized configurations, and when necessary, operate on the individual devices.

Any user in a single tenant setup with netadmin privileges and also part of global resource group is considered as global admin. Default admin user on Cisco SD-WAN Manager is also a global-admin, and that user can assign more global-admins. Global resource group encompasses all the WAN edges, controllers in the single view.

Global admin can switch to view only a specific resource group and can create templates. Local resource group admins, also called regional admins can clone the global templates and reuse them within their resource groups.

### Regional Admin

The regional admins are responsible for day-to-day operations (configuration, monitoring, onboarding, and so on) for devices in their corresponding regions. They should not have access to or visibility into devices outside of their region. The following user groups can be created:

- resource group admin – full read/write access to devices in the corresponding resource group, can troubleshoot, monitor, attach or detach templates for the WAN edges in their group
- resource group operator – read-only access to WAN edges within their resource group
- resource group basic – basic access

Resource group admins can create new templates and attach or detach to the WAN edges in their group. They can also copy global templates and re-use them.

Resource group decides which resources the user has access to. However, the level of access is controlled by the existing user group.

- If user is in **resource_group_a** and user group **resource_group_admin**, they have full read/write access to all resources in resource_group_a.
- If user is in **resource_group_a** and user group **resource_group_operator**, they have read only access to all resources in **resource_group_a**.
- If user is in **resource_group_a** and user group **resource_group_basic**, they have read only access to interface and system resources in **resource_group_a**.

### Global Resource Group

Global group is a special system pre-defined resource group that has different access control rules.

- Users within this group are considered as global-admins, who can have full access to all resources (devices, templates and policies) in the system and they can manage the resource groups and assign resources and users to groups.
- All other users have read-only access to resources within this group.
- The system default admin account (or tenantadmin account in a multi-tenant setup) is always in this group. This privilege cannot be changed. However, the admin account may add/remove other user accounts to or from this group.

### IdP (SSO)-Managed Group

An identity provider (IdP) is a service that stores and verifies user identity. IdPs typically work with single sign-on (SSO) providers to authenticate users. If a user is authenticated with a SSO service of an IdP, the group information is also provided and managed by the IDP. An IdP passes the information about the user, including the user name and all the group names, where the user belongs to. Cisco SD-WAN Manager matches the group names with the group names stored in the database to further distinguish if a particular group name passed from IdP is for user group or resource group or VPN group.

### Multi-Tenancy Support

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. The tenants share Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco SD-WAN Controller. The domain name of the service provider has subdomains for each tenant. Cisco SD-WAN Manager is deployed and configured by the service provider. The provider enables multitenancy and creates a Cisco SD-WAN Manager cluster to serve tenants. Only the provider can access a Cisco SD-WAN Manager instance through the SSH terminal.

Provider has the following features:

- resource group is not applicable as the provider manages only the controllers.
- when provider provisions a new tenant, the default user account for the tenant is tenantadmin.
- other user accounts created by the provider are included in the default global resource group.
- when a provider creates a template for a tenant, the template is included in to the global resource group.

# RBAC for Policies Overview

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

RBAC for policies allows a user or user group to have selective Read and Write (RW) access to Cisco SD-WAN Manager policies. For example,

- A user with RW access for Cflowd policy can only configure Cflowd policy, but cannot configure application-aware routing policy.
- A user with RW access for application aware routing policy can only configure application-aware routing policy, but cannot configure other policies.

This feature is only supported for centralized and localized policies, but not supported for security policies.

# Information About Granular RBAC for Templates

Minimum supported release: Cisco vManage Release 20.7.1

When setting user group permissions, you can use the following template permissions to provide an RBAC user with a specific degree of access to different types of templates. This gives you control over the types of device configurations that an RBAC user can apply.

| Permission | Description |
|---|---|
| CLI Add-On Template | Provides access to the CLI add-on feature template. |

| Permission | Description |
|---|---|
| Device CLI Template | Provides access to the device CLI template. |
| SIG Template | Provides access to the SIG feature template and SIG credential template. |
| Other Feature Templates | Provides access to all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template. |
| Feature Profile | Provides access to all feature profiles. |
| Config Group | Provides access to all the configuration groups. |

You can specify granular RBAC for each feature profile by expanding it. With the set permissions to the usergroup, ensure that you are able to access required feature profiles from **Templates** > **Configuration Groups**.

### Single-Tenant and Multi-Tenant Scenarios

You can use granular RBAC for feature templates in single-tenant and multi-tenant Cisco SD-WAN Manager scenarios.

You can create user groups to assign specific permissions to a tenant's various teams, enabling teams to manage only specific network services without granting permission to use device CLI templates. It might be undesirable to give a tenant permission to apply device CLI templates, as the device CLI template can override any other template or device configuration.

For example, you can create a user group for a tenant's security operations group, giving them read/write access only to the SIG Template option, which would enable the security operations group to work on security configuration.

# Information About Granular Configuration Task Permissions

From Cisco vManage Release 20.9.1, numerous user permission options are available, providing you fine granularity when assigning a user with permissions to manage specific configuration tasks related to configuration groups and feature profiles.

# Information About Assigning Roles Locally to a User Defined by an Identity Provider

Minimum release: Cisco vManage Release 20.11.1

When you define users in an identity provider, such as Okta, for SAML SSO, one attribute that you can define for each user is the role.

When a user logs in to a Cisco SD-WAN Manager instance, Cisco SD-WAN Manager retrieves information about the user from the identity provider, including the user’s role or roles. The roles defined in the identity provider map to user group permissions in Cisco SD-WAN Manager. Based on the roles of the user, Cisco SD-WAN Manager provides the user with the permissions defined by the corresponding user group.

You can assign roles locally (not depending on the identify provider) for a user profile that does not have a role defined in the identity provider.

If you have defined roles for a user through the identity provider and have also assigned user groups locally for the same user, the roles defined through the identity provider take priority.

The following table summarizes the ways to provide a user with specific permissions:

| Using or Not Using an Identity Provider for SAML SSO | Roles Defined in the Identity Provider | How User Permissions Are Defined |
|---|---|---|
| Not using an identity provider | Not applicable | In Cisco SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions. |
| Using an identity provider | Identity provider has one or more roles defined for the user. | Define roles for the user through the identity provider. Cisco SD-WAN Manager provides the user with the user group permissions corresponding to the roles. |
| | Identity provider does not have a role defined for the user. | Use the **Remote User** option when adding a user (**Administration** > **Manage Users** > **Add User**). See Add a User, on page 172.<br><br>In Cisco SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions. |

# Benefits of RBAC

## Benefits of Granular RBAC for Feature Templates

Minimum supported release: Cisco vManage Release 20.7.1

The permissions that you add for co-management are useful for providing detailed control over access to network configuration. They are useful when using Cisco Catalyst SD-WAN with tenants, enabling you to provide a tenant access to specific types of templates. This enables you to give the tenant self-management of network configuration tasks within the tenant's VPN.

For information about the permissions added for co-management, see Information About Granular RBAC for Templates, on page 143.

# Restrictions for RBAC

## Restrictions for Granular RBAC for Feature Templates

Minimum supported release: Cisco vManage Release 20.7.1

- To use any of the template restriction options that are provided for RBAC for co-management, provide permissions for the **Template Configuration** option. If a specific user role does not have any permissions assigned in the **Template Configuration** option, the **Templates** menu does not appear for the user in Cisco SD-WAN Manager. See Manage Users.

- To enable an RBAC user to apply templates to devices, provide **Write** permission to the **Template Deploy** option.

# Use Cases for RBAC

## Use Cases for Assigning Roles Locally to a User Defined by an Identity Provider

Minimum release: Cisco vManage Release 20.11.1

An organization uses the identity provider, Okta, to authenticate users logging in to Cisco SD-WAN Manager.

A user defined through the identity provider has not been assigned any roles. A network administrator with access to Cisco SD-WAN Manager, but no access to the identity provider, can locally assign the user to a specific user group to provide the user with specific permissions.

# Configure RBAC

## 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 47: 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 |

# User Group Permissions: Cisco IOS XE Catalyst SD-WAN device

*Table 48: User Group Permissions: Cisco IOS XE Catalyst SD-WAN devices*

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Alarms** | Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Logs** > **Alarms** page.<br><br>Cisco vManage Release 20.6.x and earlier: Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Alarms** page. | No additional permissions. |
| **Audit Log** | Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Logs** > **Alarms** page and the **Monitor** > **Logs** > **Audit Log** page.<br><br>Cisco vManage Release 20.6.x and earlier: Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Alarms** page and the **Monitor** > **Audit Log** page. | No additional permissions. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Certificates** | View a list of the devices in the overlay network under **Configuration** > **Certificates** > **WAN Edge List**.<br><br>View a certificate signing request (CSR) and certificate on the **Configuration** > **Certificates** > **Controllers** window.<br><br>**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding. | Validate and invalidate a device, stage a device, and send the serial number of valid controller devices to the Cisco Catalyst SD-WAN Validator on the **Configuration** > **Certificates** > **WAN Edge List** window.<br><br>Generate a CSR, install a signed certificate, reset the RSA key pair, and invalidate a controller device on the **Configuration** > **Certificates** > **Controllers** window.<br><br>**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding. |
| **CLI Add-On Template**<br><br>(Minimum supported release: Cisco vManage Release 20.7.1) | View the CLI add-on feature template on the **Configuration** > **Templates** window.<br><br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, delete, and copy a CLI add-on feature template on the **Configuration** > **Templates** window.<br><br>**Note** These operations require write permission for **Template Configuration**.<br><br>**Note** For information about this option, see Information About Granular RBAC for Feature Templates |
| **Cloud OnRamp** | View the cloud applications on the**Configuration** > **Cloud OnRamp for SaaS** and **Configuration** > **Cloud OnRamp for IaaS** window. | No additional permissions. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Cluster** | View information about the services running on Cisco SD-WAN Manager, a list of devices connected to a Cisco SD-WAN Manager server, and the services that are available and running on all the Cisco SD-WAN Manager servers in the cluster on the **Administration** > **Cluster Management** window. | Change the IP address of the current Cisco SD-WAN Manager, add a Cisco SD-WAN Manager server to the cluster, configure the statistics database, edit, and remove a Cisco SD-WAN Manager server from the cluster on the **Administration** > **Cluster Management** window. |
| **Colocation** | View the cloud applications on the **Configuration** > **Cloud OnRamp for Colocation** window. | No additional permissions. |
| **Config Group** > **Device** > **Deploy**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | This permission does not provide any functionality. | Deploy a configuration onto Cisco IOS XE Catalyst SD-WAN devices.<br>**Note** To edit an existing feature configuration requires write permission for **Template Configuration**.<br>For more details on deploying devices, see Deploy Devices. |
| **Device CLI Template**<br>(Minimum supported release: Cisco vManage Release 20.7.1) | View the device CLI template on the **Configuration** > **Templates** window.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, delete, and copy a device CLI template on the **Configuration** > **Templates** window.<br>**Note** These operations require write permission for **Template Configuration**.<br>**Note** For information about this option, see Information About Granular RBAC for Feature Templates |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Device Inventory** | View the running and local configuration of devices, a log of template activities, and the status of attaching configuration templates to devices on the **Configuration** > **Devices** > **WAN Edge List** window.<br><br>View the running and local configuration of the devices and the status of attaching configuration templates to controller devices on the **Configuration** > **Devices** > **Controllers** window.<br><br>**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding. | Upload a device's authorized serial number file to Cisco SD-WAN Manager, toggle a device from Cisco SD-WAN Manager configuration mode to CLI mode, copy a device configuration, and delete the device from the network on the **Configuration** > **Devices** > **WAN Edge List** window.<br><br>Add and delete controller devices from the overlay network, and edit the IP address and login credentials of a controller device on the **Configuration** > **Devices** > **Controllers** window.<br><br>**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Device Monitoring** | View the geographic location of the devices on the **Monitor** > **Geography** window.<br><br>View events that have occurred on the devices on the **Monitor** > **Logs** > **Events** page.<br><br>Cisco vManage Release 20.6.x and earlier: View events that have occurred on the devices on the **Monitor** > **Events** page.<br><br>View a list of devices in the network, along with device status summary, SD-WAN Application Intelligence Engine (SAIE) and Cflowd flow information, transport location (TLOC) loss, latency, and jitter information, control and tunnel connections, system status, and events on the **Monitor** > **Devices** page (only when a device is selected).<br><br>**Note** In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.<br><br>Cisco vManage Release 20.6.x and earlier: Device information is available in the **Monitor** > **Network** page. | Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Devices** page (only when a device is selected).<br><br>**Note** These operations require read and write permissions for **Device Monitoring**. |
| **Device Reboot** | View the list of devices on which the reboot operation can be performed on the **Maintenance** > **Device Reboot** window. | Reboot one or more devices on the **Maintenance** > **Device Reboot** window. |
| **Disaster Recovery** | View information about active and standby clusters running on Cisco SD-WAN Manager on the **Administration** > **Disaster Recovery** window. | No additional permissions. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Events** | View the geographic location of the devices on the **Monitor** > **Logs** > **Events** page.<br>View the geographic location of the devices on the **Monitor** > **Events** page. | Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Logs** > **Events** page (only when a device is selected). |
| **Feature Profile** > **Other** > **Thousandeyes**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **ThousandEyes** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **ThousandEyes** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Other Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Service** > **Dhcp**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **DHCP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **DHCP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Service** > **Lan/Vpn**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **LAN/VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **LAN/VPN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Service** > **Lan/Vpn/Interface/Ethernet**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Service** > **Lan/Vpn/Interface/Svi**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **SVI Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **SVI Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Service** > **Routing/Bgp**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Routing/BGP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Routing/BGP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Service** > **Routing/Ospf**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Service** > **Switchport**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Switchport** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Switchport** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Service** > **Wirelesslan**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Wireless LAN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Wireless LAN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **System** > **Interface/Ethernet** > **Aaa**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **AAA** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **AAA** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **System** > **Interface/Ethernet** > **Banner**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Banner** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Banner** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **System** > **Basic**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Basic** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Basic** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **System** > **Bfd**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **BFD** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **BFD** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **System** > **Global**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Global** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Global** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **System** > **Logging**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Logging** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Logging** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **System** > **Ntp**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **NTP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **NTP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **System** > **Omp**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **OMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **OMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **System** > **Snmp**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **SNMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **SNMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **Cellular Controller**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Cellular Controller** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Cellular Controller** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Transport** > **Cellular Profile**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Cellular Profile** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Cellular Profile** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **Management/Vpn**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Management VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Management VPN** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **Management/Vpn/Interface/Ethernet**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Management Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Management VPN and Management Internet Interface** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Transport** > **Routing/Bgp**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **BGP Routing** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **BGP Routing** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **Tracker**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Tracker** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Tracker** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **Wan/Vpn**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Transport** > **Wan/Vpn/Interface/Cellular**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **Wan/Vpn/Interface/Ethernet**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Integration Management** | View information about controllers running on Cisco SD-WAN Manager, on the **Administration** > **Integration Management** window. | No additional permissions. |
| **License Management** | View license information of devices running on Cisco SD-WAN Manager, on the **Administration** > **License Management** window. | On the **Administration** > **License Management** page, configure use of a Cisco Smart Account, choose licenses to manage, and synchronize license information between Cisco SD-WAN Manager and the license server. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Interface** | View information about the interfaces on a device on the **Monitor** > **Devices** > **Interface** page.<br>Cisco vManage Release 20.6.x and earlier: View information about the interfaces on a device on the **Monitor** > **Network** > **Interface** page | Edit **Chart Options** to select the type of data to display, and edit the time period for which to display data on the **Monitor** > **Devices** > **Interface** page. |
| **Application Monitoring**<br>(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1) | View the application health of the devices on the **Monitor** > **Applications** window. | View the application health of the devices on the **Monitor** > **Applications** window. |
| **Manage Users** | View users and user groups on the **Administration** > **Manage Users** window. | Add, edit, and delete users and user groups from Cisco SD-WAN Manager, and edit user group privileges on the **Administration** > **Manage Users** window. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Other Feature Templates**<br>(Minimum supported release: Cisco vManage Release 20.7.1) | View all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window.<br>**Note** This operation requires read permission for **Template Configuration**.<br>**Note** To check the mutual authentication option, you need read permission for certificates. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1) | Create, edit, delete, and copy all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window.<br>**Note** These operations require write permission for **Template Configuration**.<br>**Note** For information about this option, see Information About Granular RBAC for Feature Templates<br>**Note** To check the mutual authentication option, you need write permission for certificates. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1) |
| **Policy** | View the common policies for all Cisco Catalyst SD-WAN Controllers or devices in the network on the **Configuration** > **Policies** window. | Create, edit, and delete the common policies for all Cisco Catalyst SD-WAN Controllers or devices in the network on the **Configuration** > **Policies** window. |
| **Policy Configuration** | View the list of policies created and details about them on the **Configuration** > **Policies** window. | Create, edit, and delete the common policies for all theCisco Catalyst SD-WAN Controllers and devices in the network on the **Configuration** > **Policies** window. |
| **Policy Deploy** | View the current status of the Cisco Catalyst SD-WAN Controllers to which a policy is being applied on the **Configuration** > **Policies** window. | Activate and deactivate the common policies for all Cisco SD-WAN Manager servers in the network on the **Configuration** > **Policies** window. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **RBAC VPN** | View the VPN groups and segments based on roles on the **Monitor** > **VPN** page.<br>Cisco vManage Release 20.6.x and earlier: View the VPN groups and segments based on roles on the **Dashboard** > **VPN Dashboard** page. | Add, edit, and delete VPNs and VPN groups from Cisco SD-WAN Manager, and edit VPN group privileges on the **Administration** > **VPN Groups** window. |
| **Routing** | View real-time routing information for a device on the **Monitor** > **Devices** > **Real-Time** page.<br>Cisco vManage Release 20.6.x and earlier: View real-time routing information for a device on the **Monitor** > **Network** > **Real-Time** page. | Add command filters to speed up the display of information on the **Monitor** > **Devices** > **Real-Time** page. |
| **Security** | View the current status of the Cisco Catalyst SD-WAN Controllers to which a security policy is being applied on the **Configuration** > **Security** window. | Activate and deactivate the security policies for all Cisco SD-WAN Manager servers in the network on the **Configuration** > **Security** window. |
| **Security Policy Configuration** | Activate and deactivate the common policies for all Cisco SD-WAN Manager servers in the network on the **Configuration** > **Security** > **Add Security Policy** window. | Activate and deactivate the security policies for all Cisco SD-WAN Manager servers in the network on the **Configuration** > **Security** > **Add Security Policy** window. |
| **Session Management** | View user sessions on the **Administration** > **Manage Users** > **User Sessions** window. | Add, edit, and delete users and user groups from Cisco SD-WAN Manager, and edit user sessions on the **Administration** > **Manage Users** > **User Sessions** window. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Settings** | View the organization name, Cisco Catalyst SD-WAN Validator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the Cisco SD-WAN Manager login page, and the current settings for collecting statistics on the **Administration** > **Settings** window. | Edit the organization name, Cisco Catalyst SD-WAN Validator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the Cisco SD-WAN Manager login page, current settings for collecting statistics, generate a certificate signing request (CSR) for a web server certificate, and install a certificate on the **Administration** > **Settings** window. |
| **SIG Template**<br>(Minimum supported release: Cisco vManage Release 20.7.1) | View the SIG feature template and SIG credential template on the **Configuration** > **Templates** window.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, delete, and copy a SIG feature template and SIG credential template on the **Configuration** > **Templates** window.<br>**Note** These operations require write permission for **Template Configuration**.<br>**Note** For information about this option, see Information About Granular RBAC for Feature Templates |
| **SIG Tunnels**<br>(Minimum supported release: Cisco vManage Release 17.12) | View information about the SIG tunnels on the **Monitor** > **Tunnels** > **SIG Tunnels** page. | View information about the SIG tunnels on the **Monitor** > **Tunnels** > **SIG Tunnels** page. |
| **Software Upgrade** | View a list of devices,the custom banner on Cisco SD-WAN Manager on which a software upgrade can be performed, and the current software version running on a device on the **Maintenance** > **Software Upgrade** window. | Upload new software images on devices, upgrade, activate, and delete a software image on a device, and set a software image to be the default image on devices on the **Maintenance** > **Software Upgrade** window. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **System** | View system-wide parameters configured using Cisco SD-WAN Manager templates on the **Configuration** > **Templates** > **Device Templates** window.<br>**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**. | Configure system-wide parameters using Cisco SD-WAN Manager templates on the **Configuration** > **Templates** > **Device Templates** window.<br>**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**. |
| **Template Configuration** | View feature and device templates on the **Configuration** > **Templates** window. | Create, edit, delete, and copy a feature or device template on the **Configuration** > **Templates** window.<br>**Note** Beginning with Cisco vManage Release 20.7.1, to create, edit, or delete a template that is already attached to a device, the user requires write permission for the Template Deploy option. |
| **Template Deploy** | View the devices attached to a device template on the **Configuration** > **Templates** window. | Attach a device to a device template on the **Configuration** > **Templates** window. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Tools** | Use the **admin tech** command to collect the system status information for a device on the **Tools** > **Operational Commands** window. | Use the **admin tech** command to collect the system status information for a device, and use the **interface reset** command to shut down and then restart an interface on a device in a single operation on the **Tools** > **Operational Commands** window.<br><br>Rediscover the network to locate new devices and synchronize them with Cisco SD-WAN Manager on the **Tools** > **Operational Commands** window.<br><br>Establish an SSH session to the devices and issue CLI commands on the **Tools** > **Operational Commands** window. |
| **vAnalytics** | Launch Cisco SD-WAN Analytics on > **vAnalytics** window. | No additional permissions. |
| **Workflows** | Launch workflow library from > **Workflows** window. | No additional permissions. |
| **Config Group** > **Device** > **Deploy**<br><br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the devices associated to a configuration group on the **Configuration** > **Templates** > **Edit Configuration Group** > **Associated Devices** window. | Deploy a configuration onto Cisco IOS XE Catalyst SD-WAN devices.<br><br>**Note** To edit an existing feature configuration requires write permission for **Template Configuration**.<br><br>For more details on deploying devices, see Deploy Devices. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Transport** > **IPv4 Tracker and Tracker Group**<br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the IPv4 Tracker and Tracker Group settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **IPv4 Tracker and Tracker Group** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **IPv6 Tracker and Tracker Group**<br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the IPv6 Tracker and Tracker Group settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **IPv6 Tracker and Tracker Group** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Transport** > **Gps**<br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the GPS settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Gps** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Other** > **APPQoE**<br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the APPQoE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **APPQoE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Other** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Other** > **UCSE**<br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the UCSE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **UCSE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Other** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Wan Profile** > **Cisco VPN Interface IPSec**<br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the Cisco VPN Interface IPSec settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Wan Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Cisco VPN Interface IPSec** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Wan Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |
| **Feature Profile** > **Wan/Lan Profile** > **Cisco VPN Interface GRE**<br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the Cisco VPN Interface GRE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Wan/Lan Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Cisco VPN Interface GRE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Wan/Lan Profile** section.<br>**Note** These operations require write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Lan Profile** > **Cisco Multicast**<br><br>(Minimum supported release: Cisco vManage Release 20.11.1) | View the Cisco Multicast settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Lan Profile** section.<br><br>**Note** This operation requires read permission for **Template Configuration**. | Create, edit, and delete the **Cisco Multicast** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Lan Profile** section.<br><br>**Note** These operations require write permission for **Template Configuration**. |

**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 configuring features using Configuration Groups, see Feature Management.

# User Group Permissions: Cisco Catalyst Wireless Gateway Devices

*Table 49: User Group Permissions: Cisco Catalyst Wireless Gateway Devices*

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Teleworker** > **Basic**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the basic settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Configure tthe basic settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires write permission for **Template Configuration**. |
| **Feature Profile** > **Teleworker** > **Cellular**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the cellular network settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Configure the cellular network settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires write permission for **Template Configuration**. |
| **Feature Profile** > **Teleworker** > **Ethernet**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the ethernet settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Configure the ethernet settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires write permission for **Template Configuration**. |

| Feature | Read Permission | Write Permission |
|---|---|---|
| **Feature Profile** > **Teleworker** > **NetworkProtocol**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the network protocol settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Configure the network protocol settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires write permission for **Template Configuration**. |
| **Feature Profile** > **Teleworker** > **SecurityPolicy**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the security policy settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Configure the security policy settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires write permission for **Template Configuration**. |
| **Feature Profile** > **Teleworker** > **Vpn**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the VPN settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Configure the VPN settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires write permission for **Template Configuration**. |
| **Feature Profile** > **Teleworker** > **Wifi**<br>(Minimum supported release: Cisco vManage Release 20.9.1) | View the Wi-Fi settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires read permission for **Template Configuration**. | Configure the Wi-Fi settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section.<br>**Note** This operation requires write permission for **Template Configuration**. |

# RBAC User Group in a Multitenant Environment

The following is the list of user group permissions for role-based access control (RBAC) in a multitenant environment:

- R stands for read permission.
- W stands for write permission.

***Table 50: RBAC User Group in Multitenant Environment***

| Feature | Provider Admin | Provider Operator | Tenant Admin | Tenant Operator |
|---|---|---|---|---|
| Cloud OnRamp | RW | R | RW | R |
| Colocation | RW | R | RW | R |
| RBAC VPN | RW | R | RW | R |
| Security | RW | R | RW | R |
| Security Policy Configuration | RW | R | RW | R |
| vAnalytics | RW | R | RW | R |

# Add a User

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
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. 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. If no roles are defined for the user through the identity provider, you can enable the **Remote User** option and assign user groups locally in Cisco SD-WAN Manager. Assigning user groups locally provides an alternate method for assigning the user with permissions.

   If you enable this option, enter an email address for the user.

   If you have defined roles for a user through the identity provider and have also assigned user groups locally for the same user, the roles defined through the identity provider take priority.

**Note** This option is available from Cisco vManage Release 20.11.1.

7. In the **User Groups** drop-down list, select the user group where you want to add a user.

8. In 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.

9. Click **Add**.

# Delete a User

If a user no longer needs access to devices, you can delete the user. Deleting a user does not log out the user if the user is logged in.

To delete a user:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. For the user you wish to delete, click **...**, and click **Delete**.
3. To confirm the deletion of the user, click **OK**.

# Edit User Details

You can update login information for a user, and add or remove a user from a user group. If you edit the details of a user who is logged in, the changes take effect after the user logs out.

To edit user details:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. For the user you wish to edit, click **...**, and click **Edit**.
3. Edit the user details.

   You can also add or remove the user from user groups.
4. Click **Update**.

# Change a User Password

You can update passwords for users, as needed. We recommend that you use strong passwords.

**Before You Begin**

If you are changing the password for an admin user, detach device templates from all Cisco SD-WAN Manager instances in the cluster before you perform this procedure. You can reattach the device templates after you complete this procedure.

To change a password for a user:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. For the user you wish to change the password, click **...** and click **Change Password**.
3. Enter the new password, and then confirm it.

**Note** Note that the user, if logged in, is logged out.

4. Click **Done**.

# Check Users Logged In to a Device Using SSH Sessions

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. Select the device you want to use under the **Hostname** column.
3. Click **Real Time**.
4. From **Device Options**, choose **AAA users** for Cisco IOS XE Catalyst SD-WAN devices.

   A list of users logged in to this device is displayed.

# Check Users Logged In to a Device Using HTTP Sessions

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Sessions**.

   A list of all the active HTTP sessions within Cisco SD-WAN Manager is displayed, including, username, domain, source IP address, and so on.

# 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.

## Create User Groups

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. Click **Add User Group**.
4. Enter **User Group Name**.

5. Select the **Read** or **Write** check box against feature that you want to assign to a user group.
6. Click **Add**.
7. You can view the new user group in the left navigation path. Click **Edit** to edit the existing read or write rules.
8. Click **Save**.

# Configure and Manage VPN Segments

To configure VPN Segments:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **VPN Segments**. A web page displays the list of segments that are configured.
2. To edit or delete an existing segment, click **…**, and click **Edit** or **Delete**.
3. To add new segment, click **Add Segment**.
4. Enter the name of the segment in the **Segment Name** field.
5. Enter the number of VPNs you want to configure in **VPN Number** field.
6. To add a new segment, click **Add**.

# Configure and Manage VPN Groups

To configure VPN Groups:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **VPN Groups**. A web page displays the list of segments that are configured.
2. To edit or delete a VPN group, click **…**, and click **Edit** or **Delete**.
3. To view the existing VPN in the dashboard, click **…**, and click **View Dashboard**. The **VPN Dashboard** displays the device details of the VPN device configured.
4. To add new VPN group, click **Add Group**.
5. From **Create VPN Group**, enter VPN group name in the **VPN Group Name** field.
6. Enter a brief description of the VPN in the **Description** field.
7. Check **Enable User Group access** check box and enter the user group name.
8. From **Assign Segment**, click **Add Segment** drop-down list to add new or existing segment to the VPN group.
9. Enter the **Segment Name** and **VPN Number** in the respective fields.
10. To add the configure VPN group to a device, click **Add**.

# 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**.

# Workflow 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 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.

## 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.

## Configure Granular RBAC for Feature Templates

Minimum supported release: Cisco vManage Release 20.7.1

To configure specific template access, create a user group and assign the read and write permissions using the permission types described in Information About RBAC for Co-Management. The permission options for limiting template access appear with the other permission options that you choose when adding a user group.

For information about granular RBAC for feature templates, see Information About Granular RBAC for Templates, on page 143.

For information about adding a user group, see Create User Groups.

For a list of permission types and descriptions, see Manage Users.

# Configure RBAC Using the CLI

## Configure Users Using CLI

You can use the CLI to configure user credentials on each device. This way, you can create additional users and give them access to specific devices. The credentials that you create for a user by using the CLI can be different from the Cisco SD-WAN Manager credentials for the user. In addition, you can create different credentials for a user on each device. All Cisco IOS XE Catalyst SD-WAN device users with the **netadmin** privilege can create a new user.

To create a user account, configure the username and password, and place the user in a group:

This example, shows the addition of user, Bob, to an existing group:

```
Device(config)# system aaa user bob group basic
```

This example, shows the addition of user, Alice, to a new group `test-group`:

```
Device(config)# system aaa user test-group
Device(config)# system aaa user alice group test-group
```

The Username can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. Because some usernames are reserved, you cannot configure them. For a list of reserved usernames, see the **aaa** configuration command in the Cisco Catalyst SD-WAN Command Reference Guide.

The Password is the password for a user. Each username must have a password, and users are allowed to change their own password. The CLI immediately encrypts the string and does not display a readable version of the password. When a user logs in to a Cisco IOS XE Catalyst SD-WAN device, they have five chances

to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and must wait for 15 minutes before attempting to log in again.

**Note** Enclose any user passwords that contain the special character ! in double quotation marks (“ “). If a double quotation is not included for the entire password, the config database (?) treats the special character as a space and ignores the rest of the password.

For example, if the password is C!sc0, use “C!sc0”.

Group name is the name of a standard Cisco Catalyst SD-WAN group (**basic**, **netadmin**, or **operator**) or of a group configured with the **usergroup** command (discussed below). If an admin user changes the permission 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.

The factory-default password for the admin username is admin. We strongly recommend that you modify this password the first time you configure a Cisco IOS XE Catalyst SD-WAN device:

```
Device(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

Configure the password as an ASCII string. The CLI immediately encrypts the string and does not display a readable version of the password, for example:

```
Device# show run | sec username
username admin privilege 15 secret 9
$9$3F2M2l2G2/UM3U$TGe2kqoIibdIRDEj4cOVKbVFP/o4vnlFAwWnmzx1rRE
username appnav privilege 15 secret 9
$9$3l2L2V.F2VIM1k$p3MBAyBtGxKf/yBGnUSHQ1g/ae1QhfIbieg28buJJGI
username eft secret 9 $9$3FMJ3/UD2VEL2E$d.kE4.an41v7wEhrQc6k5wIfE9M9WkNAJxUvbbempS.
username lab privilege 15 secret 9
$9$3l.J3FUD2F.E2.$/AiVn9PmLCpgr6ExVrE7dH979Wu8nbdtAfbzUtfysg.
username test secret 9 $9$1l2J3l6D3/QL3k$7PZOXJAJOI1os5UI763G3XcpVhXlqcwJ.qEmgmx4X9g
username vbonagir privilege 15 secret 9
$9$3/2K2UwF2lQF3U$VbdQ5bq18590rRthF/NnNnOsw.dw1/EViMTFZ5.ctus
Device#
```

If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to verify the password:

```
Device(config)#  radius server tag
```

The tag is a string that you defined with the **radius server tag** command, as described in the Cisco Catalyst SD-WAN Command Reference Guide.

# Creating Groups Using CLI

The Cisco Catalyst SD-WAN software provides default user groups: **basic**, **netadmin**, **operator**, **network_operations**, and **security_operations**. The username **admin** is automatically placed in the **netadmin** usergroup.

If needed, you can create additional custom groups and configure privilege roles that the group members have. To create a custom group with specific authorization, configure the group name and privileges:

```
Device(config)# aaa authentication login user1 group radius enable
Device(config)# aaa authentication login user2 group radius enable
Device(config)# aaa authentication login user3 group radius enable
Device(config)#
```

*group-name* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters Some group names are reserved, so you cannot configure them. For a list of them, see the aaa configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the user group **basic**. If a remote server validates authentication and specifies a user group (say, X) using VSA Cisco SD-WAN-Group-Name, the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

In the **task** option, list the privilege roles that the group members have. The role can be one or more of the following: **interface**, **policy**, **routing**, **security**, and **system**.

# Verify RBAC

## 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.

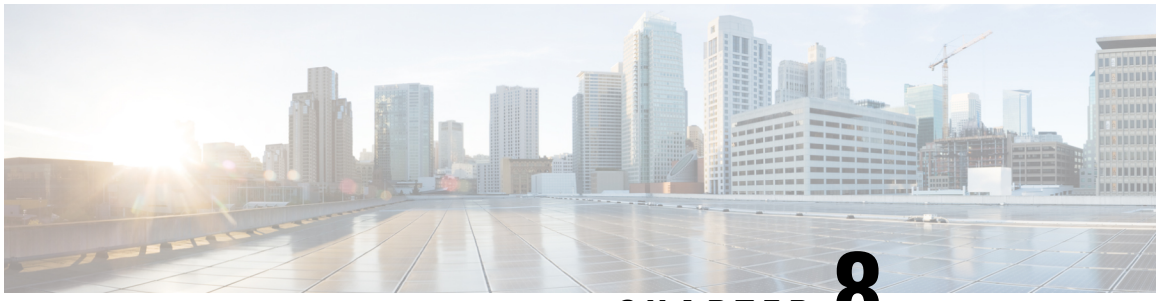
# Monitor RBAC

## Monitor devices for VPN Groups

To monitor devices:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Click **WAN - Edge**.
3. Select the **VPN Group** and **VPN Segment** for which you want to monitor the network.

   A web page displays the list of VPN groups and segments that are configured to a device.



CHAPTER 8

# 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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

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.


- Device Configuration Workflow, on page 183
- Feature Templates, on page 184
- Device Templates, on page 185
- Template Variables, on page 185
- Configuration Prerequisites, on page 185
- Create a Device Template from Feature Templates, on page 186
- Default Device Templates, on page 204
- Configuring Devices using Cisco SD-WAN Manager, on page 205


# 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**.

# 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 Templates

You 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.)

Device templates contain complete operational configuration for a device. You create device templates by consolidating individual feature templates.

Each device template is specific for a type of device. For each device type, if multiple devices have the same configuration, you can use the same device template for them. For example, many of the routers in a network might have the same basic configuration, so you can configure them with the same templates. (You specify the differences in the templates using configuration variables, which are discussed below.) If the configurations for the same type of devices are different, you create separate device templates.

You can also create a device template by entering a CLI text-style configuration directly on Cisco SD-WAN Manager. Typically, you upload a text file containing the configuration text (or cut the configuration text from a text file and paste it into Cisco SD-WAN Manager). You can also directly type the configuration text into Cisco SD-WAN Manager.

From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, you can review your last edited configuration when your latest configuration is not being pushed to the device. For more information, see Edit a Device Template When a Push Fails , on page 201.

From Cisco vManage Release 20.5.1, device variable page shows text area instead of text input field to configure CLI device template for the ease of configuration.

# 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 51:*

| 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.<br><br>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.<br><br>To change the default key, type a new string and move the cursor out of the **Enter Key** box.<br><br>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.<br><br>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.

# Manage Device Templates

*Table 52: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support for Draft Mode in Device Template | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>Cisco vManage Release 20.5.1 | This feature allows you to save the device template configuration changes in Cisco SD-WAN Manager, and then apply these configuration changes to multiple Cisco IOS XE Catalyst SD-WAN devices later. The ability to save configuration changes simplifies generating larger device template configurations and applying them to devices. |

### 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**.

# 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.

# 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**.

# 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**.

# 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.

# Edit a Device Template When a Push Fails

*Table 53: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Retrieve Last Edited Configuration | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>Cisco vManage Release 20.5.1 | This feature allows you to review the last edited configuration when a configuration push to the device fails. A copy of the last edited configuration is saved and can be retrieved to allow edits to the configuration before the next push. |

If you pushed a configuration to a device, and if the push fails, you can review the configuration you last edited to identify any issues that caused a failure in pushing the configuration to the device.

### Prerequisites

To review your last edited configuration, a device template must be attached to a device.

## Review Last Edited Configuration in Cisco SD-WAN Manager

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.

# Change the Device Rollback Timer

By default, when you attach a Cisco IOS XE Catalyst SD-WAN device to a configuration template, if the router is unable to successfully start after 5 minutes, it returns to, or rolls back to, the previous configuration. For a configuration that you have created from the CLI, you can change the device's rollback timer:

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 click **Change Device Values**.

   The right pane displays the device's configuration, and the **Config Preview** tab is selected.
4. In the left pane, click the name of a device.
5. Click **Configure Device Rollback Timer**. The **Configure Device Rollback Time** pop up page is displayed.
6. From the **Devices** drop-down list, select a device.
7. 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.
8. To disable the rollback timer, click **Enable Rollback slider**. When you disable the timer, the **Password** field dialog box appears. Enter the password that you used to log in to Cisco SD-WAN Manager.
9. 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.
10. To exclude a device from the rollback timer setting, click **Add Exception** and select the devices to exclude.
11. The table 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 of the device name.
12. Click **Save**.
13. Click **Configure Devices** to push the configuration to the devices. The **Status** column displays whether the configuration was successfully pushed. Click **(+)** to display details of the push operation.

# 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.

# Change Variable Values for a Device

For a configuration that you have created from device configuration templates, if the templates contain variables, Cisco SD-WAN Manager can automatically populate the variables with actual values when you attach the templates to the devices. To do this, you create an Excel file that lists the variable values for each device and save the file in CSV format. You can also enter values for these variables manually.

After you have pushed the configuration to a device, you can change the value assigned to any variable:

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 screen displays a table of all the devices that are attached to that device template.

4. For the desired device, click **...**, and click **Edit Device Template**.

5. In the **Update Device Template** dialog box, enter values for the items in the variable list.

6. Click **Update**.

7. Click **Next**.

8. Click **Configure Devices** to push the configuration to the device. The Status column displays if the configuration was successfully pushed or not. Click the right angle bracket to display the details of the push operation.

# Default Device Templates

*Table 54: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Default Device Templates | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | A default device template provides basic information that you can use to bring up devices in a deployment quickly.<br><br>This feature is supported on the Cisco Cloud Services Router 1000V Series, Cisco C1111-8PLTELA Integrated Services Routers, and Cisco 4331 Integrated Services Routers. |

A default device template provides basic information that you can use to bring up devices in a deployment. It provides a way for you to quickly provision devices with the minimum information that they need to operate in your network.

You cannot directly edit or update information in a device default template, but you can copy the template and then edit the copy.

To use a default 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. From the **Template Type** drop-down list, select **Default**.

   A list of default device templates displays.
4. Perform any of these actions:
   - To attach a default device template to devices, click **...**, and select **Attach Devices**.

     In the **Attach Devices** dialog box, select the devices that you want attach, and then click **Attach**.
   - To view the configuration settings for a default device template, click **...**, and choose **View**.
   - To copy a default device template, click **...**, and choose **View**.

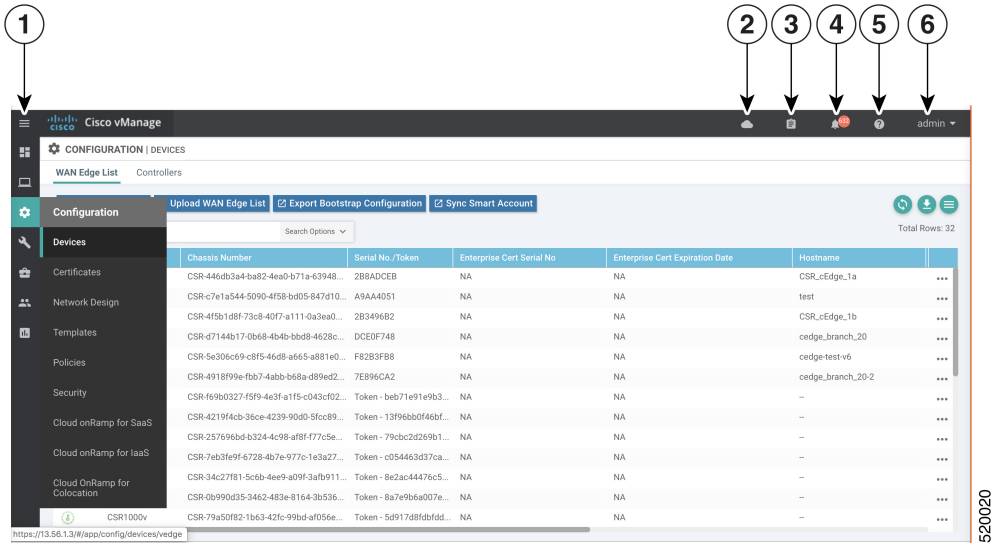
     In the **Template Copy** dialog box, enter a unique name and a description for the copy that you are creating, and then click **Copy**.

     The copied version becomes a feature template that you can edit.
   - To create an Excel file in CSV format that contains device-specific settings from a device template, click **...**, and choose **Export CSV**. Use the dialog box that displays to open or save the CSV file.

You can use this CSV file as a reference for device-specific settings when you create other device templates.

# Configuring Devices using Cisco SD-WAN Manager

Use the **Devices** screen to add and delete devices, toggle the mode of a device between CLI and Cisco SD-WAN Manager, upload the WAN Edge Serial number file, export bootstrap configuration and, and perform other device-related tasks.




| | |
|---|---|
| 1 | Menu |
| 2 | CloudExpress |
| 3 | Tasks |
| 4 | Alarms |
| 5 | Help |
| 6 | User Profile |

# 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.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

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 **Manager 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.

# Upload WAN Edge Router Authorized Serial Number File

*Table 55: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Remove Certificate SUDI requirement | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>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.

# 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.

**Note** Starting from Cisco IOS XE Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

Cisco SD-WAN Manager downloads all data from the device table to an Excel file in CSV format.

# 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.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

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.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

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**.

# Delete a WAN Edge Router

Delete a router if you need to remove it from your deployment. Doing so removes from the WAN edge router serial number list any of the following items that are stored for the router:

- Chassis number
- Certificate serial number
- Subject SUDI serial number

**Note** Deleting a router also permanently removes the router configuration from Cisco SD-WAN Manager.

To delete a router:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Mark the WAN Edge router as invalid.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
4. Click **WAN Edge List**, and select the router.
5. Click **...**, and click **Delete WAN Edge**.
6. To confirm deletion of the device, click **OK**.
7. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
8. Click **Send to Controller**.

# Decommission a Cloud Router

Decommissioning a cloud router (such as a Cisco Cloud Services Router 1000V) removes the device's serial number from Cisco SD-WAN Manager and generates a new token for the device. To do so:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List**, and select a cloud router.
3. Click **…**, and click **Decommission WAN Edge**.
4. To confirm the decommissioning of the router, click **OK**.

# View Template Log and Device Bringup

### View Log of Template Activities

A log of template activities contains information that relates to creating, editing, and deleting configuration templates, and the status of attaching configuration templates to devices. This information can be useful for troubleshooting.

To view a log of template activities:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List** or **Controllers**, and select the device.

**Note** Starting from Cisco IOS XE Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the Controllers tab is renamed as the Control Components tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

3. Click **…**, and click **Template Log**.

### View Status of Device Bringup

You can view the status of the operations involved in bringing a router or controller up in the overlay network. This information can help you monitor these operations.

To view the status of a device bringup:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List** or **Controllers**, and select the device.

**Note** Starting from Cisco IOS XE Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the Controllers tab is renamed as the Control Components tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

3. Click **…**, and click **Device Bring Up**.

# Add a Cisco SD-WAN Validator

A Cisco Catalyst SD-WAN Validator automatically orchestrates connectivity between Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager. If any Cisco IOS XE Catalyst SD-WAN device or Cisco Catalyst SD-WAN Controller is behind a NAT, the Cisco Catalyst SD-WAN Validator also serves as an initial NAT-traversal orchestrator. To add a Cisco Catalyst SD-WAN Validator:

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

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN.

3. Click **Add Validator**.
4. In the **Add Validator** window:
   a. Enter **Validator Management IP Address** of the Cisco SD-WAN Validator.
   b. Enter the **Username** and **Password** to access the Cisco SD-WAN Validator.

c. To allow the certificate-generation process to occur automatically, check the **Generate CSR** check box.

d. Click **Add**.

5. Repeat Steps 2, 3 and 4 to add additional Cisco Catalyst SD-WAN Validators.

The new Cisco Catalyst SD-WAN Validator is added to the list of controllers in the Controllers screen.

# 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**.

**Note** Cisco IOS XE Catalyst SD-WAN Release Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

3. Click **Add Controller**.
4. In the **Add Controller** 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.

**Note** Cisco IOS XE Catalyst SD-WAN Release Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

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.

**Note** Cisco IOS XE Catalyst SD-WAN Release Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

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.

**Note** Cisco IOS XE Catalyst SD-WAN Release Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

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 **Proxy**. Go to **Reverse Proxy**, and enable **Reverse Proxy**. Click **Save**.

# Create a UCS-E Template

***Table 56: Feature History***

| Feature Name | Release Information | Feature Description |
|---|---|---|
| Create a UCS-E Template | Cisco IOS XE Catalyst SD-WAN Release 16.12.1b | This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template. |

For more information about the Cisco Unified Computing System (UCS) E-Series Servers, see the Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Hardware Installation Guide.

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 Cisco IOS XE Catalyst SD-WAN device from the list.
5. From the **Other Templates** section, click **UCSE**.

   The UCSE Feature template opens. The top of the form contains fields for naming the template, and the bottom contains fields for configuring the Integrated Management Controller (IMC).
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.

## Configure Bay and Slot for Template

Click the Basic Configuration tab to configure the bay and the slot for the template.

| Parameter Name | Description |
|---|---|
| Bay | Specify the number for the SAS drive bays. |
| Slot | Specify the slot numbers for the mezzanine adapters. |

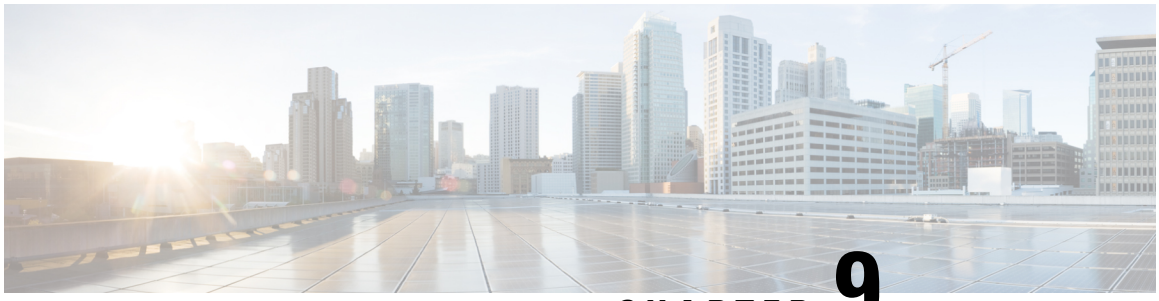
## IMC Configuration

Click the IMC tab to configure the IMC parameters for the template.

| Parameter Name | Description |
|---|---|
| Access Port | Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN.<br>Not all hardware models have a dedicated access port. See the Release Notes for your Cisco Catalyst SD-WAN release for the supported hardware.<br>Available options:<br>• Dedicated<br>• Shared<br>The type of port, GE or TE, depends on the hardware model.<br>For example:<br>`Router(config-ucse)#imc access-port shared-lom ?`<br>`GE1 GE1`<br>`TE2 TE2`<br>`TE3 TE3`<br>`console Console`<br>`failover Failover`<br>Some hardware models have GE ports whereas some have TE ports.<br>Depending on the hardware module, the appropriate port (GE or TE) needs to be configured. Otherwise you will get an error.<br>• You can obtain the UCS-E module hardware model type by using the following commands:<br>**show inventory**<br>**show platform**<br>• Failover - sub-option under Shared.<br>For example:<br>`Router(config)#ucse subslot 1/0`<br>`Router(config-ucse)#imc access-port ?`<br>`MGMT MGMT Interface`<br>`shared-lom Shared LOM`<br>`Router(config-ucse)#imc access-port shared-lom ?`<br>`GE1 GE1`<br>`TE2 TE2`<br>`TE3 TE3`<br>`console Console`<br>`failover Failover` |
| IPv4 Address | Provide the UCS-E management port address. |

| Parameter Name | Description |
|---|---|
| Default Gateway | Gateway tracking determine, for static routes, whether the next hop is reachable before adding that route to the device's route table.<br>Default: Enabled. |
| VLAN ID | Provide the VLAN number, which can be a value from 1 through 4094. |
| Assign Priority | Assign the priority. |

| Parameter Scope | Scope Description |
|---|---|
| Global (indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices. |
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter.<br>For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template.<br>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 Catalyst SD-WAN device to a device template.<br>To change the default key, type a new string and move the cursor out of the Enter Key box. |
| Default | When Default is selected, this field is not enabled. |



CHAPTER 9

# Configuration Groups and Feature Profiles

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 57: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Configuration Groups and Feature Profiles | Cisco IOS XE Catalyst SD-WAN Release 17.8.1a<br>Cisco vManage Release 20.8.1 | This feature provides a simple, reusable, and structured approach for the configurations in Cisco Catalyst SD-WAN. You can create a configuration group, that is, a logical grouping of features or configurations that is applied to one or more devices in the network that is managed by Cisco Catalyst SD-WAN. You can also create profiles based on features that are required, recommended, or uniquely used, and then combine the profiles to complete a device configuration.<br>The configuration group workflow in Cisco SD-WAN Manager provides a guided method to create configuration groups and feature profiles. |

| Feature Name | Release Information | Description |
|---|---|---|
| Configuration Groups and Feature Profiles (Phase II) | Cisco IOS XE Catalyst SD-WAN Release 17.9.1a<br>Cisco vManage Release 20.9.1 | The following enhancements are introduced in the Configuration Group feature.<br>• Adds support for the following features:<br>  • SNMP<br>  • Cellular Interface<br>  • BGP Routing (transport and management profile)<br>  • Wireless LAN<br>  • Switch Port<br>  • SVI Interface<br>  • DHCP Server<br>  • ThousandEyes<br>• Adds IPv6 configuration support in the VPN, interface, and BGP features.<br>• Adds the following options to the global settings that are a part of the system profile. These options have been added to the **Other Settings** tab.<br>  • Generate keepalive timers when incoming or outgoing network connections are idle<br>  • Enable small TCP and UDP servers<br>  • Enable console logging<br>  • Enable IP source routing<br>  • Display log messages to a VTY session<br>  • Enable SNMP IFINDEX persistence<br>  • Enable BOOTP server |
| Create Configuration Group Workflow for a Single-Router Site | Cisco IOS XE Catalyst SD-WAN Release 17.9.1a<br>Cisco vManage Release 20.9.1 | This feature introduces the Create Configuration Group workflow. This simplified workflow consolidates the various settings pages into a single page so that you can easily review your configuration at once. The workflow also enables you to set up WAN and LAN routing in addition to the basic settings, at the time of creating a configuration group. As a result, a configuration that is created from the workflow is now immediately deployable. |

| Feature Name | Release Information | Description |
|---|---|---|
| Security Feature Profile in Configuration Groups | Cisco vManage Release 20.10.1<br>Cisco IOS XE Catalyst SD-WAN Release 17.10.1a | This feature enables you to configure a security profile in configuration groups. |
| Localized Policy for QoS, ACL, and Routing | Cisco vManage Release 20.10.1<br>Cisco IOS XE Catalyst SD-WAN Release 17.10.1a | This feature enables you to configure a policy profile, a QoS map policy, a route policy, and an ACL policy through feature profiles.<br>The following enhancements are introduced in this feature:<br>• Policy objects under policy profiles:<br>  • AS Path<br>  • Standard Community<br>  • Expanded Community<br>  • Data Prefix<br>  • Extended Community<br>  • Class Map<br>  • Mirror<br>  • Policer<br>  • Prefix<br>• QoS map policy under Service and Transport profiles<br>• Route policy under Service and Transport profiles<br>• ACL policy under Service and Transport profiles |
| Variables and Type 6 Encryption in CLI Profile | Cisco vManage Release 20.10.1<br>Cisco IOS XE Catalyst SD-WAN Release 17.10.1a | After you enter or import configuration into a CLI profile, you can convert certain values to device-specific variables or encrypt strings such as passwords, using Type 6 encryption. |

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Catalyst SD-WAN Remote Access Configuration | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>Cisco vManage Release 20.11.1 | This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device, using Cisco SD-WAN Manager. Configure Remote Access in the System feature profile in a configuration group.<br>• Private IP Pool<br>• Authentication<br>• AAA Policy<br>• IKEv2 Settings<br>• IPSec Settings |
| Device Variables Option | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>Cisco vManage Release 20.11.1 | This feature enables you to modify system IP or site ID details of the device from the Associate Devices page while deploying devices. |

| Feature Name | Release Information | Description |
|---|---|---|
| Configuration Groups and Feature Profiles (Phase III) | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>Cisco vManage Release 20.11.1 | The following new features are introduced to the feature profiles:<br>• In the System Profile:<br>  • Cisco Security<br>  • IPV4-Device-Access-Policy<br>  • IPV6-Device-Access-Policy<br>  • Remote Access<br>• In the Transport Profile<br>  • OSPF Routing<br>  • VPN Interface GRE<br>  • IPSEC<br>  • Tracker Group<br>  • IPv6 Tracker<br>  • IPv6 Tracker Group<br>  • GPS<br>• In the Service Profile<br>  • VPN Interface GRE<br>  • IPSEC<br>  • Tracker<br>  • Tracker Group<br>  • AppQoE<br>  • Multicast<br>• In the Other Profile<br>  • UCSE |
| Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br>Cisco Catalyst SD-WAN Manager Release 20.12.1 | This feature enables you to configure the following Cisco Catalyst SD-WAN Remote Access features for a device in SSL-VPN mode, using Cisco SD-WAN Manager:<br>• Private IP Pool<br>• Authentication<br>• AAA Policy |

| Feature Name | Release Information | Description |
|---|---|---|
| Configuration Groups and Feature Profiles (Phase IV) | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br><br>Cisco Catalyst SD-WAN Control Components Release 20.12.1 | |

| Feature Name | Release Information | Description |
|---|---|---|
| | | The following new features are introduced to the feature profiles:<br>• In the System Profile:<br>• Flexible Port Speed<br>• In the Transport Profile:<br>• OSPFv3 IPv4 Routing<br>• OSPFv3 IPv6 Routing<br>• T1/E1 Controller<br>• Subfeatures for transport VPN:<br>• OSPFv3 IPv4 Routing<br>• OSPFv3 IPv6 Routing<br>• T1/E1/Serial<br>• DSL PPPoE<br>• DSL PPPoA<br>• DSL IPoE<br>• Ethernet PPPoE<br>• In the Service Profile:<br>• OSPFv3 IPv4 Routing<br>• OSPFv3 IPv6 Routing<br>• EIGRP Routing<br>• Object Tracker<br>• Object Tracker Group<br>• Subfeatures for service VPN:<br>• OSPFv3 IPv4 Routing<br>• OSPFv3 IPv6 Routing<br>• EIGRP Routing<br>• Multilink Controller<br>• Object Tracker<br>• Object Tracker Group<br>The **Route leak to Global VPN** option is added to the |

| Feature Name | Release Information | Description |
|---|---|---|
| | | **Route Leak** parameter in the service VPN |
| Support for Dual Device Site Configuration | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br>Cisco Catalyst SD-WAN Manager Release 20.12.1 | This feature supports dual devices site configuration in the configuration groups workflow. You can select the dual router type configuration group workflow to deploy two devices in the same site considering the redundancy in the router. |


- Information About Configuration Groups, on page 226
- Supported Devices for Configuration Groups, on page 228
- Prerequisites for Configuration Groups, on page 229
- Restrictions for Configuration Groups, on page 229
- Use Cases for Configuration Groups, on page 229
- Use the Configuration Group Workflows, on page 232
- Add Devices to a Configuration Group, on page 235
- Deploy Configuration Groups, on page 239
- Remove Devices from a Configuration Group, on page 241
- Feature Management, on page 241


# Information About Configuration Groups

The Configuration Group feature enables you to do the following:

- Create a configuration group using one of the guided workflows—Create Configuration Group, Rapid Site Configuration Group, or Custom Configuration Group

**Note** The Rapid Site Configuration Group and the Custom Configuration Group workflows are available only in Cisco vManage Release 20.8.x.

- Deploy devices with a configuration group using the Deploy Configuration Group workflow

**Note** In Cisco vManage Release 20.8.x, the Deploy Configuration Group workflow is called the Provision WAN Sites and Devices workflow.

## Overview of Configuration Groups

The Configuration Group feature provides a simple, reusable, and structured approach for the configurations in Cisco Catalyst SD-WAN.

- **Configuration Group:** A configuration group is a logical grouping of features or configurations that can be applied to one or more devices in the network managed by Cisco Catalyst SD-WAN. You can define and customize this grouping based on your business needs.
- **Feature Profile:** A feature profile is a flexible building block of configurations that can be reused across different configuration groups. You can create profiles based on features that are required, recommended, or uniquely used, and then put together the profiles to complete a device configuration.
- **Feature:** A feature profile consists of features. Features are the individual capabilities you want to share across different configuration groups.

# Overview of Configuration Group Workflows

From Cisco vManage Release 20.9.1, the simplified Create Configuration Group workflow guides you in creating a configuration group for a single-router site. The workflow provides you with an improved configuration and troubleshooting experience. The workflow has the following features:

- You can specify a name and description for a configuration group and configure the basic settings to keep your network running.
- In addition to the basic settings, you can also configure advanced options at the time of creating a configuration group. For example, you can set up WAN and LAN routing; you can configure a BGP route, multiple static IPv4 routes, or both, for the WAN transport VPN. Similarly, you can configure a BGP route, an OSPF route, multiple static IPv4 routes, or all these routes, for a LAN service VPN. Thus, you can configure all the necessary options at the time of creating the configuration group itself, and do not have to modify the features separately after the group is created. As a result, any configuration created from the workflow is immediately deployable.
- You can review the various configuration settings on a single page within the workflow.
- When you specify an incorrect setting, it is highlighted in red. As a result, you can easily identify errors, if any, and fix them. In addition, an asterisk adjacent to the field names helps you identify the mandatory settings within the workflow.

You can access the workflow from the **Workflow Library** in Cisco SD-WAN Manager.

**Note** In Cisco vManage Release 20.8.x, the Rapid Site Configuration Group and the Custom Configuration Group workflows enabled you to create a configuration group. However, these workflows are deprecated from Cisco vManage Release 20.9.1.

# Overview of the Deploy Configuration Group Workflow

The Deploy Configuration Group workflow enables you to associate devices to a configuration group and to deploy the configuration to the selected devices.

**Note** In Cisco vManage Release 20.8.x, the Deploy Configuration Group workflow is called the Provision WAN Sites and Devices workflow.

You can access the workflow from the **Workflow Library** in Cisco SD-WAN Manager.

# Overview of Dual Device Site Configuration

Minimum Supported Releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier releases, you could configure dual devices in the same site using a single router type configuration group workflow. Here all the configuration group features are applicable to both the routers. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can deploy dual device site configuration by selecting dual router type configuration group workflow, and distribute the transport side WAN and service side LAN interface configurations between the two routers based on your requirements.

This feature automates the deployment of two routers in the same site considering the redundancy in the router. One router acts as a primary device and the other as the secondary device. If there is a failure scenario in the primary router, the secondary router takes over ensuring that there's no connectivity issues.

Depending on your requirement, you can configure the transport side WAN and service side LAN interfaces, enable TLOC or a full mesh topology, and select specific configuration groups features for both the routers.

# Benefits of Configuration Groups

- Simplicity: The workflow-based configuration guides you with step-by-step instructions. You can clearly identify what is necessary, what is optional, and what is the recommended Cisco networking best practice.

  In addition, the basic and advanced settings of a configuration group are auto-populated, which in turn, simplifies the process of a configuration.

- Day-zero Deployment: The day-zero setup of configuration groups helps you easily create a branch and deploy devices quickly.

- Reusability: You can reuse configuration components across an entire device family instead of one device model. This helps in easier management of configuration components.

- Structure: You can group devices based on a shared configuration in Cisco SD-WAN Manager.

- Visibility: A site-level topology is generated for Cisco IOS XE Catalyst SD-WAN devices that are attached to a configuration group. For complete information about viewing the topology of a site, see View Network Site Topology.

- Findability: The tagging feature helps you easily identify a subset of devices from hundreds of devices in a configuration group. For complete information about adding tags to devices, see Device Tagging.

# Supported Devices for Configuration Groups

This feature is supported only on Cisco IOS XE Catalyst SD-WAN devices.

# Prerequisites for Configuration Groups

Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

**Note** The downward compatibility support is till Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Minimum software version for Cisco SD-WAN Manager: Cisco vManage Release 20.8.1

# Restrictions for Configuration Groups

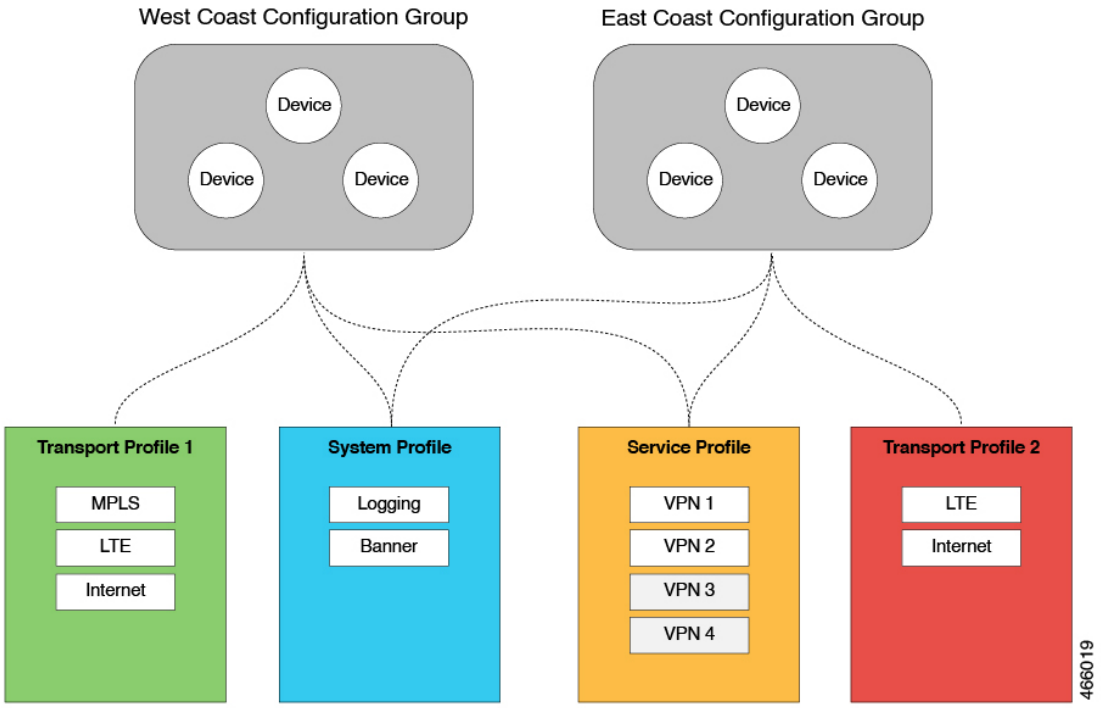
- You can associate a device to either a configuration group or a device template, but not both.
- You can add a device to only one configuration group.
- You can add only one tag rule to a configuration group.
- (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1) You can only apply the dual device configuration group to a site with two or less devices. For additional devices in the same site, use a single device configuration group.

# Use Cases for Configuration Groups

You can create configuration groups according to your business needs. For example, if your organization operates in North America and has offices and network infrastructure on both the West Coast and the East Coast, you can create two configuration groups—the East Coast Configuration Group and the West Coast Configuration Group.

The following figure shows that both the East Coast Configuration Group and the West Coast Configuration Group use the same system profile and service profile. The transport profile is different for both the groups.

*Figure 1: Example of Configuration Groups*



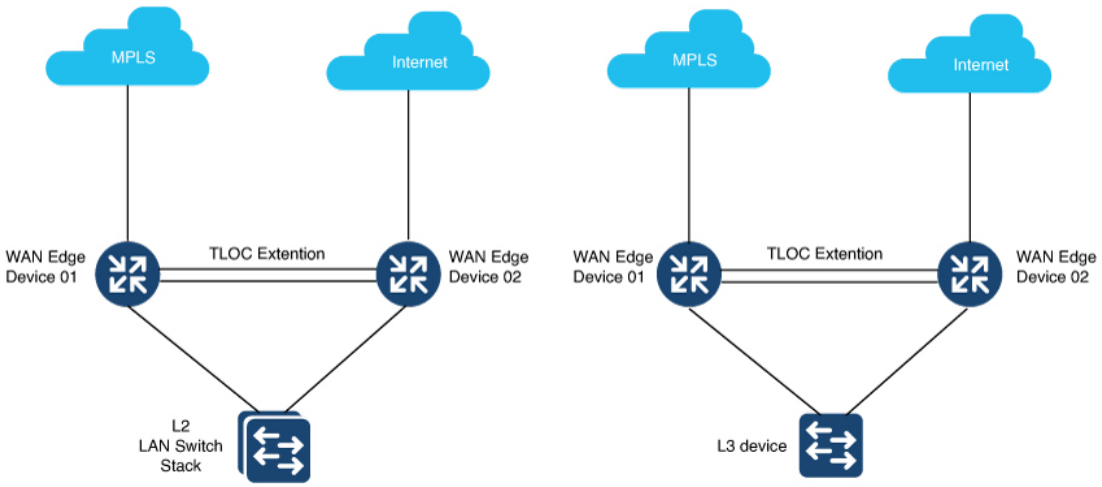

In this figure,

- The East Coast Configuration Group and the West Coast Configuration Group are examples of configuration groups. Similarly, a supply chain organization can create configuration groups for different facilities, such as a retail store configuration group and a distribution center configuration group. A multinational company can create configuration groups to cater to its business needs in different regions, such as the Americas Configuration Group and the EMEA Configuration Group.
- System profile, transport profile, and service profile are examples of feature profiles.
- Logging; Banner; interfaces, such as MPLS, LTE, and Internet; VPN1; VPN2; and so on are examples of features.

# Use Case for Dual Device Site Configurations

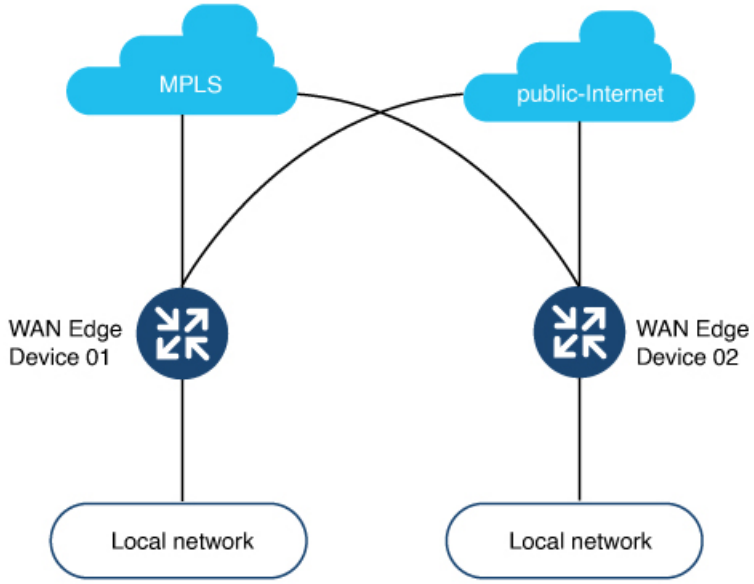
To deploy dual device site configuration, you can choose a TLOC extension or a full mesh topology in the dual router type configuration group workflow. Use of TLOC extensions is recommended for failure scenarios and redundancy.

*Figure 2: TLOC Extension Topology*




When you use a TLOC extension, there's a transport extension between the two devices. One end acts like a tunnel interface and the other end acts like a TLOC interface. By default, there's a single uplink to the public interface for each of the device. One device has an uplink to MPLS and the other device has an uplink to the internet.

*Figure 3: Full Mesh Topology*




In the full mesh topology, there's no transport extension and there's an assumption that each device has its own public uplink.

# 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** > **Validator**.
2. Enter the IP address of the Cisco SD-WAN Validator.
3. Enter the port number to use to connect to it.

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.

## Examples of Applying Rules Using Tags

Scenario: There are five devices in the network, and you want to add the devices to configuration groups based on tagging.

1. Tag each device. For information about tagging devices, see Add Tags to Devices Using Cisco SD-WAN Manager.

   In the following example, tags have been added to five Cisco Catalyst 8000V devices.

   ***Table 58: Example of Device Tagging***

| Device UUID | Tags |
|---|---|
| C8K-0001 | CA1, CA2 |
| C8K-0002 | CA1, CA2, CA3 |
| C8K-0003 | CA1, CA4, CA5 |
| C8K-0004 | CA3, CA4 |
| C8K-0005 | CA3, CA5 |

2. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)

   Choose any one of the following rule conditions:

   - **Match All**
   - **Match Any**

3. Use rules to add the devices to specific configuration groups based on the tags that you have added to each device.

   When applying a rule, you can use the following operators:

   - Equal: This operator checks for matching data.
   - Not equal: This operator checks for nonmatching data.
   - Contain: This operator finds a value anywhere in your data.
   - Not contain: This operator filters data that does not contain any of the specified values.
   - (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)

     Starts with: This operator filters data that starts with any specified values.
   - (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)

     Ends with: This operator filters data that ends with any specified values.

   For information about using rules to add devices to configuration groups, see Add Devices to a Configuration Group Using Rules.

The following examples show the effects of using different operators when applying a rule, based on how devices are tagged.

### Rule Example 1

Condition: Match Any

Operator: EQUAL

Specified tags: CA1, CA2

Effect: Matches any device containing these two tags.

Configuration group: A

Result: Devices C8K-0001 and C8K-0002 are added to configuration group A.

### Rule Example 2

Condition: Match Any

Operator: NOT EQUAL

Specified tags: CA1, CA2

Effect: Matches any device that does not contain both of these tags.

Configuration group: B

Result: Devices C8K-0003, C8K-0004, and C8K-0005 are added to configuration group B.

### Rule Example 3

Condition: Match Any

Operator: CONTAIN

Specified tags: CA1, CA2

Effect: Matches any device that contains any one of these tags.

Configuration group: C

Result: Devices C8K-0001, C8K-0002, and C8K-0003 are added to configuration group C.

### Rule Example 4

Condition: Match Any

Operator: NOT CONTAIN

Specified tags: CA1, CA2

Effect: Matches any device that does not contain any one of these tags.

Configuration group: D

Result: Devices C8K-0004 and C8K-0005 are added to configuration group D.

### Rule Example 5

Condition: Match Any

Operator: STARTS WITH

Specified tags: CA

Effect: Matches any device that has a tag that starts with the specified value.

Configuration group: E

Result: Devices C8K-0001, C8K-0002, C8K-0003, C8K-0004, and C8K-0005 are added to configuration group E.

#### Rule Example 6

Condition: Match All

Operator: ENDS WITH

Specified tags: 1

Effect: Matches all devices that have a tag that ends with the specified value.

Configuration group: F

Result: Devices C8K-0001, C8K-0002, and C8K-0003 are added to configuration group F.

# Deploy Configuration Groups

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 configuration groups.

## Deploy Configuration Groups 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 Configuration Group 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.

# Configure Device Values

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

The **Change Device Values** workflow enables you to provide device variable values without deploying a configuration group to the devices. If you do not have RBAC permission for deploying, you can use **Change Device Values** workflow to modify device variable values.

You can associate devices of different models to the same configuration group. Not all of the associated devices necessarily support each feature configured in the configuration group. For example, Cisco Catalyst 8000v devices do not support the ThousandEyes feature. When you deploy a configuration group to devices, for each device, Cisco SD-WAN Manager applies only the features that the device supports.

### Before You Begin

Role-Based Access Control (**Administration** > **Manage Users** > **User Group**) permissions determine which variables you can view and update.

### Configure Device Values

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 click **Change Device Values**.

   The **Change Device Values** workflow starts.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Control Components Release 20.12.1, the variable name can contain dots (.), forward slashes (/) and square brackets ([]).

5. Follow the instructions provided in the workflow.

The **Devices** table lists the selected devices.

6. Click **Next**.

   The **Select Devices to Change Values** page is displayed.

7. Select the devices.

8. Click **Next**.

   The **Add and Review Device Configuration** page is displayed.

9. Follow the instructions and update the **Device Configuration** details.

   Modify the configurations as needed or edit the table to add system IPs and site IDs.

10. Click **Save**.

# Remove Devices from a Configuration Group

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. In the **Devices** table, choose the devices that you want to remove from the configuration group.

5. Click **Remove Devices**.

**Note** If a device is automatically added to a configuration group based on a tag rule, you cannot remove the device from the group using the above method. To do this, you must edit the tag rule or delete the rule. For complete information on adding or editing a tag rule, see Add Devices to a Configuration Group Using Rules.

# Feature Management

## Add a Feature to a Feature Profile

### Before You Begin

Adding a feature to a feature profile requires a configuration group. For information about creating a configuration group, see ___.

### Add a Feature to a Feature 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. Click **…** adjacent to a configuration group name and choose **Edit**.
3. Click a feature profile to open it.
4. Click **Add Feature**.
5. From the feature drop-down list, choose a feature.

**Note** Features that have already been added are grayed out.

6. In the **Name** field, enter a name for the feature.

   The name can be up to 128 characters and can contain only alphanumeric characters.

7. In the **Description** field, enter a description of the feature.

   The description can be up to 2048 characters and can contain only alphanumeric characters and spaces.

8. Configure the options as needed.

   Some parameter have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (indicated by a globe icon) | Enter a value for the parameter to apply the value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the field. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value is shown for parameters that have a default setting. |

9. Click **Save**.

# Add a Subfeature

### Before You Begin

Some features include subfeature options.

### Add a Subfeature

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 a configuration group name and choose **Edit**.
3. Click a feature profile to open it.
4. Click **…** adjacent to a feature and choose **Add Sub-Feature**.
5. From the drop-down list, choose a subfeature.
6. In the **Name** field, enter a name for the feature.
7. In the **Description** field, enter a description of the feature.
8. Configure the options as needed.
9. Click **Save**.

# Edit 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 a feature profile to open it.
4. Click **…** adjacent to a feature and choose **Edit Feature**.
5. Configure the options as needed.
6. Click **Save**.

# Delete 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 **…** adjacent to the feature and choose **Delete Feature**.

# Feature Configuration

The configuration group workflows generate the feature profiles. The various features are a part of one of these profiles.

## System Profile

### AAA

The authentication, authorization, and accounting (AAA) feature helps the device authenticate users logging in to the Cisco Catalyst SD-WAN router, decide what permissions to give them, and perform accounting of their actions.

The following tables describe the options for configuring the AAA feature.

#### Local

| Field | Description |
|---|---|
| **Enable AAA Authentication** | Enable authentication parameters. |
| **Accounting Group** | Enable accounting parameters. |
| **Add AAA User** | |
| **Name** | Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.<br>The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved. |
| **Password** | Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, The YANG 1.1 Data Modeling Language.<br>Each username must have a password. Users are allowed to change their own passwords.<br>The default password for the admin user is admin. We strongly recommended that you change this password. |
| **Confirm Password** | Re-enter the password for the user. |

| Field | Description |
|---|---|
| **Privilege** | Select between privilege level 1 or 15.<br>• Level 1: User EXEC mode. Read-only, and access to limited commands, such as the ping command.<br>• Level 15: Privileged EXEC mode. Full access to all commands, such as the reload command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1. |
| **Add Public Key Chain** | |
| **Key String*** | Enter the authentication string for a key. |
| **Key Type** | Choose **ssh-rsa**. |

**Radius**

| Field | Description |
|---|---|
| **Add Radius Server** | |
| **Address*** | Enter the IP address of the RADIUS server host. |
| **Acct Port** | Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server.<br>Range: 0 through 65535.<br>Default: 1813 |
| **Auth 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.<br>Default: 1812 |
| **Retransmit** | Enter the number of times the device transmits each RADIUS request to the server before giving up.<br>Default: 3 seconds |
| **Timeout** | Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request.<br>Default: 5 seconds<br>Range: 1 through 1000 |
| **Key*** | Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. |
| **Key Type** | Choose Protected Access Credential (PAC) or key type. |

### TACACS Server

| Field | Description |
|---|---|
| **Add TACACS Server** | |
| **Address*** | Enter the IP address of the TACACS+ server host. |
| **Port** | Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0.<br>Default: 49 |
| **Timeout** | Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request.<br>Default: 5 seconds<br>Range: 1 through 1000 |
| **Key*** | Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type 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 TACACS+ server. |

### Accounting

| Field | Description |
|---|---|
| **Add Accounting Rule** | |
| **Rule Id*** | Enter the accounting rule ID. |
| **Method*** | Specifies the accounting method list. Choose one of the following:<br>• **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level.<br>• **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.<br>• **network**: Runs accounting for all network-related service requests.<br>• **system**: Performs accounting for all system-level events not associated with users, such as reloads.<br>**Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes. |
| **Level** | Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level. |
| **Start Stop** | Enable this option to 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. |

| Field | Description |
|---|---|
| **Use Server-group*** | 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. |

### Authorization

| Field | Description |
|---|---|
| **Server Auth Order*** | Choose the authentication order. It dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port. |
| **Authorization Console** | Enable this option to perform authorization for console access commands. |
| **Authorization Config Commands** | Enable this option to perform authorization for configuration commands. |
| **Add Authorization Rule** | |
| **Rule Id*** | Enter the authorization rule ID. |
| **Method*** | Choose **Commands**, which causes commands that a user enters to be authorized. |
| **Level** | Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level. |
| **If Authenticated** | Enable this option to apply the authorization rule parameters only to the authenticated users. If you do not enable this option, the rule is applied to all users. |
| **Use Server-group*** | 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. |

## BFD

Bidirectional Forwarding Detection (BFD) is a protocol that detects link failures as part of the Cisco Catalyst SD-WAN high-availability solution. This feature helps you configure options such as color, DSCP values, poll interval, multiplier for detection, and so on.

The following tables describe the options for configuring the BFD feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Poll Interval(In Millisecond)** | Specify how often BFD polls all data plane tunnels on a router to collect packet latency, loss, and other statistics used by application-aware routing.<br>Range: 1 through 4,294,967,296 ($2^{32}$ – 1) milliseconds<br>Default: 600,000 milliseconds (10 minutes) |
| **Multiplier** | Specify the value by which to multiply the poll interval, to set how often application-aware routing acts on the data plane tunnel statistics to figure out the loss and latency and to calculate new tunnels if the loss and latency times do not meet the configured SLAs.<br>Range: 1 through 6<br>Default: 6 |
| **DSCP Values for BFD Packets(decimal)** | Specify the Differentiated Services Code Point (DSCP) value of the BFD packets that is used in the DSCP control traffic.<br>Range: 0-63<br>Default: 48 |

### Color

| Field | Description |
|---|---|
| **Add Color** | |
| **Color*** | Choose the color of the transport tunnel for data traffic moving between the devices. The color identifies a specific WAN transport provider.<br>Values: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver<br>Default: default |
| **Hello Interval (milliseconds)*** | Specify how often BFD sends Hello packets on the transport tunnel. BFD uses these packets to detect the liveness of the tunnel connection and to detect faults on the tunnel.<br>Range: 100 through 300000 milliseconds<br>Default: 1000 milliseconds (1 second) |
| **Multiplier*** | Specify how many Hello packet intervals BFD waits before declaring that a tunnel has failed. BFD declares that the tunnel has failed when, during all these intervals, BFD has received no Hello packets on the tunnel. This interval is a multiplier of the Hello packet interval time.<br>Range: 1 through 60<br>Default: 7 |

| Field | Description |
|---|---|
| **Path MTU Discovery*** | Enable or disable path MTU discovery for the transport tunnel. When path MTU discovery is enabled, the path MTU for the tunnel connection is checked periodically, about once per minute, and it is updated dynamically. When path MTU discovery is disabled, the expected tunnel MTU is 1472 bytes, but the effective tunnel MTU is 1468 bytes.<br>Default: Enabled |
| **Default DSCP value for BFD packets*** | Specify the Differentiated Services Code Point (DSCP) value of the BFD packets that is used in the DSCP control traffic.<br>Range: 0-63<br>Default: 48 |

## Banner

The Banner feature helps you to configure the system login banner.

For each parameter of the feature 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 to the left of the parameter field and choose one of the following:

The following table describes the options for configuring the Banner 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. |
| **Login** | Enter the text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type \n. |
| **MOTD** | On a Cisco IOS XE Catalyst SD-WAN device, enter the message-of-the-day text to display before the login banner. The string can be up to 2048 characters long. To insert a line break, type \n. |

## Basic

The Basic feature helps you configure the basic system-wide functionality of the network devices, such as time zone, GPS location, baud rate of the console connection on the router, and so on.

The following tables describe the options for configuring the Basic feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Time Zone** | Choose the time zone to use on the device. |

| Field | Description |
|---|---|
| **Device Groups** | Enter the names of one or more groups to which the device belongs, separated by commas. |
| **Location** | Enter a description of the location of the device. It can be up to 128 characters. |
| **Description** | Enter any additional descriptive information about the device. |
| **Console Baud Rate(bps)** | Choose the baud rate of the console connection on the router.<br>Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps).<br>Default: 9600 |
| **Overlay ID** | Specifies the overlay ID of a device in the Cisco Catalyst SD-WAN overlay network.<br>Range: 0 - 4294967295 ($2^{32} – 1$)<br>Default: 1 |
| **Controller Group** | List the Cisco Catalyst SD-WAN Controller groups to which the router belongs. |
| **Max OMP Sessions** | Set the maximum number of OMP sessions that a router can establish to a Cisco SD-WAN Controller.<br>Range: 1 through 100 |

### GPS

| Field | Description |
|---|---|
| **GPS Latitude** | Enter the latitude of the device, in the format decimal-degrees. |
| **GPS Longitude** | Enter the longitude of the device, in the format decimal-degrees. |

### Track Settings

| Field | Description |
|---|---|
| **Track Transport** | Enable this option to regularly check whether the DTLS connection between the device and a Cisco SD-WAN Validator is up.<br>Default: Enabled |
| **Track Default Gateway** | Enable or disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the route table of the device.<br>Default: Enabled |

| Field | Description |
|---|---|
| **Track Interface Tag** | Set the tag string to include in routes associated with a network that is connected to a non-operational interface.<br>Range: 1 through 4294967295 |
| **Tracker DIA Stabilize Status** | Enable this option to stabilize interface flaps by using the multiplier to update HTTP or ICMP tracker status from DOWN to UP. |

### Advanced

| Field | Description |
|---|---|
| **Port Hopping** | Enable or disable port hopping. When a Cisco Catalyst SD-WAN device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other Cisco Catalyst SD-WAN devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value.<br>Default: Enabled |
| **Port Offset** | Enter a number by which to offset the base port number. Configure this option when multiple Cisco Catalyst SD-WAN devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections.<br>Values: 0 through 19 |
| **On Demand Tunnel** | Enable dynamic on-demand tunnels between any two Cisco Catalyst SD-WAN spoke devices. |
| **On Demand Tunnel Idle Timeout (In Minute)** | Enter the on-demand tunnel idle timeout time. After the configured time, the tunnel between the spoke devices is removed.<br>Range: 1 to 65535 minutes<br>Default: 10 minutes |
| **Control Session PPS** | Enter a maximum rate of DTLS control session traffic to police the flow of control traffic.<br>Range: 1 through 65535 pps<br>Default: 300 pps |
| **Multi Tenant** | Enable this option to specify the device as multitenant. |
| **Admin Tech On Failure** | Enable this option to collect admin-tech information when the device reboots.<br>Default: Enabled |

## Cisco Security

Use this feature to configure security parameters for the data plane in the Cisco Catalyst SD-WAN overlay network.

The following tables describe the options for configuring the Cisco Security feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Rekey Time (seconds)** | Specify how often a device changes the AES key. Before Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices can exchange data traffic, they set up a secure authenticated communications channel between them. The routers use IPSec tunnels between them as the channel, and the AES-256 cipher to perform encryption. Each router generates a new AES key for its data path periodically.<br>Range: 10 through 1209600 seconds (14 days)<br>Default: 86400 seconds (24 hours) |
| **Extended AR Window** | Enabling an extended AR window causes a router to add a time stamp to each packet using the IPsec tunnel. This prevents valid packets from being dropped if they arrive out of sequence.<br>This option is turned off by default. Click **On** to enable it.<br>Enabling the feature displays the **Extended Anti-Replay Window** field.<br>Range: 10 ms to 2048 ms<br>Default: 256 ms |
| **Replay Window** | Specify the size of the sliding replay window.<br>Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets.<br>Default: 512 packets |
| **IPsec pairwise-keying** | This option is turned off by default. Click **On** to enable it. |

### Authentication Type

| Field | Description |
|---|---|
| **Integrity Type** | Choose one of the following integrity types:<br>• **esp**: Enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header.<br>• **ip-udp-esp**: Enables ESP encryption. In addition to the integrity checks on the ESP header and payload, the checks include the outer IP and UDP headers.<br>• **ip-udp-esp-no-id**: Ignores the ID field in the IP header so that Cisco Catalyst SD-WAN can work with the non-Cisco devices.<br>• **none**: Turns integrity checking off on IPSec packets. We don't recommend using this option. |

### Key Chain

| Field | Description |
|---|---|
| **Add Key Chain** | |
| **Key ID*** | Select a key chain ID. |
| **Key Chain Name*** | Select a key chain name. |

### Key ID

| Field | Description |
|---|---|
| **Add Key ID** | |
| **ID*** | Select a key chain ID. |
| **Name*** | Select a key chain name. |
| **Include TCP Options** | This field indicates whether a TCP option other than TCP Authentication Option (TCP-AO) is used to calculate Message Authentication Codes (MACs).<br>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.<br>When options are included, the content of all options is included in the MAC with TCP-AO's **MAC** field is filled with zeroes.<br>When the options aren't included, all options other than TCP-AO are excluded from all MAC calculations. |
| **Key String** | Specify the master key for deriving the traffic keys.<br>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 through 80 characters. |
| **Receiver ID*** | Specify the receive identifier for the key.<br>Range: 0 through 255. |
| **Send ID*** | Specify the send identifier for the key.<br>Range: 0 through 255. |
| **TCP** | Specify the algorithm to compute MACs for TCP segments. You can choose one of the following:<br>• **aes-128-cmac**<br>• **hmac-sha-1**<br>• **hmac-sha-256** |

| Field | Description |
|---|---|
| **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. |
| **Accept Lifetime** | The following fields appear when you click this field:<br>• **Accept Local**: This option is disabled by default. Click **On** to enable it.<br>• **Accept Start Epoch**: 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.<br>• **End Time Format**: You can specify the end time in three ways—infinite (no expiry), duration (1 through 2147483646 sec), or exact (either UTC or local). |
| **Send Lifetime** | The following fields appear when you click this field:<br>• **Send Local**: This option is disabled by default. Click **On** to enable it.<br>• **Send Start Epoch**: 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.<br>• **End Time Format**: You can specify the end time in three ways—infinite (no expiry), duration (1 through 2147483646 sec), or exact time (either UTC or local). |

## Global

The Global feature helps you enable or disable various services on the devices such as HTTP, HTTPS, Telnet, IP domain lookup, and several other device settings.

The following tables describe the options for configuring the Global feature.

### Services

| Field | Description |
|---|---|
| **HTTP Server** | Enable or disable HTTP server. |
| **HTTPS Server** | Enable or disable secure HTTPS server. |
| **FTP Passive** | Enable or disable passive FTP. |
| **Domain Lookup** | Enable or disable Domain Name System (DNS) lookup. |
| **ARP Proxy** | Enable or disable proxy ARP. |
| **RSH/RCP** | Enable or disable remote shell (RSH) and remote copy (rcp) on the device. |
| **Line Virtual Teletype (Configure Outbound Telnet)** | Enable or disable outbound telnet. |

| Field | Description |
|---|---|
| **Cisco Discovery Protocol (CDP)** | Enable or disable Cisco Discovery Protocol (CDP). |
| **Link Layer Discovery Protocol (LLDP)** | Enable or disable Link Layer Discovery Protocol (LLDP). |
| **Specify interface for source address** | Enter the address of the source interface in all HTTPS client connections. |

### NAT 64

| Field | Description |
|---|---|
| **UDP Timeout** | Specify the NAT64 translation timeout for UDP.<br>Range: 1 to 536870 (seconds)<br>Default: 300 seconds (5 minutes) |
| **TCP Timeout** | Specify the NAT64 translation timeout for TCP.<br>Range: 1 to 536870 (seconds)<br>Default: 3600 seconds (1 hour) |

### Authentication

| Field | Description |
|---|---|
| **HTTP Authentication** | Choose the HTTP authentication mode.<br>Accepted values: Local, AAA<br>Default: Local |

### SSH Version

| Field | Description |
|---|---|
| **SSH Version** | Choose the SSH version.<br>Default: Disabled |

### Other Settings

| Field | Description |
|---|---|
| **TCP Keepalives (In)** | Enable or disable generation of keepalive timers when incoming network connections are idle. |
| **TCP Keepalives (Out)** | Enable or disable generation of keepalive timers when outgoing network connections are idle. |

| Field | Description |
|---|---|
| **TCP Small Servers** | Enable or disable small TCP servers (for example, ECHO). |
| **UDP Small Servers** | Enable or disable small UDP servers (for example, ECHO). |
| **Console Logging** | Enable or disable console logging. By default, the router sends all log messages to its console port. |
| **IP Source Routing** | Enable or disable IP source routing. IP source routing is a feature that enables the originator of a packet to specify the path for the packet to use to get to the destination. |
| **VTY Line Logging** | Enable or disable the device to display log messages to a vty session in real time. |
| **SNMP IFINDEX Persist** | Enable or disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots. |
| **Ignore BOOTP** | Enable or disable BOOTP server. When enabled, the device listens for the BOOTP packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets. |

## Logging

The Logging feature helps you configure logging to either the local hard drive or a remote host.

The following tables describe the options for configuring the Logging feature.

### Disk

| Field | Description |
|---|---|
| **Enable Disc** | Enable this option to allow syslog messages to be saved in a file on the local hard disk, or disable this option to disallow it. By default, logging to a local disk file is enabled on all Cisco IOS XE Catalyst SD-WAN devices. |
| **Max File Size(In Megabytes)** | Enter the maximum size of syslog files. The syslog files are rotated on an hourly basis based on the file size. When the file size exceeds the configured value, the file is rotated and the syslog process is notified.<br>Range: 1 to 20 MB<br>Default: 10 MB |
| **Rotations** | Enter the number of syslog files to create before discarding the oldest files.<br>Range: 1 to 10<br>Default: 10 |

### TLS Profile

| Field | Description |
|---|---|
| **Add TLS Profile** | |

| Field | Description |
|---|---|
| **TLS Profile Name*** | Enter the name of the TLS profile. |
| **TLS Version** | Choose a TLS version:<br>• **TLSv1.1**<br>• **TLSv1.2** |
| **Authentication Type*** | Choose **Server**. |
| **Cipher Suite List** | Choose groups of cipher suites (encryption algorithm) based on the TLS version.<br>The following is the list of cipher suites.<br>• **aes-128-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_128_sha<br>• **aes-256-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_256_sha<br>• **dhe-aes-cbc-sha2**: Encryption type tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 and above)<br>• **dhe-aes-gcm-sha2**: Encryption type tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 and above)<br>• **ecdhe-ecdsa-aes-gcm-sha2**: Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 and above) SuiteB<br>• **ecdhe-rsa-aes-cbc-sha2**: Encryption type tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 and above)<br>• **ecdhe-rsa-aes-gcm-sha2**: Encryption type tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 and above)<br>• **rsa-aes-cbc-sha2**: Encryption type tls_rsa_with_aes_cbc_sha2 (TLS1.2 and above)<br>• **rsa-aes-gcm-sha2**: Encryption type tls_rsa_with_aes_gcm_sha2 (TLS1.2 and above) |

**Server**

| Field | Description |
|---|---|
| **Add Server** | |
| **Hostname/IPv4 Address*** | Enter the DNS name, hostname, or IP address of the system on which to store syslog messages.<br>To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry. |

| Field | Description |
|---|---|
| **VPN*** | Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached.<br>Range: 0 through 65530 |
| **Source Interface** | Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them. |
| **Priority** | Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of the following:<br>• **informational**: Routine condition (the default) (corresponds to syslog severity 6)<br>• **debugging**: Prints additional logs to help debugging the issue.<br>• **notice**: A normal, but significant condition (corresponds to syslog severity 5)<br>• **warn**: A minor error condition (corresponds to syslog severity 4)<br>• **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3)<br>• **critical**: A serious condition (corresponds to syslog severity 2)<br>• **alert**: Action must be taken immediately (corresponds to syslog severity 1)<br>• **emergency**: System is unusable (corresponds to syslog severity 0) |
| **TLS Enable*** | Enable this option to allow syslog over TLS. When you enable this option, the following field appears:<br>**TLS Properties Custom Profile**: Enable this option to choose a TLS profile. When you enable this option, the following field appears:<br>**TLS Properties Profile**: Choose a TLS profile that you have created for server or mutual authentication in the IPv4 server configuration. |
| **Add IPv6 Server** | |
| **Hostname/IPv6 Address*** | Enter the DNS name, hostname, or IP address of the system on which to store syslog messages.<br>To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry. |
| **VPN*** | Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached.<br>Range: 0 through 65530 |

| Field | Description |
|---|---|
| **Source Interface** | Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them. |
| **Priority** | Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of the following:<br>• **informational**: Routine condition (the default) (corresponds to syslog severity 6)<br>• **debugging**: Prints additional logs to help debugging the issue.<br>• **notice**: A normal, but significant condition (corresponds to syslog severity 5)<br>• **warn**: A minor error condition (corresponds to syslog severity 4)<br>• **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3)<br>• **critical**: A serious condition (corresponds to syslog severity 2)<br>• **alert**: Action must be taken immediately (corresponds to syslog severity 1)<br>• **emergency**: System is unusable (corresponds to syslog severity 0) |
| **TLS Enable*** | Enable this option to allow syslog over TLS. |
| **TLS Properties Custom Profile*** | Enable this option to choose a TLS profile. |
| **TLS Properties Profile** | Choose a TLS profile that you have created for server or mutual authentication in the IPv6 server configuration. |

## Multi-Region Fabric

Multi-Region Fabric provides the option to divide the architecture of the Cisco Catalyst SD-WAN overlay network into the following:

- A core overlay network: This network, called region 0, consists of border routers that connect to regional overlays and connect to each other.
- One or more regional overlay networks: Each regional network consists of edge routers that connect to other edge routers within the same region, and can connect to core region border routers that are assigned to the region.

For information, see the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*.

The following table describes the options for configuring Multi-Region Fabric.

| 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** | Enter a description of the feature. |
| **Region** | Choose a Multi-Region Fabric region in the range 1 to 63. For the edge router role, this value determines the access region in which a router operates. For the border router role, this value determines which access region the border router serves.<br>For information, see Cisco Catalyst SD-WAN Multi-Region Fabric in the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*. |
| **Secondary Region ID** | Secondary regions contain only edge routers and enable direct tunnel connections between edge routers in different primary regions. When you add an edge router to a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.<br>Choose a secondary region in the range 1 to 63.<br>For information, see Secondary Regions in the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*. |
| **Role** | Choose **Edge Router** or **Border Router**.<br>**Note** Only Cisco IOS XE Catalyst SD-WAN devices can have the border router role. |
| **Transport Gateway** | To configure a router as a transport gateway, enable this option.<br>For information, see Transport Gateways in the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*. |
| **Enable Migration Mode to Multi-Region Fabric** | To enable a router to migrate to a Multi-Region Fabric network architecture, enable this option.<br>For information about migration, see Migrating to Multi-Region Fabric in the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*. |

## NTP

Network Time Protocol (NTP) is a protocol that allows a distributed network of servers and clients to synchronize the timekeeping across the network. The NTP feature helps you configure NTP settings on the Cisco Catalyst SD-WAN network.

The following tables describe the options for configuring the NTP feature.

### Server

| Field | Description |
|---|---|
| **Add Server** | |
| **Hostname/IP address*** | Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server. |
| **VPN to reach NTP Server*** | Enter the number of the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN.<br>Range: 0 to 65530 |
| **Set authentication key for the server** | Specify the MD5 key associated with the NTP server, to enable MD5 authentication.<br>For the key to work, you must mark it as trusted in the **Trusted Key** field under **Authentication**. |
| **Set NTP version*** | Enter the version number of the NTP protocol software.<br>Range: 1 to 4<br>Default: 4 |
| **Set interface to use to reach NTP server** | Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored. |
| **Prefer this NTP server*** | Enable this option if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, Cisco Catalyst SD-WAN chooses the one at the highest stratum level. |

### Authentication

| Field | Description |
|---|---|
| **Add Authentication Keys** | |
| **Key Id*** | Enter an MD5 authentication key ID.<br>Range: 1 to 65535 |
| **MD5 Value*** | Enter an MD5 authentication key. Enter either a cleartext key or an AES-encrypted key. |
| **Trusted Key** | Enter the MD5 authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value that you entered for the **Set authentication key for the server** field under **Server**. |

### Authoritative NTP Server

| Field | Description |
|---|---|
| **Authoritative NTP Server** | Choose **Global** from the drop-down list, and enable this option if you want to configure one or more supported routers as a primary NTP router.<br>When you enable this option, the following field appears:<br>**Stratum**: Enter the stratum value for the primary NTP router. The stratum value defines the hierarchical distance of the router from its reference clock.<br>Valid values: Integers 1 to 15. If you do not enter a value, the system uses the router internal clock default stratum value, which is 8. |
| **Source** | Enter the name of the exit interface for NTP communication. If configured, the system sends NTP traffic to this interface.<br>For example, enter **`GigabitEthernet1`** or **`Loopback0`**. |

## OMP

This feature helps you configure the Overlay Management Protocol (OMP) parameters.

The following tables describe the options for configuring the OMP feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Graceful Restart Enable** | Enable graceful restart. By default, the graceful restart for OMP is enabled. |
| **Paths Advertised Per Prefix** | Specify the maximum number of equal-cost routes to advertise per prefix. A Cisco IOS XE Catalyst SD-WAN device advertises routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistribute the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE Catalyst SD-WAN device can have up to four TLOCs, and by default advertises each route-TLOC tuple to the Cisco Catalyst SD-WAN Controller. If a local site has two Cisco IOS XE Catalyst SD-WAN devices, a Cisco Catalyst SD-WAN Controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised.<br>Range: 1 through 16<br>Default: 4 |
| **ECMP Limit** | Specify the maximum number of OMP paths received from the Cisco Catalyst SD-WAN Controller that can be installed in the local route table of the Cisco IOS XE Catalyst SD-WAN device. By default, a Cisco IOS XE Catalyst SD-WAN device installs a maximum of four unique OMP paths into its route table.<br>Range: 1 through 16<br>Default: 4 |

| Field | Description |
|---|---|
| **Advertisement Interval (In Second)** | Specify the time between OMP update packets.<br>Range: 0 through 65535 seconds<br>Default: 1 second |
| **Hold Time(In Second)** | Specify how long to wait before closing the OMP connection to a peer. If the peer doesn't receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed.<br>Range: 0 through 65535 seconds<br>Default: 60 seconds |
| **EOR Timer(In Second)** | Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that weren't refreshed after the OMP session came back up are considered to be stale and are deleted from the route table.<br>Range: 1 through 3600 seconds (1 hour)<br>Default: 300 seconds (5 minutes) |
| **Overlay AS** | Specify a BGP AS number that OMP advertises to the BGP neighbors of the router. |
| **Shutdown** | Enable this option to disable OMP and disable the Cisco Catalyst SD-WAN overlay network. OMP is enabled by default. |
| **OMP Admin Distance Ipv4** | To advertise a route over OMP, configure the OMP administrative distance for the IPv4 address lower than the leaked route administrative distance.<br>Range: 1 through 255 |
| **OMP Admin Distance Ipv6** | To advertise a route over OMP, configure the OMP administrative distance for the IPv6 address lower than the leaked route administrative distance.<br>Range: 1 through 255 |

### Timers

| Field | Description |
|---|---|
| **Graceful Restart(In Second)** | Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart.<br>Range: 0 through 604800 seconds (168 hours, or 7 days)<br>Default: 43200 seconds (12 hours) |

### Advertise

| Field | Description |
|---|---|
| **Advertise Ipv4 BGP** | Enable this option to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP. |
| **Advertise Ipv4 OSPF** | Enable this option to advertise external OSPF routes to OMP. By default, external OSPF routes are not advertised to OMP. |
| **Advertise Ipv4 OSPF v3** | Enable this option to advertise external OSPFv3 routes to OMP. By default, external OSPFv3 routes are not advertised to OMP. |
| **Advertise Ipv4 Connected** | Enable this option to advertise connected routes to OMP. By default, connected routes are not advertised to OMP. |
| **Advertise Ipv4 Static** | Enable this option to advertise static routes to OMP. By default static routes are not advertised to OMP. |
| **Advertise Ipv4 LISP** | Enable this option to advertise LISP routes to OMP. By default, LISP routes are not advertised to OMP. |
| **Advertise Ipv4 ISIS** | Enable this option to advertise IS-IS routes to OMP. By default, IS-IS routes are not advertised to OMP. |
| **Advertise Ipv4 EIGRP** | Enable this option to advertise EIGRP routes to OMP. By default, EIGRP routes are not advertised to OMP. |
| **Advertise Ipv6 BGP** | Enable this option to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP. |
| **Advertise Ipv6 OSPF** | Enable this option to advertise external OSPF routes to OMP. By default, external OSPF routes are not advertised to OMP. |
| **Advertise Ipv6 Connected** | Enable this option to advertise connected routes to OMP. By default, connected routes are not advertised to OMP. |
| **Advertise Ipv6 Static** | Enable this option to advertise static routes to OMP. By default static routes are not advertised to OMP. |
| **Advertise Ipv6 LISP** | Enable this option to advertise LISP routes to OMP. By default, LISP routes are not advertised to OMP. |
| **Advertise Ipv6 ISIS** | Enable this option to advertise IS-IS routes to OMP. By default, IS-IS routes are not advertised to OMP. |
| **Advertise Ipv6 EIGRP** | Enable this option to advertise EIGRP routes to OMP. By default, EIGRP routes are not advertised to OMP. |

## SNMP

The application-layer Simple Network Management Protocol (SNMP) provides a communication standard for interaction between SNMP managers and agents. The protocol defines a standardized language that is commonly used for monitoring and managing devices in a network. The SNMP feature helps you configure the SNMP functionality on the Cisco IOS XE Catalyst SD-WAN devices.

The following tables describe the options for configuring the SNMP feature.

### SNMP

| Field | Description |
|---|---|
| **Shutdown** | By default, SNMP is enabled. |
| **Contact Person** | Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN device. It can be a maximum of 255 characters. |
| **Location of Device** | Enter a description of the location of the device. It can be a maximum of 255 characters. |

### SNMP Version

| Field | Description |
|---|---|
| **SNMP Version** | Choose one of the following SNMP versions:<br>• **SNMP v2**<br>• **SNMP v3** |
| **SNMP v2: Add View** | |
| **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 views before adding a community. |
| **Add OID** | Click this option to add object identifiers (OID) and configure the following parameters:<br>• **Id***: Enter the OID of the object. For example, to view the internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the Cisco Catalyst SD-WAN MIB, enter the OID 1.3.6.1.4.1.41916. 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.<br>• **Exclude**: Enable this option to include the OID in the view or disable this option to exclude the OID from the view. |
| **SNMP v2: Add Community** | |
| **Name*** | Enter a name for the community. The name can be from 1 through 32 characters and can include angle brackets (< and >). |
| **User Label*** | (Minimum release: Cisco vManage Release 20.9.2) Enter a label or identifier for the community name. It helps you distinguish or update a community name when there are multiple community names for an SNMP target. |
| **View*** | Choose a view to apply to the community. The view specifies the portion of the MIB tree that the community can access. |

| Field | Description |
|---|---|
| **Authorization*** | Choose **read-only** from the drop-down list. The MIBs supported by Cisco Catalyst SD-WAN do not allow write operations, so you can configure only read-only authorization. |
| **SNMP v2: Add Target** | |
| **VPN ID*** | Enter the number of the VPN to use to reach the trap server.<br>Range: 0 through 65530 |
| **IPv4/IPv6 address of SNMP server*** | Enter the IP address of the SNMP server. |
| **UDP port number to connect to SNMP server*** | Enter the UDP port number for connecting to the SNMP server.<br>Range: 1 though 65535 |
| **Community Name*** | Choose the name of a community that was configured under **Add Community**.<br>This field is applicable only to Cisco vManage Release 20.9.1 and earlier releases. |
| **User Label*** | (Minimum release: Cisco vManage Release 20.9.2) Choose a user label that was configured under **Add Community**. |
| **Source interface for outgoing SNMP trap*** | Enter the interface to use to send traps to the SNMP server that is receiving the trap information. |
| **SNMP v3: Add View** | |
| **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. |
| **Add OID** | Click this option to add object identifiers (OID) and configure the following parameters:<br>• **Id***: Enter the OID of the object. For example, to view the internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the Cisco Catalyst SD-WAN MIB, enter the OID 1.3.6.1.4.1.41916. 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.<br>• **Exclude**: Enable this option to include the OID in the view or disable this option to exclude the OID from the view. |
| **SNMP v3: Add Group** | |
| **Name*** | Enter a name for the trap group. It can be from 1 to 32 characters long. |

| Field | Description |
|---|---|
| **Security Level*** | Choose the authentication to use for the group.<br>• **no-auth-no-priv**: Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials.<br>**auth-no-priv**: Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password.<br>**auth-priv**: Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password and a privacy and privacy password. |
| **View*** | Choose an SNMP view that the trap group can access. |
| **SNMP v3: Add User** | |
| **Name*** | Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters. |
| **Authentication Protocol** | Choose the authentication mechanism for the user:<br>• **md5**<br>• **sha** |
| **Authentication Password** | Enter the authentication password either in cleartext or as an AES-encrypted key. |
| **Privacy Protocol** | Choose the privacy type for the user.<br>• **aes-cfb-128**: Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key. This is a SHA-1 authentication protocol.<br>• **aes-256-cfb-128**: Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 256-bit key. This is a SHA-256 authentication protocol. |
| **Privacy Password** | Enter the privacy password either in cleartext or as an AES-encrypted key. |
| **Group*** | Choose the name of an SNMPv3 group. |
| **SNMP v3: Add Target** | |
| **VPN ID*** | Enter the number of the VPN to use to reach the trap server.<br>Range: 0 through 65530 |
| **IPv4/IPv6 address of SNMP server*** | Enter the IP address of the SNMP server. |

| Field | Description |
|---|---|
| **UDP port number to connect to SNMP server*** | Enter the UDP port number for connecting to the SNMP server.<br>Range: 1 though 65535 |
| **User*** | Choose the name of a user that was configured under **Add User**. |
| **Source interface for outgoing SNMP trap*** | Enter the interface to use to send traps to the SNMP server that is receiving the trap information. |

## Performance Monitoring

Using Cisco SD-WAN Manager, you can monitor the performance of applications.

The following tables describe the options for configuring the Performance Monitoring feature.

### Application Performance Monitoring

| Field | Description |
|---|---|
| **Monitoring** | To enable monitoring, check the check box. You can enable monitoring only in Global mode.<br>Enabling monitoring displays a list of application groups. Fourteen application groups are enabled by default. You can disable or enable more applications based on your requirements. Check the check box adjacent to an application group to enable monitoring. |

### Underlay Measurement Track Service

| Field | Description |
|---|---|
| **Monitoring** | Click **Monitoring** drop-down list, and choose **Global** to trace tunnel paths regularly according to a configured time interval.<br>Click the toggle button to enable the continuous monitoring option in UMTS. |
| **Monitoring Interval (Minutes)** | In the **Monitoring Interval (Minutes)** field, choose a time.<br>This option enables you to monitor exact path at a specific time period. |
| **Event Driven** | Click the **Event Driven** drop-down list, and choose **Global** to trace tunnel paths when triggered by one of the events as per the event type. |
| **Event Type** | Click the **Event Type** drop-down list, and choose an event type. The event types are:<br>• **SLA Change**: Change in the service-level agreement (SLA) parameter for the tunnel.<br>• **PMTU Change**: Change in the Path MTU (PMTU) parameter for the tunnel. |

To save the configuration, click **Save**.

## IPv4 Device Access Policy

Use the IPv4 device access policy to create a device configuration to handle both SSH and SNMP traffic directed towards the control plane.

Device access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies in routed and transparent firewall mode to control IP traffic.

The following tables describe the options for configuring the IPv4 device access policy.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name*** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| **Description** | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |

| Field | Description |
|---|---|
| **Add ACL Sequence** | |
| **ACL Sequence Name** | Enter a name for the ACL Sequence. |
| **Action Type** | Choose one of the following actions for the ACL policy:<br>• **Accept**<br>• **Drop** |
| **Default Action** | The **Default Action** in the left pane is to drop the packets. Change the default action by clicking the ellipsis (**...**) icon. |
| **Condition** | • **Device Access Protocol (required)**: Choose a carrier from the drop-down list. For example, SNMP, SSH.<br>• **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12.<br>• **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535.<br>• **Destination Data Prefix**: Select an existing destination data prefix or provide a destination IP address when you have chosen SSH as the device access protocol. For example, 10.0.0.0/12. |

## IPv6 Device Access Policy

Use the IPv6 device access policy to create a device configuration to handle both SSH and SNMP traffic directed towards the control plane.

Device access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies in routed and transparent firewall mode to control IP traffic.

The following tables describe the options for configuring the IPv6 device access policy.

| Field | Description |
|---|---|
| **Add ACL Sequence** | |
| **ACL Sequence Name** | Enter a name for the ACL Sequence. |
| **Action Type** | Choose one of the following actions for the ACL policy:<br>• **Accept**<br>• **Drop** |
| **Default Action** | The **Default Action** in the left pane is to drop the packets. Change the default action by clicking the ellipsis (**...**) icon. |
| **Condition** | • **Device Access Protocol (required)**: Choose a carrier from the drop-down list. For example, SNMP, SSH.<br>• **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12.<br>• **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535.<br>• **Destination Data Prefix**: Select an existing destination data prefix or provide a destination IP address when you have chosen SSH as the device access protocol. For example, 10.0.0.0/12. |

## Cisco Catalyst SD-WAN Remote Access

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

Cisco Catalyst SD-WAN remote access fully integrates remote access functionality into the Cisco Catalyst SD-WAN fabric, extending the benefits of Cisco Catalyst SD-WAN to remote access users. Cisco Catalyst SD-WAN remote access enables Cisco IOS XE Catalyst SD-WAN devices to provide remote access headend functionality, managed through Cisco SD-WAN Manager.

For more details on Cisco Catalyst SD-WAN remote access feature, see Cisco Catalyst SD-WAN Remote Access.

For information about configuring Cisco Catalyst SD-WAN Remote Access feature, see Configure Cisco Catalyst SD-WAN Remote Access Using Cisco SD-WAN Manager.

### *Configure Remote Access Feature Settings*

The following table describes options to specify the name and description for the remote access feature.

| Field | Description |
|---|---|
| **Type** | Choose Remote Access 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. |
| **Connection Type** | Choose the connection type from the following:<br>• **IPsec**<br>• **SSL-VPN**<br>By default, IPsec is selected. We recommend using IPsec mode. SSL-VPN mode is supported only on Cisco Catalyst 8000v Edge Software with limited features. |

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown.

### Private IP-Pool

The **Private IP-Pool** pane allows you to specify the size of the private IP pool to allocate to a device from the global IP pool for the remote access defined in the network hierarchy. The device uses the private IP pool to assign an IP address to each remote access client.

If you enable the remote access feature through the Create Configuration Group workflow, the workflow creates a global IPv4 pool in Network Hierarchy for remote access use. In Cisco vManage Release 20.11.1, if you want to enable the IPv6 pool for the remote access feature, you must create IPv6 pool manually in the network hierarchy. You can edit the remote access feature in a configuration groups to update the pool size.

To release the IP pool allocated to a device, remove the remote access feature, disable remote access in the service VPN, and successfully deploy the configuration group to the device. Then the IPv4 and IPv6 pools allocated to a device are returned to the global IPv4 and IPv6 pool for remote access, in the network hierarchy. The global remote access pools reflect the latest capacity.

| Field | Description |
|---|---|
| **Maximum Number of Clients** | Enter the maximum number of remote access clients that can connect to a remote access headend device. This number determines the size of the IPv4 pool allocated to the device.<br>If a global IPv6 pool is defined for remote access in the network hierarchy, each SD-WAN RA headend device will be allocated an IPv6 pool sufficient for the maximum number of remote access clients (8000). |

### Authentication

| Field | Description |
|---|---|
| **Radius Group Name** | Choose an existing RADIUS group or create a new RADIUS group.<br>Click **Add Radius Group** to add a RADIUS server and group to the AAA feature profile in the System Profile. |
| **Pre-Shared Key (PSK) Authentication** | Enable Pre-Shared Key (PSK) authentication.<br>• **AAA-based-PSK**: Choose this option to fetch the pre-shared keys from the RADIUS server. This option allows configuring a pre-shared key on the RADIUS server that is unique per remote access client or a group of remote access clients.<br>• **Groups PSK**: Choose this option to configure a common pre-shared key for all remote access clients connecting to a device.<br>**Note** **Pre-Shared Key (PSK) Authentication** is applicable only for connection-type IPsec and not for SSL-VPN. |
| **CA Server Setup** | Choose a CA server for certificate-based authentication. The certificate from the selected CA is used by the device to authenticate the remote access clients.<br>Before choosing a CA server, configure the CA server from **Configuration** > **Certificate Authority**. |
| **User Authentication** | Choose the user authentication option for AnyConnect Extensible Authentication Protocol (EAP) authentication used by remote access client.<br>**Note** The **User Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN. |
| **User & Device Authentication** | Choose the user and device authentication option for AnyConnect EAP authentication used by remote access client.<br>The **User & Device Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN. |
| **Enable Profile Download** | Enable download of an AnyConnect profile XML file to Cisco AnyConnect clients from the remote access headend devices.<br>In the **Upload Profile XML File** pane, choose an XML file or drag and drop to upload. The maximum file size is 20 KB. |

### AAA Policy

| Field | Description |
|---|---|
| **Specify Name** | Choose this option to specify the name of the policy to look up on the RADIUS server.<br>In the **Policy Name** field, which appears only for the **Specify Name** option, enter the name of the policy. |
| **Derive Name from Peer Identity** | Choose this option to use the identity of the peer as the name of the policy to lookup on the RADIUS server.<br>**Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN. |
| **Derive Name from Peer Identity Domain** | Choose this option to use the domain portion of the identity of the peer as the name of the policy to look up on the RADIUS server.<br>**Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN. |
| **Policy Password** | Enter the policy password. |
| **Enable Accounting** | Enable accounting. |

**Note** The IKEv2 and IPsec settings are applicable only for the IPsec connection type and not for SSL-VPN.

### IKEv2 and IPsec Settings

| Field | Description |
|---|---|
| **Local IKE Identity Type** | Enter the local IKEv2 identity type. The options are:<br>• IPv4 Address or IPv6 Address<br>• Email<br>• FQDN<br>• Key-ID |
| **Local IKE Identity Value*** | Enter the value of the local IKEv2 identity based on the identity type selected. |
| **Security Association (SA) Lifetime** | Enter the lifetime in seconds for the IKEv2 security association.<br>The range is from 3600 to 86400. The default lifetime is 86400 seconds. |
| **Enable Anti - Denial of Service (DOS) Check** | Enable an Anti-Denial of Service (DOS) check. |

| Field | Description |
|---|---|
| **Anti-DOS Threshold** | Enter the Anti-DOS threshold value.<br>Range: 10 to 1000.<br>Default: 100. |

## Flexible Port Speed

The Flexible Port Speed feature is applicable only to the Cisco Catalyst 8500-12X4QC router. Use this feature to configure interfaces to work as 100GE, 40GE, 10GE, or 1GE based on your requirement. Any changes made to the port type take effect only after applying the configuration group to devices.

Updating the port configuration using the Flexible Port Speed feature may enable some ports and disable others. For instance, by default , C8500-12X4QC operates Bay 1 in 10GE mode and Bay 2 in 40GE mode. The Bay 1 mode can be 10GE, 40GE, or 100GE. Setting Bay 1 to 100GE disables all ports of Bay 0. For more information, see Bay Configuration of the Cisco Catalyst 8500-12X4QC device.

**Note** In Cisco Catalyst SD-WAN Manager Release 20.13.1, you cannot update the Cisco Catalyst 8500-12X4QC port configuration to 2 ports of 100GE by using the Flexible Port Speed feature.

For more information about the Cisco Catalyst 8500-12X4QC platform's port options in each of its bays, see the C8500-12X4QC product overview in the *Cisco Catalyst 8500 Series Edge Platforms Data Sheet*.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the field. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value appears for parameters that have a default setting. |

### Basic Settings

| Parameter Name | Description |
|---|---|
| Port Type | Choose from one of the following port combinations:<br>• **12 ports of 1/10GE + 3 ports of 40GE**<br>• **8 ports of 1/10GE + 4 ports of 40GE**<br>• **2 ports of 100GE**<br>• **12 ports of 1/10GE + 1 port of 100GE**<br>• **8 ports of 1/10GE + 1 port of 40GE + 1 port of 100GE**<br>• **3 ports of 40GE + 1 port of 100GE**<br>Default is 12 ports of 1/10GE + 3 ports of 40GE. |

## Transport and Management Profile

### Transport VPN

The Transport VPN feature helps you configure VPN 0 or the WAN VPN.

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown.

The following table describes the options for configuring the Transport VPN feature.

#### Basic Configuration

| Field | Description |
|---|---|
| **VPN** | Enter the numeric identifier of the VPN. |
| **Enhance ECMP Keying** | Enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key.<br>Default: Disabled |

#### DNS

| Field | Description |
|---|---|
| **Add DNS** | |
| **Primary DNS Address (IPv4)** | Enter the IP address of the primary IPv4 DNS server in this VPN. |
| **Secondary DNS Address (IPv4)** | Enter the IP address of a secondary IPv4 DNS server in this VPN. |

| Field | Description |
|---|---|
| **Add DNS IPv6** | |
| **Primary DNS Address (IPv6)** | Enter the IP address of the primary IPv6 DNS server in this VPN. |
| **Secondary DNS Address (IPv6)** | Enter the IP address of a secondary IPv6 DNS server in this VPN. |

### Host Mapping

| Field | Description |
|---|---|
| **Add New Host Mapping** | |
| **Hostname*** | Enter the hostname of the DNS server. The name can be up to 128 characters. |
| **List of IP*** | Enter up to 14 IP addresses to associate with the hostname. Separate the entries with commas. |

### Route

| Field | Description |
|---|---|
| **Add IPv4 Static Route** | |
| **Network address*** | Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN. |
| **Subnet Mask*** | Enter the subnet mask. |
| **Gateway*** | Choose one of the following options to configure the next hop to reach the static route:<br>• **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear:<br>  • **Address***: Enter the next-hop IPv4 address.<br>  • **Administrative distance***: Enter the administrative distance for the route.<br>• **dhcp**<br>• **null0**: When you choose this option, the following field appears:<br>  • **Administrative distance**: Enter the administrative distance for the route. |
| **Add IPv6 Static Route** | |
| **Prefix*** | Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN. |

| Field | Description |
|---|---|
| **Next Hop/Null 0/NAT** | Choose one of the following options to configure the next hop to reach the static route:<br>• **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear:<br>• **Address***: Enter the next-hop IPv6 address.<br>**Administrative distance***: Enter the administrative distance for the route.<br>• **Null 0**: When you choose this option, the following field appears:<br>• **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages.<br>• **NAT**: When you choose this option, the following field appears:<br>• **IPv6 NAT***: Choose NAT64 or NAT66. |
| **Add BGP Routing** | Choose a BGP route. |

### NAT

| Field | Description |
|---|---|
| **Add NAT64 v4 Pool** | |
| **NAT64 v4 Pool Name*** | Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router. |
| **NAT64 Pool Range Start*** | Enter a starting IP address for the NAT pool. |
| **NAT64 Pool Range End*** | Enter a closing IP address for the NAT pool. |
| **NAT64 Overload** | Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured.<br>Default: Disabled |

### Service

| Field | Description |
|---|---|
| **Add Service** | |
| **Service Type** | Choose the service available in the VPN.<br>Value: **TE** |

## Ethernet Interface

This feature helps you configure Ethernet interface in VPN 0 or the WAN VPN.

The following table describes the options for configuring the Ethernet Interface feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Associated VPN** | Choose a VPN. |
| **Associated Tracker/Trackergroup** | Choose a tracker or tracker group. |

### Basic Configuration

| Field | Description |
|---|---|
| **Shutdown** | Enable or disable the interface. |
| **Interface Name*** | Enter a name for the interface. Spell out the interface names completely (for example, GigabitEthernet0/0/0).<br>Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured. |
| **Description** | Enter a description for the interface. |
| **Auto Detect Bandwidth** | Enable this option to automatically detect the bandwidth for WAN interfaces. The device detects the bandwidth by contacting an iPerf3 server to perform a speed test. |
| **IPv4 Settings** | Configure an IPv4 VPN interface.<br>• **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server.<br>• **Static**: Choose **Static** to enter an IP address that doesn't change. |
| **Dynamic DHCP Distance** | Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**.<br>Default: 1 |
| **IP Address** | Enter a static IPv4 address. This option is available when you choose **Static**. |
| **Subnet Mask** | Enter the subnet mask. |
| **Configure Secondary IP Address** | Enter up to four secondary IPv4 addresses for a service-side interface.<br>• **IP Address**: Enter the IP address.<br>• **Subnet Mask:** Enter the subnet mask. |

| Field | Description |
|---|---|
| **DHCP Helper** | To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BOOTP (broadcast) DHCP requests that it receives from the specified DHCP servers. |
| **IPv6 Settings** | Configure an IPv6 VPN interface.<br>• **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server.<br>• **Static**: Choose **Static** to enter an IP address that doesn't change.<br>• **None** |
| **IPv6 Address Primary** | Enter a static IPv6 address. This option is available when you choose **Static**. |
| **Add Secondary Ipv6** | |
| **IP Address** | Enter up to two secondary IPv6 addresses for a service-side interface. |

### Tunnel

### NAT

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **NAT** | Enable this option to have the interface act as a NAT device. |
| **NAT Type** | Choose the NAT translation type for IPv4:<br>• **interface**<br>• **pool**<br>• **loopback**<br>Default: **interface**. It is supported for NAT64. |
| **UDP Timeout** | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 1 minute |
| **TCP Timeout** | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 60 minutes (1 hour) |
| **Configure New Static NAT** | Add a static NAT mapping |

| Field | Description |
|---|---|
| **Source IP** | Enter the source IP address to be translated. |
| **Translate IP** | Enter the translated source IP address. |
| **Direction** | Choose the direction in which to perform network address translation.<br>• **inside**: Translates the IP address of packets that are coming from the service side of the device and that are destined for the transport side of the router.<br>• **outside**: Translates the IP address of packets that are coming to the device from the transport side device and that are destined for a service-side device. |
| **Source VPN** | Enter the source VPN ID. |
| **IPv6 Settings** | |
| **IPv6 NAT** | Enable this option to have the interface act as a NAT device. |
| **Select NAT** | Choose NAT64 or NAT66. When you choose NAT66, the following fields appear:<br>• **Source Prefix**: Enter the source IPv6 prefix.<br>• **Translated Source Prefix**: Enter the translated source prefix.<br>• **Source VPN ID**: Enter the source VPN ID.<br>• **Egress Interface**: Enable this option to have the interface act as an egress interface. |

### ARP

| Field | Description |
|---|---|
| **IP Address** | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| **MAC Address** | Enter the MAC address in colon-separated hexadecimal notation. |

### Advanced

| Field | Description |
|---|---|
| **Duplex** | Specify whether the interface runs in full-duplex or half-duplex mode.<br>Default: full |
| **MAC Address** | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |

| Field | Description |
|---|---|
| **IP MTU** | Specify the maximum MTU size of packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **Interface MTU** | Enter the maximum transmission unit size for frames received and transmitted on the interface.<br>Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet)<br>Default: 1500 bytes |
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 500 to 1460 bytes<br>Default: None |
| **Speed** | Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation.<br>Values: 10, 100, 1000, 2500, or 10000 Mbps |
| **ARP Timeout** | ARP timeout controls how long we maintain the ARP cache on a router. Specify how long it takes for a dynamically learned ARP entry to time out.<br>Range: 0 through 2147483 seconds<br>Default: 1200 seconds |
| **Autonegotiate** | Enable this option to turn on autonegotiation. |
| **Media Type** | Specify the physical media connection type on the interface. Choose one of the following:<br>• **auto-select**: A connection is automatically selected.<br>• **rj45**: Specifies an RJ-45 physical connection.<br>• **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media. |

| Field | Description |
|---|---|
| **TLOC Extension** | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.<br>**Note** TLOC extension over L3 is supported only for Cisco IOS XE Catalyst SD-WAN devices. If configuring TLOC extension over L3 for a Cisco IOS XE Catalyst SD-WAN device, enter the IP address of the L3 interface. |
| **GRE tunnel source IP** | Enter the IP address of the extended WAN interface. |
| **XConnect** | Enter the name of a physical interface on the same router that connects to the WAN transport. |
| **Load Interval** | Enter an interval value for interface load calculation. |
| **IP Directed Broadcast** | An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.<br>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.<br>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet. |
| **ICMP Redirect Disable** | ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway.<br>By default, an interface allows ICMP redirect messages. |

## Management VPN

This feature helps you configure VPN 512 or the management VPN.

The following table describes the options for configuring the Management VPN 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. |

### Basic Configuration

| Field | Description |
|---|---|
| **VPN** | Management VPN carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices. |
| **Name** | Enter a name for the interface. |

### DNS

| Field | Description |
|---|---|
| **Add DNS** | |
| **Primary DNS Address (IPv4)** | Enter the IPv4 address of the primary DNS server in this VPN. |
| **Secondary DNS Address (IPv4)** | Enter the IPv4 address of a secondary DNS server in this VPN. |
| **Add DNS IPv6** | |
| **Primary DNS Address (IPv6)** | Enter the IPv6 address of the primary DNS server in this VPN. |
| **Secondary DNS Address (IPv6)** | Enter the IPv6 address of a secondary DNS server in this VPN. |

### Host Mapping

| Field | Description |
|---|---|
| **Add New Host Mapping** | |
| **Hostname*** | Enter the hostname of the DNS server. The name can be up to 128 characters. |
| **List of IP Address*** | Enter IP addresses to associate with the hostname. Separate the entries with commas. |

### IPv4/IPv6 Static Route

| Field | Description |
|---|---|
| **Add IPv4 Static Route** | |
| **IP Address*** | Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN. |
| **Subnet Mask*** | Enter the subnet mask. |
| **Gateway*** | Choose one of the following options to configure the next hop to reach the static route:<br>• **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear:<br>  • **Address***: Enter the next-hop IPv4 address.<br>  • **Administrative distance***: Enter the administrative distance for the route.<br>• **dhcp**<br>• **null0**: When you choose this option, the following field appears:<br>  • **Administrative distance**: Enter the administrative distance for the route. |
| **Add IPv6 Static Route** | |
| **Prefix*** | Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN. |
| **Next Hop/Null 0/NAT** | Choose one of the following options to configure the next hop to reach the static route:<br>• **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear:<br>  • **Address***: Enter the next-hop IPv6 address.<br>  **Administrative distance***: Enter the administrative distance for the route.<br>• **Null 0**: When you choose this option, the following field appears:<br>  • **NULL0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages.<br>• **NAT**: When you choose this option, the following field appears:<br>  • **IPv6 NAT**: Choose NAT64 or NAT66. |

## Management Ethernet Interface

This feature helps you configure Ethernet Interface in VPN 512 or the management VPN.

The following table describes the options for configuring the Management Ethernet Interface feature.

| Field | Description |
|---|---|
| **Associated VPN** | Management VPN or VPN 512. |

### Basic Configuration

| Field | Description |
|---|---|
| **Shutdown** | Enable or disable the interface. |
| **Interface Name** | Enter a name for the interface. Spell out the interface names completely (for example, GigabitEthernet1). |
| **Description** | Enter a description for the interface. |
| **IPv4 Settings** | Configure an IPv4 VPN interface.<br>• **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server.<br>• **Static**: Choose **Static** to enter an IP address that doesn't change. |
| **Dynamic DHCP Distance** | Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**.<br>Default: 1 |
| **DHCP Helper** | To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BOOTP (broadcast) DHCP requests that it receives from the specified DHCP servers. |
| **Iperf server for auto bandwidth detect** | 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. |
| **Auto Detect Bandwidth** | Enable this option so that the device detects the bandwidth. |
| **IPv6 Settings** | Configure an IPv6 VPN interface.<br>• **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server.<br>• **Static**: Choose **Static** to enter an IP address that doesn't change.<br>• **None** |
| **IPv6 Address Primary** | Enter a static IPv6 address. This option is available when you choose **Static**. |

### NAT

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **NAT** | Enable this option to have the interface act as a NAT device. |
| **NAT Type** | Choose the NAT translation type for IPv4:<br>• **interface**<br>• **pool**<br>• **loopback**<br>Default: **interface** |
| **UDP Timeout** | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 1 minute |
| **TCP Timeout** | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 60 minutes (1 hour) |
| **Configure New Static NAT** | Add a static NAT mapping |
| **Source IP** | Enter the source IP address to be translated. |
| **Translate IP** | Enter the translated source IP address. |
| **Direction** | Choose the direction in which to perform network address translation.<br>• **inside**: Translates the IP address of packets that are coming from the service side of the device and that are destined for the transport side of the router.<br>• **outside**: Translates the IP address of packets that are coming to the device from the transport side device and that are destined for a service-side device. |
| **Source VPN** | Enter the source VPN ID. |
| **IPv6 Settings** | |
| **NAT** | Enable this option to have the interface act as a NAT device. |

| Field | Description |
|---|---|
| **Select NAT** | Choose NAT64 or NAT66. When you choose NAT66, the following fields appear:<br>• **Source Prefix**: Enter the source IPv6 prefix.<br>• **Translated Source Prefix**: Enter the translated source prefix.<br>• **Source VPN ID**: Enter the source VPN ID. |

### ARP

| Field | Description |
|---|---|
| **IP Address** | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| **MAC Address** | Enter the MAC address in colon-separated hexadecimal notation. |

### Advanced

| Field | Description |
|---|---|
| **Duplex** | Specify whether the interface runs in full-duplex or half-duplex mode. |
| **MAC Address** | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| **IP MTU** | Specify the maximum MTU size of packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 500 to 1460 bytes<br>Default: None |
| **Speed** | Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation.<br>Values: 10, 100, 1000, 2500, or 10000 Mbps |
| **ARP Timeout** | ARP timeout controls how long we maintain the ARP cache on a router. Specify how long it takes for a dynamically learned ARP entry to time out.<br>Range: 0 through 2147483 seconds<br>Default: 1200 seconds |

| Field | Description |
|---|---|
| **Autonegotiate** | Enable this option to turn on autonegotiation. |
| **Media Type** | Specify the physical media connection type on the interface. Choose one of the following:<br>• **auto-select**: A connection is automatically selected.<br>• **rj45**: Specifies an RJ-45 physical connection.<br>• **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media. |
| **XConnect** | Enter the name of a physical interface on the same router that connects to the WAN transport. |
| **Load Interval** | Enter an interval value for interface load calculation. |
| **ICMP/ICMPv6 Redirect Disable** | ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway.<br>By default, an interface allows ICMP redirect messages. |
| **IP Directed Broadcast** | An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.<br>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.<br>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet. |

## Cellular Controller

This feature helps you configure a cellular controller in VPN 0 or the WAN VPN.

The following table describes the options for configuring the Cellular Controller feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |

| Field | Description |
|---|---|
| **Description** | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |
| **Cellular ID** | Enter the interface slot and port number in which the cellular NIM card is installed. Currently, it can be 0/1/0 or 0/2/0. |
| **Primary SIM slot** | Enter the number of the primary SIM slot. It can be 0 or 1. The other slot is automatically set to be the secondary. If there is a single SIM slot, this parameter is not applicable. |
| **SIM Failover Retries** | Specify the maximum number of times to retry connecting to the secondary SIM when service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.<br>Range: 0 through 65535<br>Default: 10 |
| **SIM Failover Timeout** | Specify how long to wait before switching from the primary SIM to the secondary SIM if service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.<br>Range: 3 to 7 minutes<br>Default: 3 minutes |
| **Firmware Auto Sim** | By default, this option is enabled. AutoSIM analyzes any active SIM card and determines which service provider network is associated with that SIM. Based on that analysis, AutoSIM automatically loads the appropriate firmware. |

After configuring the above parameters, choose a cellular profile to associate with the cellular controller and click **Save**.

## Cellular Profile

This feature helps you configure a cellular profile in VPN 0 or the WAN VPN.

The following table describes the options for configuring the Cellular Profile feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| **Description** | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |
| **Profile ID** | Enter the identification number of the profile to use on the router.<br>Range: 1 through 15 |

| Field | Description |
|---|---|
| **Access Point Name** | Enter the name of the gateway between the service provider network and the public internet. It can be up to 32 characters long. |
| **Authentication** | Choose the authentication method used for the connection to the cellular network. It can be **none**, **pap**, **chap**, or **pap_chap**. |
| **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. |
| **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. |
| **Packet Data Network Type** | Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv4v6. |
| **No Overwrite** | Enable this option to overwrite the profile on the cellular modem. By default, this option is disabled. |

## Tracker

This feature helps you configure the tracker for the VPN interface.

For each parameter of the feature 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 to the left of the parameter field and choose one of the following:

The following table describes the options for configuring the Tracker feature.

| Field | Description |
|---|---|
| **Tracker Name*** | Name of the tracker. The name can be up to 128 alphanumeric characters. |
| **Endpoint Tracker Type*** | Choose a tracker type to configure endpoint trackers:<br>• **http** |

| Field | Description |
|---|---|
| **Endpoint** | Choose an endpoint type:<br>• **Endpoint IP**: When you choose this option, the following field appears:<br>**Endpoint IP**: IP address of the endpoint. This is the destination on the internet to which the probes are sent to determine the status of an endpoint.<br>• **Endpoint DNS Name**: When you choose this option, the following field appears:<br>**Endpoint DNS Name**: DNS name of the endpoint. This is the destination on the internet to which probes are sent to determine the status of the endpoint. The DNS name can contain a minimum of one character and a maximum of 253 characters.<br>• **Endpoint API URL**:<br>When you choose this option, the following field appears:<br>**API URL of endpoint***: API URL for the endpoint of the tunnel. This is the destination on the internet to which probes are sent to determine the status of the endpoint. |
| **Interval** | Time interval between probes to determine the status of the configured endpoint.<br>Range: 20 to 600 seconds<br>Default: 60 seconds (1 minute). |
| **Multiplier** | Number of times probes are sent before declaring that the endpoint is down.<br>Range: 1 to 10<br>Default: 3 |
| **Threshold** | Wait time for the probe to return a response before declaring that the configured endpoint is down.<br>Range: 100 to 1000 milliseconds<br>Default: 300 milliseconds |

## Cellular Interface

This feature helps you configure the cellular interface in VPN 0 or the WAN VPN.

The following tables describe the options for configuring the Cellular Interface 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. |
| **Associated VPN** | VPN 0 or the WAN transport VPN. |
| **Associated Tracker** | Choose a tracker. |

### Basic Configuration

| Field | Description |
|---|---|
| **Shutdown*** | Enable or disable the interface. |
| **Interface Name*** | Enter the name of the interface. |
| **Description*** | Enter a description of the cellular interface. |
| **DHCP Helper** | Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |

### Tunnel

| Field | Description |
|---|---|
| **Tunnel Interface** | Enable this option to create a tunnel interface. |
| **Carrier** | Choose the carrier name or private network identifier to associate with the tunnel.<br>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>Default: default |
| **Color** | Choose a color for the TLOC. |
| **Hello Interval** | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>Range: 100 through 600000 milliseconds<br>Default: 1000 milliseconds (1 second) |
| **Hello Tolerance** | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>Range: 12 through 6000 seconds<br>Default: 12 seconds |
| **Last-Resort Circuit** | Enable this option to use the tunnel interface as the circuit of last resort. |

| Field | Description |
|---|---|
| **Restrict** | Enable this option to limit the remote TLOCs that the local TLOC can establish BFD sessions with. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color. |
| **Group** | Enter a group number.<br>Range: 1 through 4294967295 |
| **Border** | Enable this option to set the TLOC as a border TLOC. |
| **Maximum Control Connections** | Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>Range: 0 through 100<br>Default: 2 |
| **NAT Refresh Interval** | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>Range: 1 through 60 seconds<br>Default: 5 seconds |
| **Validator As Stun Server** | Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT. |
| **Exclude Controller Group List** | Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allowed to connect to.<br>Range: 1 through 100 |
| **Manager Connection Preference** | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager.<br>Range: 0 through 8<br>Default: 5 |
| **Port Hop** | Enable port hopping. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value.<br>Default: Enabled |
| **Low-Bandwidth Link** | Enable this option to characterize the tunnel interface as a low-bandwidth link. |

| Field | Description |
|---|---|
| **Tunnel TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 500 to 1460 bytes<br>Default: None |
| **Clear-Dont-Fragment** | Enable this option to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. |
| **Network Broadcast** | Enable this option to accept and respond to network-prefix-directed broadcasts. |
| **Allow Service** | Allow or disallow the following services on the interface:<br>• **All**<br>• **BGP**<br>• **DHCP**<br>• **NTP**<br>• **SSH**<br>• **DNS**<br>• **ICMP**<br>• **HTTPS**<br>• **OSPF**<br>• **STUN**<br>• **SNMP**<br>• **NETCONF**<br>• **BFD** |
| **Encapsulation** | |
| **GRE** | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |

| Field | Description |
|---|---|
| **GRE Preference** | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0 |
| **GRE Weight** | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1 |
| **IPsec** | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| **IPsec Preference** | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0 |
| **IPsec Weight** | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1 |

### NAT

| Field | Description |
|---|---|
| **NAT** | Enable this option to have the interface act as a NAT device. |
| **UDP Timeout*** | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 1 minutes |
| **TCP Timeout*** | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 60 minutes (1 hour) |

### ARP

| Field | Description |
|---|---|
| **IP Address*** | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| **MAC Address*** | Enter the MAC address in colon-separated hexadecimal notation. |

### Advanced

| Field | Description |
|---|---|
| **MAC Address** | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| **IP MTU** | Specify the maximum MTU size of packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **Interface MTU** | Enter the maximum transmission unit size for frames received and transmitted on the interface.<br>Range: 1500 through 9216<br>Default: 1500 bytes |
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 500 to 1460 bytes<br>Default: None |
| **TLOC Extension** | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.<br>**Note** TLOC extension over L3 is supported only for Cisco IOS XE Catalyst SD-WAN devices. If configuring TLOC extension over L3 for a Cisco IOS XE Catalyst SD-WAN device, enter the IP address of the L3 interface. |

| Field | Description |
|---|---|
| **Tracker** | Tracking the interface status is useful when you enable NAT on 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 on 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.<br><br>When you enable transport tunnel tracking, Cisco Catalyst SD-WAN periodically probes the path to the internet to determine whether it is up. If Cisco Catalyst SD-WAN 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 Cisco Catalyst SD-WAN detects that the path to the internet is again functioning, the route to the internet is reinstalled.<br><br>Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| **IP Directed-Broadcast** | An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.<br><br>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.<br><br>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet. |

## BGP Routing

This feature helps you configure the Border Gateway Protocol (BGP) routing in VPN 0 or the WAN VPN.

For each parameter of the feature 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 to the left of the parameter field and choose one of the following:

### Basic Configuration

| Field | Description |
|---|---|
| **AS Number** | Enter the local AS number. |
| **Router ID** | Enter the BGP router ID, in decimal four-part dotted notation. |
| **Propagate AS Path** | Enable this option to carry BGP AS path information into OMP. |

| Field | Description |
|---|---|
| **Propagate Community** | Enable this option to propagate BGP communities between Cisco Catalyst SD-WAN sites, across VPNs using OMP redistribution. |
| **External Routes Distance** | Specify the BGP route administrative distance for routes learned from other sites in the overlay network.<br>Range: 1 through 255<br>Default: 20 |
| **Internal Routes Distance** | Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another.<br>Range: 1 through 255<br>Default: 200 |
| **Local Routes Distance** | Specify the BGP route administrative distance for routes within the local AS. By default, a route received locally from BGP is preferred over a route received from OMP.<br>Range: 1 through 255<br>Default: 20 |

### Unicast Address Family

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **Maximum Paths** | Specify the maximum number of parallel internal BGP paths that can be installed into a route table to enable internal BGP multipath load sharing.<br>Range: 0 to 32 |
| **Originate** | Enable this option to allow the default route to be artificially generated and injected into the BGP Route Information Base (RIB), regardless of whether it is present in the routing table. The newly injected default is advertised to all the BGP peers. |
| **Redistribute** | |
| **Protocol*** | Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, **eigrp**, and **nat**.<br>At a minimum, choose **connected**, and then under **Route Policy**, specify a route policy that has BGP advertise the loopback interface address to its neighbors.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Route Policy** | Enter the name of the route policy to apply to redistributed routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |

| Field | Description |
|---|---|
| **Network** | |
| **Network Prefix*** | Enter a network prefix to be advertised by BGP. The network prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0. |
| **Aggregate Address** | |
| **Aggregate Prefix*** | Enter the prefix of the addresses to aggregate for all BGP sessions. The aggregate prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0. |
| **AS Set Path** | Enable this option to generate set path information for the aggregated prefixes. |
| **Summary Only** | Enable this option to filter out more specific routes from BGP updates. |
| **Table Map** | |
| **Policy Name** | Enter the route map that controls the downloading of routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Filter** | When you enable this option, the route map specified in the **Policy Name** field controls whether a BGP route is to be downloaded to the Route Information Base (RIB). A BGP route is not downloaded to the RIB if it is denied by the route map.<br>When you disable this option, the route map specified in the **Policy Name** field is used to set certain properties, such as the traffic index, of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map. |
| **IPv6 Settings** | |
| **Maximum Paths** | Specify the maximum number of parallel internal BGP paths that can be installed into a route table to enable internal BGP multipath load sharing.<br>Range: 0 to 32 |
| **Originate** | Enable this option to allow the default route to be artificially generated and injected into the BGP Route Information Base (RIB), regardless of whether it is present in the routing table. The newly injected default is advertised to all the BGP peers. |
| **Redistribute** | |
| **Protocol*** | Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, and **eigrp**.<br>At a minimum, choose **connected**, and then under **Route Policy**, specify a route policy that has BGP advertise the loopback interface address to its neighbors.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |

| Field | Description |
|---|---|
| **Route Policy** | Enter the name of the route policy to apply to redistributed routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Network** | |
| **Network Prefix*** | Enter a network prefix to be advertised by BGP. The IPv6 network prefix is composed of the IPv6 address and the prefix length (1-128). For example, the IPv6 subnet is 2001:DB8:0000:0000:: and the prefix length is 64. |
| **Aggregate Address** | |
| **Aggregate Prefix*** | Enter the prefix of the addresses to aggregate for all BGP sessions. The IPv6 aggregate prefix is composed of the IPv6 address and the prefix length (1-128). For example, the IPv6 subnet is 2001:DB8:0000:0000:: and the prefix length is 64. |
| **AS Set Path** | Enable this option to generate set path information for the aggregated prefixes. |
| **Summary Only** | Enable this option to filter out more specific routes from BGP updates. |
| **Table Map** | |
| **Policy Name** | Enter the route map that controls the downloading of routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Filter** | When you enable this option, the route map specified in the **Policy Name** field controls whether a BGP route is to be downloaded to the Route Information Base (RIB). A BGP route is not downloaded to the RIB if it is denied by the route map.<br>When you disable this option, the route map specified in the **Policy Name** field is used to set certain properties, such as the traffic index, of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map. |

### MPLS Interface

| Field | Description |
|---|---|
| **Interface Name*** | Enter a name for the MPLS interface. |

### Neighbor

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **Address*** | Specify the IP address of the BGP neighbor. |

| Field | Description |
|---|---|
| **Description** | Enter a description of the BGP neighbor. |
| **Remote AS*** | Enter the AS number of the remote BGP peer. |
| **Interface Name** | Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface. |
| **Allows in Number** | Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used. |
| **AS Override** | Enable this option to replace the AS number of the originating router with the AS number of the sending BGP router. |
| **Shutdown** | Disable this option to enable BGP for the VPN. |
| **Advanced Options** | |
| **Next-Hop Self** | Enable this option to configure the router to be the next hop for routes advertised to the BGP neighbor. |
| **Send Community** | Enable this option to send the BGP community attribute of the local router to the BGP neighbor. |
| **Send Extended Community** | Enable this option to send the BGP extended community attribute of the local router to the BGP neighbor. |
| **EBGP Multihop** | Set the time to live (TTL) for BGP connections to external peers.<br>Range: 1 to 255<br>Default: 1 |
| **Password** | Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number. |
| **Keepalive Time (seconds)** | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. Specify the keepalive time for the neighbor, to override the global keepalive time.<br>Range: 0 through 65535 seconds<br>Default: 60 seconds (one-third the hold-time value) |

| Field | Description |
|---|---|
| **Hold Time (seconds)** | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor, to override the global hold time.<br>Range: 0 through 65535 seconds<br>Default: 180 seconds (three times the keepalive time) |
| **Send Label** | Enable this option to allow the routers advertise to each other so that they can send MPLS labels with the routes. If the routers successfully negotiate their ability to send MPLS labels, the routers add MPLS labels to all the outgoing BGP updates. |
| **Add Neighbor Address Family** | |
| **Family Type*** | Choose the BGP IPv4 unicast address family. |
| **In Route Policy** | Specify the name of a route policy to apply to prefixes received from the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Out Route Policy** | Specify the name of a route policy to apply to prefixes sent to the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |

| Field | Description |
|---|---|
| **Maximum Prefix Reach Policy*** | Choose one of the following options:<br>• **Policy Off**: Policy is off.<br>• **Policy On - Restart**: Configure the time interval at which a peering session is re-established by a device when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit.<br>When you choose this option, the following fields appear:<br>• **Maximum Number of Prefixes***: Enter the maximum prefix limit.<br>Range: 1 to 4294967295<br>• **Threshold (percentage)**: Enter the threshold value:<br>Range: 1 to 100<br>Default: 75<br>• **Restart Interval (minutes)***: Enter the time interval.<br>Range: 1 to 65535 minutes<br>• **Policy On - Warning message**: Configure the device to disable the restart capability to allow you to adjust a peer that is sending too many prefixes.<br>• **Policy On - Disable Peer Neighbor**: When the device receives too many prefixes from a peer, and the maximum prefix limit is exceeded, the peering session is disabled or brought down. |
| **IPv6 Settings** | |
| **Address*** | Specify the IP address of the BGP neighbor. |
| **Description** | Enter a description of the BGP neighbor. |
| **Remote AS*** | Enter the AS number of the remote BGP peer. |
| **Interface Name** | Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface. |
| **Allowas in Number** | Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used. |
| **AS Override** | Enable this option to replace the AS number of the originating router with the AS number of the sending BGP router. |
| **Shutdown** | Disable this option to enable BGP for the VPN. |

| Field | Description |
|---|---|
| **Advanced Options** | |
| **Next-Hop Self** | Enable this option to configure the router to be the next hop for routes advertised to the BGP neighbor. |
| **Send Community** | Enable this option to send the BGP community attribute of the local router to the BGP neighbor. |
| **Send Extended Community** | Enable this option to send the BGP extended community attribute of the local router to the BGP neighbor. |
| **EBGP Multihop** | Set the time to live (TTL) for BGP connections to external peers.<br>Range: 1 to 255<br>Default: 1 |
| **Password** | Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number. |
| **Keepalive Time (seconds)** | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. Specify the keepalive time for the neighbor, to override the global keepalive time.<br>Range: 0 through 65535 seconds<br>Default: 60 seconds (one-third the hold-time value) |
| **Hold Time (seconds)** | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor, to override the global hold time.<br>Range: 0 through 65535 seconds<br>Default: 180 seconds (three times the keepalive time) |
| **Add IPv6 Neighbor Address Family** | |
| **Family Type*** | Choose the BGP IPv6 unicast address family. |
| **In Route Policy** | Specify the name of a route policy to apply to prefixes received from the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Out Route Policy** | Specify the name of a route policy to apply to prefixes sent to the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |

| Field | Description |
|---|---|
| **Maximum Prefix Reach Policy*** | Choose one of the following options:<br>• **Policy Off**: Policy is off.<br>• **Policy On - Restart**: Configure the time interval at which a peering session is re-established by a device when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit.<br>When you choose this option, the following fields appear:<br>• **Maximum Number of Prefixes***: Enter the maximum prefix limit.<br>Range: 1 to 4294967295<br>• **Threshold (percentage)**: Enter the threshold value:<br>Range: 1 to 100<br>Default: 75<br>• **Restart Interval (minutes)***: Enter the time interval.<br>Range: 1 to 65535 minutes<br>• **Policy On - Warning message**: Configure the device to disable the restart capability to allow you to adjust a peer that is sending too many prefixes.<br>• **Policy On - Disable Peer Neighbor**: When the device receives too many prefixes from a peer, and the maximum prefix limit is exceeded, the peering session is disabled or brought down. |

### Advanced

| Field | Description |
|---|---|
| **Keepalive (seconds)** | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. This keepalive time is the global keepalive time.<br>Range: 0 through 65535 seconds<br>Default: 60 seconds (one-third the hold-time value) |
| **Hold Time (seconds)** | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. This hold time is the global hold time.<br>Range: 0 through 65535 seconds<br>Default: 180 seconds (three times the keepalive time) |

| Field | Description |
|---|---|
| **Compare MED** | Enable this option to compare the router IDs among BGP paths to determine the active path. |
| **Deterministic MED** | Enable this option to compare MEDs from all routes received from the same AS regardless of when the route was received. |
| **Missing MED as Worst** | Enable this option to consider a path as the worst path if the path is missing a MED attribute. |
| **Compare Router ID** | Enable this option to always compare MEDs regardless of whether the peer ASs of the compared routes are the same. |
| **Multipath Relax** | Enable this option to have the BGP best-path process select from routes in different ASs. By default, when you are using BGP multipath, the BGP best-path process selects from routes in the same AS to load-balance across multiple paths. |

## IPSEC

Use the IPsec feature to configure IPsec tunnels on Cisco IOS XE Catalyst SD-WAN devices that are being used for Internet Key Exchange (IKE) sessions.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the following table:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value appears for parameters that have a default setting. |

The following tables describe the options for configuring the VPN Interface IPsec 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. |

### Basic Configuration

| Field | Description |
|---|---|
| **Interface Name** | Enter the name of the IPsec interface. |
| **Description** | Enter a description of the IPsec interface. |
| **Interface Address** | Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list. |
| **Mask** | Enter the subnet mask. |
| **Preshared Key for IKE** | Enter the preshared key (PSK) for authentication. |
| **Associated Tracker / Tracker Group** | Choose a tracker or a tracker group from the drop-down list to associate with the IPsec tunnel. |
| **Tunnel Source** | Enter the source of the IPsec interface:<br>• **IP Address**: Enter the source IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address that is based on your selection in the **Tunnel Mode** option. This address is on the local router.<br>• **Interface**: Enter the physical interface in the **IPsec Source Interface** field, which is the source of the IPsec tunnel. |
| **Tunnel Destination** | Enter the destination IP address of the IPsec tunnel interface. This address is on a remote device.<br>• **Address**: Enter the destination IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address based on your selection in the **Tunnel Mode** option.<br>• **Application**: Choose an application from the drop-down list.<br>  • **None**<br>  • **Sig** |

### Internet Key Exchange

| Field | Description |
|---|---|
| **IKE Version** | Enter 1 to choose IKEv1.<br>Enter 2 to choose IKEv2.<br>Default: IKEv1 |

| Field | Description |
|---|---|
| **IKE Integrity Protocol** | Choose one of the following modes for the exchange of keying information and setting up IKE security associations:<br>• **Main**: Establishes an IKE SA session before starting IPsec negotiations.<br>• **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties.<br>Default: Main mode |
| **IPsec Rekey Interval** | Specify the interval for refreshing IKE keys.<br>Range: 3600 through 1209600 seconds (1 hour through 14 days)<br>Default: 14400 seconds (4 hours) |
| **IKE Cipher Suite** | Specify the type of authentication and encryption to use during IKE key exchange.<br>Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2<br>Default: aes256-cbc-sha1 |
| **IKE Diffie-Hellman Group** | Specify the Diffie-Hellman group to use in IKE key exchanges.<br>Values: 2, 14, 15, 16, 19, 20, 21, 24<br>Default: 16 |
| **IKE ID for Local End Point** | If the remote IKE peer requires a local endpoint identifier, specify it.<br>Range: 1 through 64 characters<br>Default: Source IP address of the tunnel |
| **IKE ID for Remote End Point** | If the remote IKE peer requires a remote endpoint identifier, specify it.<br>Range: 1 through 64 characters<br>Default: Destination IP address of the tunnel<br>There is no default option if you choose IKEv2. |

### IPSEC

| Field | Description |
|---|---|
| **IPsec Rekey Interval** | Specify the interval for refreshing IKE keys.<br>Range: 3600 through 1209600 seconds (1 hour through 14 days)<br>Default: 3600 seconds (1 hour) |

| Field | Description |
|---|---|
| **IPsec Replay Window** | Specify the replay window size for the IPsec tunnel.<br>Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes<br>Default: 512 bytes |
| **IPsec Cipher Suite** | Specify the authentication and encryption to use on the IPsec tunnel.<br>Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1**<br>Default: **aes256-gcm** |
| **Perfect Forward Secrecy** | Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values:<br>• **group-2**: Use the 1024 bit Diffie-Hellman prime modulus group<br>• **group-14**: Use the 2048 bit Diffie-Hellman prime modulus group<br>• **group-15**: Use the 3072 bit Diffie-Hellman prime modulus group<br>• **group-16**: Use the 4096 bit Diffie-Hellman prime modulus group<br>• **none**: Disable PFS<br>Default: **group-16** |

### Advanced

| Field | Description |
|---|---|
| **Associated VPN** | Select a VPN from the drop-down list to associate with the IPsec tunnel. |
| **Tunnel Route Via** | Specify the tunnel route details to steer the application traffic through.<br>**Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route. |
| **DPD Interval** | Specify the interval for IKE to send Hello packets on the connection.<br>Range: 10 through 3600 seconds (1 hour)<br>Default: 10 seconds |
| **DPD Retries** | Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer.<br>Range: 2 through 60<br>Default: 3 |

| Field | Description |
|---|---|
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |
| **IP MTU** | Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **Shutdown** | Click **Off** to enable the interface. |

## OSPF Routing

Use the OSPF feature to configure transport-side routing, to provide reachability to networks at the local site.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the **Enter Key** field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the **Enter Key** field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value is shown for parameters that have a default setting. |

The following tables describe the options for configuring the OSPF Routing 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. |

### Basic Configuration

| Field | Description |
|---|---|
| **Router ID** | Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address associated with the router for OSPF adjacencies.<br>Default: <Device specific IPv4 system_ip > |
| **Distance for External Routes** | Specify the OSPF route administration distance for routes learned from other domains.<br>Range: 1 through 255<br>Default: 110 |
| **Distance for Inter-Area Routes** | Specify the OSPF route administration distance for routes coming from one area into another.<br>Range: 1 through 255<br>Default: 110 |
| **Distance for Intra-Area Routes** | Specify the OSPF route administration distance for routes within an area.<br>Range: 0 through 255<br>Default: 110 |

### Redistribute

| Field | Description |
|---|---|
| **Add Redistribute** | |
| **Protocol** | Choose the protocol from which to redistribute routes into OSPF.<br>• **Static**<br>• **Connected**<br>• **BGP**<br>• **NAT** |
| **Select Route Policy** | Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF. |

### Maximum Metric (Router LSA)

| Field | Description |
|---|---|
| **Add Router LSA** | |

| Field | Description |
|---|---|
| **Type** | Configure OSPF to advertise a maximum metric so that other routers do not prefer this router as an intermediate hop in their Shortest Path First (SPF) calculation.<br>Choose a type:<br>• **administrative**: Force the maximum metric to take effect immediately, through operator intervention.<br>• **on-startup**: Advertise the maximum metric for the specified time.<br>**Note** You can configure a maximum of one router LSA. |

### Area

| Field | Description |
|---|---|
| **Add Area** | |
| **Area Number*** | Enter the number of the OSPF area.<br>Allowed value: Any 32-bit integer |
| **Set the area type** | Choose the type of OSPF area:<br>• **Stub**<br>• **NSSA**<br>**Note** The **Set the area type** option won't appear if you have entered 0 as a value for **Area Number***. |
| **Add Interface** | Configure the properties of an interface in an OSPF area. |
| **Name*** | Enter the name of the interface. For example, GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1. |
| **Hello Interval (seconds)** | Specify how often the router sends OSPF hello packets.<br>Range: 1 through 65535 seconds<br>Default: 10 seconds |
| **Dead Interval (seconds)** | Specify how often the router must receive an OSPF hello packet from its neighbor. If no packet is received, the router assumes that the neighbor is down.<br>Range: 1 through 65535 seconds<br>Default: 40 seconds (four times the default hello interval) |

| Field | Description |
|---|---|
| **LSA Retransmission Interval (seconds)** | Specify how often the OSPF protocol retransmits LSAs to its neighbors.<br>Range: 1 through 65535 seconds<br>Default: 5 seconds |
| **Interface Cost** | Specify the cost of the OSPF interface.<br>Range: 1 through 65535 |
| **Designated Router Priority** | Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the router with the highest router ID becomes the DR or the backup DR.<br>Range: 0 through 255<br>Default: 1 |
| **OSPF Network Type** | Choose the OSPF network type to which the interface is to connect:<br>• **Broadcast network**<br>• **Point-to-point network**<br>• **Non-broadcast network**<br>• **Point-to-multipoint network** |
| **Passive Interface** | Specify whether to set the OSPF interface to be passive. A passive interface advertises its address, but does not actively run the OSPF protocol.<br>Default: Disabled |
| **Authentication Type** | Specify the key ID and authentication key if you use message digest (MD5):<br>• **Message Digest Key ID**: Enter the key ID for message digest (MD5 authentication). The input value must be an integer.<br>Range: 1 through 255<br>• **Message Digest Key**: Enter the MD5 authentication key.<br>Range: 1 through 127 characters |
| **Add Range** | Configure the area range of an interface in an OSPF area. |
| **IP Address*** | Enter the IP address. |
| **Subnet Mask*** | Enter the subnet mask. |
| **Cost** | Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination.<br>Range: 0 through 16777214 |
| **No-advertise*** | Enable this option to not advertise the Type 3 summary LSAs. |

### Advanced

| Field | Description |
|---|---|
| **Reference Bandwidth (Mbps)** | Specify the reference bandwidth for the OSPF auto-cost calculation for the interface.<br>Range: 1 through 4294967 Mbps<br>Default: 100 Mbps |
| **RFC 1583 Compatible** | By default, the OSPF calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328. |
| **Originate** | Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear:<br>• **Always**: Enable this option to always advertise the default route in an OSPF routing domain.<br>• **Default Metric**: Set the metric used to generate the default route.<br>Range: 0 through 16777214<br>Default: 10<br>• **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route. |
| **SPF Calculation Delay (milliseconds)** | Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 200 ms |
| **Initial Hold Time (milliseconds)** | Specify the amount of time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 1000 ms |
| **Maximum Hold Time (milliseconds)** | Specify the longest time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 10000 ms (10 seconds) |
| **Select Route Policy** | Enter the name of a localized control policy to apply to routes coming from OSPF neighbors. |

## 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) map 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 table describes 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). |

## GPS

Use the GPS feature to detect the device location and to monitor GPS coordinates of Cisco IOS XE Catalyst SD-WAN devices.

The following tables describe the options for configuring the GPS feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name*** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| **Description** | Enter a description of the feature. The description can be up to 2,048 characters and can contain only alphanumeric characters. |
| **GPS** | Click **On** to enable the GPS feature on the router. |
| **GPS Mode** | Select the GPS mode:<br>• **MS-based**: Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, cell tower data is used to enhance the quality and precision in determining location, which is useful when satellite signals are poor.<br>• **Standalone**: Use satellite information when determining position. |
| **NMEA** | Click **On** to enable the use of NMEA streams to help with determining position. NMEA streams data from the router's cellular module to any marine device, such as a Windows-based PC, that is running a commercially available GPS-based application. |
| **Source Address*** | Enter the IP address of the router's interface that connects to the external device reading the NMEA. |
| **Destination Address*** | Enter the IP address of the external device's interface that's connected to router. |
| **Destination Port*** | Enter the number of the port to use to send NMEA data to the external device's interface. |

## Tracker Group

Use the Tracker Group feature profile to track the status of transport interfaces.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

The following table describes the options for configuring the Tracker Group feature.

| Field | Description |
|---|---|
| **Tracker Elements*** | This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Add the existing interface tracker names, separated with 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 Boolean** | This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**.<br>**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.<br>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. |

## IPv6 Tracker

This feature helps you configure the IPv6 tracker for the VPN interface.

The following table describes the options for configuring the IPv6 Tracker feature.

***Table 59: IPv6 Tracker***

| 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. |
| **Tracker Name*** | Name of the tracker. The name can be up to 128 alphanumeric characters. |
| **Endpoint Tracker Type*** | Choose a tracker type to configure endpoint trackers:<br>• **ipv6-interface**<br>**Note** This tracker type is available only in Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier.<br>• **http**<br>• **icmp**<br>This tracker type is available from Cisco Catalyst SD-WAN Manager Release 20.13.1. |

| Field | Description |
|---|---|
| **Endpoint** | Choose an endpoint type:<br>• **Endpoint DNS Name**: When you choose this option, the following field appears:<br>**Endpoint DNS Name**: DNS name of the endpoint. This is the destination on the internet to which probes are sent to determine the status of the endpoint. The DNS name can contain a minimum of one character and a maximum of 253 characters.<br>• **Endpoint IP**: When you choose this option, the following field appears:<br>**Endpoint IP**: IPv6 address of the endpoint. This is the destination on the internet to which the probes are sent to determine the status of an endpoint. The IPv6 address can be a valid IPv6 address in dotted-decimal notation.<br>• **Endpoint API URL**: When you choose this option, the following field appears:<br>**API url of endpoint**: API URL of the endpoint. The API URL can be a valid URL as described by RFC 3986. |
| **Interval** | Time interval between probes to determine the status of the configured endpoint.<br>From Cisco Catalyst SD-WAN Manager Release 20.13.1, this option is called **Probe Interval**, allowing you to configure the time interval between probes.<br>Range: 20 to 600 seconds<br>Default: 60 seconds (1 minute)<br>From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you select **icmp** as the endpoint tracker type, the default probe interval is 2 seconds. |
| **Multiplier** | Number of times probes are sent before declaring that the endpoint is down.<br>Range: 1 to 10<br>Default: 3 |
| **Threshold** | Wait time for the probe to return a response before declaring that the configured endpoint is down.<br>Range: 100 to 1000 milliseconds<br>Default: 300 milliseconds |

## IPv6 Tracker Group

This feature helps you configure the IPv6 tracker froup for the VPN interface.

The following table describes the options for configuring the IPv6 tracker group feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name*** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| **Description** | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |

*Table 60: IPv6 Tracker Group*

| Field | Description |
|---|---|
| **Tracker Name** | Enter a tracker name. |
| **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 Boolean** | This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**.<br>**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.<br>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. |

## GRE

Use the GRE feature for all Cisco IOS XE Catalyst SD-WAN devices.

The following tables describe the options for configuring the GRE feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Interface Name (1..255)*** | Enter the name of the GRE interface.<br>Range: 1 through 255. |
| **Interface Description** | Enter a description of the GRE interface. |

### Advanced

| Field | Description |
|---|---|
| **Shutdown** | Click **Off** to enable the interface. |

| Field | Description |
|---|---|
| **IP MTU** | Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv6 packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **TCP MSS** | Based on your choice in the **Tunnel Mode** option, specify the maximum segment size (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.<br>Range: 552 through 1460 bytes<br>Default: None |

## OSPFv3 IPv4 Routing

Use this feature to configure the Open Shortest Path First version 3 (OSPFv3) IPv4 link-state routing protocol for IPv4 unicast address families.

The following tables describe the options for configuring the OSPFv3 IPv4 Routing feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name*** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| **Description** | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |

### Basic Settings

| Field | Description |
|---|---|
| **Router ID** | Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address that is associated with the router for OSPF adjacencies. Default: No Router ID is configured. |
| **Add Redistribute** | |
| **Protocol** | Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions.<br>• **Connected**<br>• **Static**<br>• **Nat-route**<br>• **BGP** |

| Field | Description |
|---|---|
| **Select Route Policy** | Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF. |

**Area**

| Field | Description |
|---|---|
| **Area Number*** | Enter the number of the OSPFv3 area.<br>Allowed value: Any 32-bit integer |
| **Area Type** | Choose the type of OSPFv3 area:<br>• **Stub** - no external routes<br>• **NSSA**: not-so-stubby area, allows external routes<br>• **Normal**<br>**Note** You can't enter a value for **Area type** if you have entered 0 as a value for **Area Number**. |
| **Interface** | |
| **Add Interface** | Configure the properties of an interface in an OSPFv3 area. |
| **Name*** | Enter the name of the interface. Examples of interface names: GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1. |
| **Cost** | Specify a number for the Type 3 summary link-state advertisement (LSA). OSPFv3 uses this metric during its SPF calculation to determine the shortest path to a destination.<br>Range: 0 through 16777215 |
| **Authentication Type** | Specify the SPI and authentication key if you use IPSec SHA1.<br>• **no-auth**: Select no authentication.<br>• **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication. |
| **SPI** | Specifies the Security Policy Index (SPI) value.<br>Range: 256 through 4294967295 |
| **Authentication Key** | Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long. |

| Field | Description |
|---|---|
| **Passive Interface** | Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol.<br>Default: Disabled |
| **IPv4 Range** | |
| **Add IPv4 Range** | Configure the area range of an interface in an OSPFv3 area. |
| **Network Address*** | Enter the IPv4 address. |
| **Subnet Mask*** | Enter the subnet mask. |
| **No Advertise*** | Enable this option to not advertise the Type 3 summary LSAs. |
| **Cost** | Specify the cost of the OSPFv3 interface.<br>Range: 1 through 65535 |

### Advanced

| Field | Description |
|---|---|
| **Route Policy** | Enter the name of a localized control policy to apply to routes coming from OSPFv3 neighbors. |
| **Reference Bandwidth (Mbps)** | Specify the reference bandwidth for the OSPFv3 autocost calculation for the interface.<br>Range: 1 through 4294967 Mbps<br>Default: 100 Mbps |
| **RFC 1583 Compatible** | By default, the OSPFv3 calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328. |
| **Originate** | Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear:<br>• **Always**: Enable this option to always advertise the default route in an OSPF routing domain.<br>• **Default Metric**: Set the metric used to generate the default route.<br>Range: 0 through 16777214<br>Default: 10<br>• **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route. |
| **Distance** | Define the OSPFv3 route administration distance based on route type.<br>Default: 100 |

| Field | Description |
|---|---|
| **Distance for External Routes** | Set the OSPFv3 distance for routes learned from other domains.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Inter-Area Routes** | Set the distance for routes coming from one area into another.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Intra-Area Routes** | Set the distance for routes within an area.<br>Range: 0 through 255<br>Default: 110 |
| **SPF Calculation Timers** | Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm. |
| **SPF Calculation Delay (milliseconds)** | Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 200 ms |
| **Initial Hold Time (milliseconds)** | Specify the amount of time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 1000 ms |
| **Maximum Hold Time (milliseconds)** | Specify the longest time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 10000 ms (10 seconds) |
| **Maximum Metric (Router LSA)** | Configure OSPFv3 to advertise a maximum metric so that other routers do not prefer this Cisco vEdge Device as an intermediate hop in their Shortest Path First (SPF) calculation.<br>• **Immediately**: Force the maximum metric to take effect immediately, through operator intervention.<br>• **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up.<br>Range: 5 through 86400 seconds<br>Maximum metric is disabled by default. |

## OSPFv3 IPv6 Routing

Use this feature to configure the Open Shortest Path First version 3 (OSPFv3) IPv6 link-state routing protocol for IPv6 unicast address families.

The following tables describe the options for configuring the OSPFv3 IPv6 Routing feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name*** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| **Description** | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |

### Basic Settings

| Field | Description |
|---|---|
| **Router ID** | Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address that is associated with the router for OSPF adjacencies.<br>Default: No Router ID is configured. |
| **Add Redistribute** | |
| **Protocol** | Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions.<br>• **Connected**<br>• **Static**<br>• **BGP** |
| **Select Route Policy** | Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF. |

### Area

| Field | Description |
|---|---|
| **Area Number*** | Enter the number of the OSPFv3 area.<br>Allowed value: Any 32-bit integer |
| **Area Type** | Choose the type of OSPFv3 area:<br>• **Stub**: No external routes<br>• **NSSA**: Not-so-stubby area, allows external routes<br>• **Normal**<br>**Note** You can't enter a value for **Area type** if you have entered 0 as a value for **Area Number**. |
| **Interface** | |

| Field | Description |
|---|---|
| **Add Interface** | Configure the properties of an interface in an OSPFv3 area. |
| **Name*** | Enter the name of the interface. Examples of interface names: GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1. |
| **Cost** | Specify a number for the Type 3 summary link-state advertisement (LSA). OSPFv3 uses this metric during its SPF calculation to determine the shortest path to a destination.<br>Range: 0 through 16777215 |
| **Authentication Type** | Specify the SPI and authentication key if you use IPSec SHA1.<br>• **no-auth**: Select no authentication.<br>• **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication. |
| **SPI** | Specifies the Security Policy Index (SPI) value.<br>Range: 256 through 4294967295 |
| **Authentication Key** | Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long. |
| **Passive Interface** | Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol.<br>Default: Disabled |
| **IPv6 Range** | |
| **Add IPv6 Range** | Configure the area range of an interface in an OSPFv3 area. |
| **Network Address*** | Enter the IPv6 address. |
| **Subnet Mask*** | Enter the subnet mask. |
| **No Advertise*** | Enable this option to not advertise the Type 3 summary LSAs. |
| **Cost** | Specify the cost of the OSPFv3 interface.<br>Range: 1 through 65535 |

### Advanced

| Field | Description |
|---|---|
| **Route Policy** | Enter the name of a localized control policy to apply to routes coming from OSPFv3 neighbors. |

| Field | Description |
|---|---|
| **Reference Bandwidth (Mbps)** | Specify the reference bandwidth for the OSPFv3 autocost calculation for the interface.<br>Range: 1 through 4294967 Mbps<br>Default: 100 Mbps |
| **RFC 1583 Compatible** | By default, the OSPFv3 calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328. |
| **Originate** | Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear:<br>• **Always**: Enable this option to always advertise the default route in an OSPF routing domain.<br>• **Default Metric**: Set the metric used to generate the default route.<br>Range: 0 through 16777214<br>Default: 10<br>• **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route. |
| **Distance** | Define the OSPFv3 route administration distance based on route type.<br>Default: 100 |
| **Distance for External Routes** | Set the OSPFv3 distance for routes learned from other domains.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Inter-Area Routes** | Set the distance for routes coming from one area into another.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Intra-Area Routes** | Set the distance for routes within an area.<br>Range: 0 through 255<br>Default: 110 |
| **SPF Calculation Timers** | Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm. |
| **SPF Calculation Delay (milliseconds)** | Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 200 ms |

| Field | Description |
|---|---|
| **Initial Hold Time (milliseconds)** | Specify the amount of time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 1000 ms |
| **Maximum Hold Time (milliseconds)** | Specify the longest time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 10000 ms (10 seconds) |
| **Maximum Metric (Router LSA)** | Configure OSPFv3 to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation.<br>• **Immediately**: Force the maximum metric to take effect immediately, through operator intervention.<br>• **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up.<br>Range: 5 through 86400 seconds<br>Maximum metric is disabled by default. |

## Route Policy

Use this feature to configure the policy-based routing if you want certain packets to be routed through a specific path other than the obvious shortest path.

The following table describes the options for configuring the route policy feature.

| Field | Description |
|---|---|
| **Routing Sequence Name** | Specifies the name of the routing sequence. |
| **Protocol** | Specifies the internet protocol. The options are IPv4, IPv6, or Both. |
| **Condition** | Specifies the routing condition. The options are:<br>• **Address**<br>• **AS Path List**<br>• **Community List**<br>• **Extended Community List**<br>• **BGP Local Preference**<br>• **Metric**<br>• **Next Hop**<br>• **OMP Tag**<br>• **OSPF Tag** |

| Field | Description |
|---|---|
| **Action Type** | Specifies the action type. The options are **Accept** or **Reject**. |
| **Accept Condition** | Specifies the accept condition type. The options are:<br>• **AS Path**<br>• **Community**<br>• **Local Preference**<br>• **Metric**<br>• **Metric Type**<br>• **Next Hop**<br>• **OMP Tag**<br>• **Origin**<br>• **OSPF Tag**<br>• **Weight** |

## T1/E1 Controller

Use this feature to configure the T1 or E1 network interface module (NIM) parameters for Cisco IOS XE Catalyst SD-WAN devices.

### Configure a T1 Controller

To configure a T1 controller, choose **T1** and configure the following parameters. Parameters marked with an asterisk are mandatory.

| Parameter Name | Description |
|---|---|
| Slot* | Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0. |
| Description | Enter a description for the controller. |
| Framing | It is an optional field. Enter the T1 frame type:<br>• **esf**: Send T1 frames as extended superframes. This is the default.<br>• **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing. |
| Line Code | It is an optional field. Select the line encoding to use to send T1 frames:<br>• **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes.<br>• **b8zs**: Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes |

| Parameter Name | Description |
|---|---|
| Cable Length | Select the cable length to configure the attenuation<br>• **short**: Set the transmission attenuation for cables that are 660 feet or shorter.<br>• **long**: Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet.<br>There is no default length. |
| Clock Source | Select the clock source:<br>• **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source.<br>• **internal**: Use the controller framer as the primary clock.<br>• **loop-timed**:<br>• **network**: |

### Configure an E1 Controller

To configure an E1 controller, choose **E1** and configure the following parameters. Parameters marked with an asterisk are mandatory.

| Parameter Name | Description |
|---|---|
| Slot* | Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0. |
| Description | Enter a description for the controller. |
| Framing | Enter the E1 frame type:<br>• **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default.<br>• **no-crc4**: Do not use CRC4. |
| Line Code | Choose the line encoding to use to send E1 frames:<br>• **ami**: Use alternate mark inversion (AMI) as the linecode.<br>• **hdb3**: Use high-density bipolar 3 as the linecode. This is the default. |
| Clock Source | Choose the clock source:<br>• **internal**: Use the controller framer as the primary clock.<br>• **line**: Use phase-locked loop (PLL) on the interface. This is the default. |

### Channel Group

| Parameter Name | Description |
|---|---|
| Add Channel Group | To configure the serial WAN on the E1 interface, enter a channel group number and a value for the timeslot.<br>• **Channel Group**: Enter a value for the channel group.<br>Range: 0 through 30<br>• **Time Slot**: Type a value for the timeslot.<br>Range: 0 through 31 |

## T1/E1/Serial

Configure the T1/E1/Serial feature for the VPN interface for Cisco IOS XE Catalyst SD-WAN devices.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the **Enter Key** field. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the **Enter Key** field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value appears for parameters that have a default setting. |

### Basic Configuration

| Parameter Name | Description |
|---|---|
| Shutdown | Click **No** to enable the interface. |
| Interface name* | Enter a name for the interface. The name should be in the following format:<br>**serial** *slot* / *subslot* / *port* **:** *channel-group*<br>You must also configure a number for the channel group in the T1/E1 Controller feature configuration template. |
| Description | Enter a description for the interface. |
| **More Settings** | |

| Parameter Name | Description |
|---|---|
| IPv4 Address* | Enter an IPv4 address. |
| IPv6 Address* | Enter an IPv6 address. |
| Bandwidth | For transmitted traffic, set the bandwidth above which to generate notifications.<br>Range: 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>Range: 1 through ($2^{32}$ / 2) – 1 kbps |
| Clock Rate | Specify a value for the clock rate.<br>Range: 1200 through 800000 |
| Encapsulation | Choose an encapsulation method for traffic that crosses a WAN link.<br>• **hdlc**: High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces.<br>• **ppp**: Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links. |

### Tunnel

| Parameter Name | Description |
|---|---|
| Tunnel Interface* | From the drop-down list, select **Global**. Click **On** to create a tunnel interface. |
| Per-tunnel QoS | From the drop-down list, select **Global**. Click **On** to create per-tunnel QoS.<br>You can apply a Quality of Service (QoS) policy on individual tunnels, and is only supported for hub-to-spoke network topologies. |
| Color | From the drop-down list, select **Global**. Select a color for the TLOC. The color typically used for cellular interface tunnels is **lte**. |
| Groups | From the drop-down list, select **Global**. Enter the list of groups in the field. |
| Border | From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC. |
| Maximum Control Connections | Set the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>Range: 0 through 8<br>Default: 2 |

| Parameter Name | Description |
|---|---|
| Validator As Stun Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Control Group List | Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allows to establish control connections with.<br>Range: 0 through 100 |
| Manager Connection Preference | Set the preference for using the tunnel to exchange control traffic with Cisco SD-WAN Manager.<br>Range: 0 through 9<br>Default: 5<br>If the edge device has two or more cellular interfaces, you can minimize the amount of traffic between Cisco SD-WAN Manager and the cellular interfaces by setting one of the interfaces to be the preferred one to use when sending updates to the Cisco SD-WAN Manager and receiving configurations from the Cisco SD-WAN Manager.<br>To have a tunnel interface never connect to Cisco SD-WAN Manager, set the number to 0. At least one tunnel interface on the edge device must have a nonzero Cisco SD-WAN Manager connection preference. |
| Port Hop | From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface.<br>Default: **On**, which disallows port hopping on tunnel interface. |
| Low-Bandwidth Link | Click **On** to set the tunnel interface as a low-bandwidth link.<br>Default: **Off** |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br>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.<br>Range: 552 through 1460 bytes<br>Default: None |

| Parameter Name | Description |
|---|---|
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Network Broadcast | From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template.<br>Default: **Off** |
| Allow Service | Click **On** or **Off** for each service to allow or disallow the service on the cellular interface. |
| **Encapsulation** | |
| Add Encapsulation | From the drop-down list, select **Global** and choose from one of the two encapsulation methods:<br>• **gre**: Enter a value to set GRE preference for TLOC.<br>Range: 0 to 4294967295<br>• **ipsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0 |
| Preference | From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0 |
| Weight | From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1 |
| **Advanced Options** | |

| Parameter Name | Description |
|---|---|
| Carrier | From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel.<br>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default.<br>Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format:<br>**ge** *slot*/*port*. |
| Last-Resort Circuit | From the drop-down list, select **Global** and click **On** to use the tunnel interface as the circuit of last resort. By default, it is disabled.<br>**Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>Range: 1 through 60 seconds<br>Default: 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>Range: 100 through 10000 milliseconds<br>Default: 1000 milliseconds (1 second) |

| Parameter Name | Description |
|---|---|
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>Range: 12 through 60 seconds<br>Default: 12 seconds<br>The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable. |

### ACL/QoS

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| **ACL** | |
| Select ACL IPv4 Ingress | Enter the name of an IPv4 access list to packets being received on the interface. |
| Select ACL IPv4 Egress | Enter the name of an IPv4 access list to packets being transmitted on the interface. |
| Select ACL IPv6 Ingress | Enter the name of an IPv6 access list to packets being received on the interface. |
| Select ACL IPv6 Egress | Enter the name of an IPv6 access list to packets being transmitted on the interface. |

### Advanced

| Parameter Name | Description |
|---|---|
| TCP MSS | Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 500 through 1460 bytes<br>Default: 536 |
| MTU | Enter the path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.<br>Default: 1500 |
| IP MTU | Enter the maximum MTU size of packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds this service-side interface to the WAN transport, by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface. |

## DSL PPPoA

Configure PPP-over-ATM interfaces on routers with DSL NIM modules to provide support for service provider digital subscriber line (DSL) functionality for Cisco IOS XE Catalyst SD-WAN devices.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value appears for parameters that have a default setting. |

### Basic Configuration

| Parameter Name | Description |
|---|---|
| Controller Slot* | Enter the slot number of the DSL controller, in the following format:<br>*slot*/*subslot*/*port* (for example, 0/2/0) |
| Controller Mode | Select the operating mode of the DSL controller from the drop-down list:<br>• **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br>• **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br>• **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br>• **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br>• **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps. |
| SRA | Disabled by default. Enable SRA to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |
| Dialer Pool Member* | Enter the number of the dialer pool to which the interface belongs.<br>Range: 1 through 255 |

### ATM

***Table 61:***

| Parameter Name | Description |
|---|---|
| ATM Sub Interface Name* | The ATM Sub interface name is auto populated based on the controller slot. Enter a value for the ATM sub interface, in the format *subslot*/*port* (for example ATM0/2/0.100). In this example, ".100" is the sub interface value. |
| Sub Interface Description | Enter a description for the interface. |
| VPI/VCI* | Create an ATM permanent virtual circuit (PVC), in the following format:<br>*vpi*/*vci*<br>Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI). |

| Parameter Name | Description |
|---|---|
| Encapsulation | Select the encapsulation type to use on the ATM PVC from the drop-down list:<br>• AAL5 NLPID: Use NLPID multiplexing.<br>• AAL5 SNAP: Multiplex two or more protocols on the same PVC.<br>• AAL5 MUX: Dedicate the PVC to a single protocol. |
| **PVC Mode** | |
| VBR-NRT | Configure variable bit rate non-real-time parameters:<br>• Peak Cell Rate: Enter a value from 48 through 1015 Kbps.<br>• Sustainable Cell Rate: Enter the sustainable cell rate, in Kbps.<br>• Maximum Burst Size: This size can be 1 through 65535. |
| VBR-RT | Configure variable bit rate real-time parameters:<br>• Peak Cell Rate: Enter a value from 48 through 25000 Kbps.<br>• Average Cell Rate: Enter the average cell rate, in Kpbs.<br>• Maximum Burst Size: This size can be 1 through 65535. |
| None | Don't configure variable bit rate parameters |

**PPP**

| Parameter Name | Description |
|---|---|
| PPP Authentication Protocol | Select the authentication protocol used by the MLP:<br>• **PAP**: Enter the username and password that are provided by your ISP. *username* can be up to 255 characters.<br>• **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol. |
| Authentication Type | Select the type authentication from one of the following options.:<br>• **Unidirectional**: Only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server.<br>• **Bidirectional**: Each side independently sends an Authenticate-Request (AUTH-REQ) and receives either an Authenticate-Acknowledge (AUTH-ACK) or Authenticate-Not Acknowledged (AUTH-NAK). |
| CHAP Hostname* | Enter the CHAP hostname. |

| Parameter Name | Description |
|---|---|
| CHAP Password* | Enter the CHAP password. |
| PAP Hostname* | Enter the PAP hostname. |
| PAP Password* | Enter the PAP password. |

**Tunnel**

| Parameter Name | Description |
|---|---|
| **Tunnel Interface** | |
| Per Tunnel QoS | Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies:<br>• **Spoke**<br>• **Hub**<br>If you select hub topology, the following option appears:<br>• **Bandwidth Percentage**: Enter a value for the bandwidth percentage.<br>Default: 50 |
| Color | Choose a color for the TLOC. |
| Groups | Enter the list of groups in the field. |
| Exclude Controller Group List | Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to.<br>Range: 0 through 100 |
| Maximum Control Connections | Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>Range: 0 through 8<br>Default: 2 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager.<br>Range: 0 through 8<br>Default: 5 |

| Parameter Name | Description |
|---|---|
| Tunnel TCP MSS | TCP MSS affects any packet containing 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU.<br>Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 to 1460 bytes |
| Border | From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC. |
| Validator As Stun Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Port Hop | From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface.<br>Default: **On**, which disallows port hopping on a tunnel interface |
| Low-Bandwidth Link | Click **On** to set the tunnel interface as a low-bandwidth link.<br>Default: **Off** |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets.<br>the router fragments packets larger than the MTU of the interface before sending the packets.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Network Broadcast | From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template.<br>Default: **Off** |

| Parameter Name | Description |
|---|---|
| Carrier | From the drop-down list, select **Global** and select the carrier name or private network identifier to associate with the tunnel.<br>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default.<br>Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format:<br>**ge** *slot*/*port* |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>Range: 1 through 60 seconds<br>Default: 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>Range: 100 through 10000 milliseconds<br>Default: 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>Range: 12 through 60 seconds<br>Default: 12 seconds<br>The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable. |

| Parameter Name | Description |
|---|---|
| Last Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br>**Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| Allow Services | Click **On** or **Off** for each service to anable or disable the service on the cellular interface. |
| **Encapsulation** | |

| Parameter Name | Description |
|---|---|
| Encapsulation | Enable at least one of the following encapsulation methods:<br>• **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1<br>• **GRE**: Enter a value to set GRE preference for TLOC.<br>Range: 0 through 4294967295<br>• **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1 |

### NAT

| Parameter Name | Description |
|---|---|
| UDP Timeout (Minutes) | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 1 minute |

| Parameter Name | Description |
|---|---|
| TCP Timeout (Minutes) | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 60 minutes (1 hour) |

### QoS

| Parameter Name | Description |
|---|---|
| Adaptive QoS | Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values.<br>• **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes.<br>• **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps.<br>• **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps. |
| Shaping Rate (kbps) | Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).<br>Range: 8 through 100000000 |

### ACL

| Parameter Name | Description |
|---|---|
| IPv4 Ingress Access List | Enter the name of an IPv4 access list to packets being received on the interface. |
| IPv4 Egress Access List | Enter the name of an IPv4 access list to packets being transmitted on the interface. |
| IPv6 Ingress Access List | Enter the name of an IPv6 access list to packets being received on the interface. |
| IPv6 Egress Access List | Enter the name of an IPv6 access list to packets being transmitted on the interface. |

### Advanced

| Parameter Name | Description |
|---|---|
| Shutdown | Click **No** to enable the interface. |
| Tracker / Tracker Group | Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet. |
| Service Provider | Specify the details of the service provider. |

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream (Kbps) | Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value. |
| Bandwidth Downstream (Kbps) | Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value. |
| IP MTU | Enter the maximum MTU size of packets on the interface.<br>Range: 576 through 1804<br>Default: 1500 |
| TCP MSS | Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: 1500 |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface. |
| IP Directed Broadcast | From the drop-down list, select **Global** to enable IP Directed Broadcast.<br>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. |

## DSL IPoE

Configure IPoE on routers with DSL interfaces, to provide support for service provider digital subscriber line (DSL) functionality for Cisco IOS XE Catalyst SD-WAN devices.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |

| Parameter Scope | Scope Description |
|---|---|
| **Default** (indicated by a check mark) | The default value appears for parameters that have a default setting. |

### Basic Configuration

| Parameter Name | Description |
|---|---|
| Controller Slot* | Enter the slot number of the controller, in the following format:<br>*slot*/*subslot*/*port* (for example, 0/2/0) |
| Controller Mode | Select the operating mode of the DSL controller from the drop-down list:<br>• **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br>• **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br>• **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br>• **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br>• **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps. |
| SRA | Enabled by default. Click **No** to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |

### Ethernet

| Parameter Name | Description |
|---|---|
| Ethernet Interface Name * | Enter the name of an ethernet interface.<br>For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**). |
| Description | Enter a description for the interface. |
| VLAN ID | Enter the VLAN identifier of the Ethernet interface. |

### Tunnel

| Parameter Name | Description |
|---|---|
| **Tunnel Interface** | |

| Parameter Name | Description |
|---|---|
| Per Tunnel QoS | Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies:<br>• **Spoke**<br>• **Hub** |
| Color | Select a color for the TLOC. |
| Groups | Enter the list of groups in the field. |
| Exclude Controller Group List | Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to.<br>Range: 0 through 100 |
| Maximum Control Connections | Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>Range: 0 through 8<br>Default: 2 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager.<br>Range: 0 through 8<br>Default: 5 |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU.<br>Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |
| Border | From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC. |
| Validator As Stun Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |

| Parameter Name | Description |
|---|---|
| Port Hop | From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface.<br>Default: **On**, which disallows port hopping on tunnel interface. |
| Low-Bandwidth Link | Click **On** to set the tunnel interface as a low-bandwidth link.<br>Default: **Off** |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Network Broadcast | From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template.<br>Default: **Off** |
| Carrier | From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel.<br>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default.<br>Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format:<br>**ge** *slot*/*port* |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>Range: 1 through 60 seconds<br>Default: 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>Range: 100 through 10000 milliseconds<br>Default: 1000 milliseconds (1 second) |

| Parameter Name | Description |
|---|---|
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>Range: 12 through 60 seconds. Default: 12 seconds.<br><br>The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable. |
| Last Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br><br>**Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br><br>When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br><br>If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| Allow Services | Click **On** or **Off** for each service to enable or disable the service on the cellular interface. |
| **Encapsulation** | |

| Parameter Name | Description |
|---|---|
| Encapsulation | Enable atleast one of the following encapsulation methods:<br>• **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1<br>• **GRE**: Enter a value to set GRE preference for TLOC.<br>Range: 0 through 4294967295<br>• **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1 |

### NAT

| Parameter Name | Description |
|---|---|
| UDP Timeout (Minutes) | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 65536 minutes<br>Default: 1 minute |

| Parameter Name | Description |
|---|---|
| TCP Timeout (Minutes) | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 65536 minutes<br>Default: 60 minutes (1 hour) |

### QoS

| Parameter Name | Description |
|---|---|
| Adaptive QoS | Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values.<br>• **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes.<br>• **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps.<br>• **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps. |
| Shaping Rate (kbps) | Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).<br>Range: 8 through 100000000 |

### ACL

| Parameter Name | Description |
|---|---|
| IPv4 Ingress Access List | Enter the name of an IPv4 access list to packets being received on the interface. |
| IPv4 Egress Access List | Enter the name of an IPv4 access list to packets being transmitted on the interface. |
| IPv6 Ingress Access List | Enter the name of an IPv6 access list to packets being received on the interface. |
| IPv6 Egress Access List | Enter the name of an IPv6 access list to packets being transmitted on the interface. |

### Advanced

| Parameter Name | Description |
|---|---|
| Shutdown | Click **No** to enable the interface. |
| Tracker / Tracker Group | Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet. |
| Service Provider | Specify the details of the service provider. |

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream (Kbps) | Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value. |
| Bandwidth Downstream (Kbps) | Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value. |
| IP MTU | Enter the maximum MTU size of packets on the interface.<br>Range: 576 through 1804<br>Default: 1500 |
| TCP MSS | Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: 1500 |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface. |
| IP Directed Broadcast | From the drop-down list, select **Global** to enable IP Directed Broadcast.<br>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. |

## DSL PPPoE

Configure the PPP-over-Ethernet interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality for Cisco IOS XE Catalyst SD-WAN devices.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |

| Parameter Scope | Scope Description |
|---|---|
| **Default** (indicated by a check mark) | The default value appears for parameters that have a default setting. |

### Basic Configuration

| Parameter Name | Description |
|---|---|
| Controller Slot* | Enter the slot number of the controller, in the following format:<br>*slot*/*subslot*/*port* (for example, 0/2/0) |
| Controller Mode | Select the operating mode of the DSL controller from the drop-down list:<br>• **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br>• **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br>• **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br>• **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br>• **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps. |
| SRA | Disabled by default. Enable SRA to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |
| Dialer Pool Member* | Enter the number of the dialer pool to which the interface belongs.<br>Range: 1 through 255 |

### Ethernet

| Parameter Name | Description |
|---|---|
| Ethernet Interface Name * | Enter the name of an ethernet interface.<br>For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**). |
| Description | Enter a description for the interface. |
| VLAN ID | Enter the VLAN identifier of the Ethernet interface. |

### PPP

| Parameter Name | Description |
|---|---|
| PPP Authentication Protocol | Select the authentication protocol used by the MLP:<br>• **PAP**: Enter the username and password that are provided by your ISP. *username* can be up to 255 characters.<br>• **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol. |
| Authentication Type | Select the type authentication from one of the following options:<br>• **Unidirectional**: Only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server.<br>• **Bidirectional**: Each side independently sends an Authenticate-Request (AUTH-REQ) and receives either an Authenticate-Acknowledge (AUTH-ACK) or Authenticate-Not Acknowledged (AUTH-NAK). |
| CHAP Hostname* | Enter the CHAP hostname. |
| CHAP Password* | Enter the CHAP password. |
| PAP Hostname* | Enter the PAP hostname. |
| PAP Password* | Enter the PAP password. |

### Tunnel

| Parameter Name | Description |
|---|---|
| **Tunnel Interface** | |
| Per Tunnel QoS | Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies:<br>• **Spoke**<br>• **Hub** |
| Color | Select a color for the TLOC. |
| Groups | Enter the list of groups in the field. |
| Exclude Controller Group List | Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to.<br>Range: 0 through 100 |

| Parameter Name | Description |
|---|---|
| Maximum Control Connections | Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>Range: 0 through 8<br>Default: 2 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager.<br>Range: 0 through 8<br>Default: 5 |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU.<br>Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |
| Border | From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC. |
| Validator As Stun Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Port Hop | From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface.<br>Default: **On**, which disallows port hopping on tunnel interface. |
| Low-Bandwidth Link | Click **On** to set the tunnel interface as a low-bandwidth link.<br>Default: **Off** |

| Parameter Name | Description |
|---|---|
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Network Broadcast | From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template.<br>Default: **Off** |
| Carrier | From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel.<br>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default.<br>Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format:<br>**ge***slot*/*port* |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>Range: 1 through 60 seconds<br>Default: 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>Range: 100 through 10000 milliseconds<br>Default: 1000 milliseconds (1 second) |

| Parameter Name | Description |
|---|---|
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>Range: 12 through 60 seconds<br><br>Default: 12 seconds<br><br>The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable. |
| Last Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br><br>**Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br><br>When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br><br>If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| Allow Services | Click **On** or **Off** for each service to allow or disallow the service on the cellular interface. |
| **Encapsulation** | |

| Parameter Name | Description |
|---|---|
| Encapsulation | Enable atleast one of the following encapsulation methods:<br>• **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1<br>• **GRE**: Enter a value to set GRE preference for TLOC.<br>Range: 0 through 4294967295<br>• **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1 |

### NAT

| Parameter Name | Description |
|---|---|
| UDP Timeout (Minutes) | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 65536 minutes<br>Default: 1 minute |

| Parameter Name | Description |
|---|---|
| TCP Timeout (Minutes) | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 65536 minutes<br>Default: 60 minutes (1 hour) |

### QoS

| Parameter Name | Description |
|---|---|
| Adaptive QoS | Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values.<br>• **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes.<br>• **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps.<br>• **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps. |
| Shaping Rate (kbps) | Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).<br>Range: 8 through 100000000 |

### ACL

| Parameter Name | Description |
|---|---|
| IPv4 Ingress Access List | Enter the name of an IPv4 access list to packets being received on the interface. |
| IPv4 Egress Access List | Enter the name of an IPv4 access list to packets being transmitted on the interface. |
| IPv6 Ingress Access List | Enter the name of an IPv6 access list to packets being received on the interface. |
| IPv6 Egress Access List | Enter the name of an IPv6 access list to packets being transmitted on the interface. |

### Advanced

| Parameter Name | Description |
|---|---|
| Shutdown | Click **No** to enable the interface. |
| Tracker / Tracker Group | Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet. |

| Parameter Name | Description |
|---|---|
| PPP Maximum Payload | Enter the maximum receive unit (MRU) value to be negotiated during PPP-over-Ethernet negotiation.<br>Range: 64 through 1792 bytes |
| Service Provider | Specify the details of the service provider. |
| Bandwidth Upstream (Kbps) | Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value. |
| Bandwidth Downstream (Kbps) | Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value. |
| IP MTU | Enter the maximum MTU size of packets on the interface.<br>Range: 576 through 1804<br>Default: 1500. |
| TCP MSS | Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: 1500 |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface. |
| IP Directed Broadcast | From the drop-down list, select **Global** to enable IP Directed Broadcast.<br>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. |
| Tracker / Tracker Group | Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet. |

## Ethernet PPPoE

Configure the PPPoE over GigabitEthernet interfaces on Cisco IOS XE Catalyst SD-WAN devices, to provide PPPoE client support.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

| Parameter Scope | Scope Description |
|---|---|
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the **Enter Key** field. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the **Enter Key** field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value appears for parameters that have a default setting. |

### Basic Configuration

| Parameter Name | Description |
|---|---|
| Ethernet Interface Name * | Enter the name of an ethernet interface.<br>For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**). |
| Description | Enter a description for the ethernet interface. |
| VLAN ID | Enter the VLAN identifier of the Ethernet interface. |
| Dialer Pool Member * | Enter the number of the dialer pool to which the interface belongs.<br>Range: 1 through 255 |

### PPP

| Parameter Name | Description |
|---|---|
| PPP Authentication Protocol* | Select the authentication protocol used by the MLP:<br>• **PAP**: Enter the username and password that are provided by your ISP. *username* can be up to 255 characters.<br>• **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol. |
| Authentication Type | Select the type authentication from one of the following options.:<br>• **Unidirectional**: Only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server.<br>• **Bidirectional**: Each side independently sends an Authenticate-Request (AUTH-REQ) and receives either an Authenticate-Acknowledge (AUTH-ACK) or Authenticate-Not Acknowledged (AUTH-NAK). |

| Parameter Name | Description |
|---|---|
| CHAP Hostname* | Enter the CHAP hostname. |
| CHAP Password* | Enter the CHAP password. |
| PAP Hostname* | Enter the PAP hostname. |
| PAP Password* | Enter the PAP password. |

**Tunnel**

| Parameter Name | Description |
|---|---|
| **Tunnel Interface** | |
| Per Tunnel QoS | Enable per tunnel QoS and choose **Spoke** to configure the spoke network topology |
| Color | Select a color for the TLOC. |
| Groups | Enter the list of groups in the field. |
| Exclude Controller Group List | Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to.<br>Range: 0 through 100 |
| Maximum Control Connections | Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>Range: 0 through 8 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager.<br>Range: 0 through 8<br>Default: 5 |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU.<br>Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |
| Border | From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC. |

| Parameter Name | Description |
|---|---|
| Validator As Stun Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Port Hop | From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface.<br>Default: **On**, which disallows port hopping on tunnel interface. |
| Low-Bandwidth Link | Click **On** to set the tunnel interface as a low-bandwidth link.<br>Default: **Off** |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Network Broadcast | From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template.<br>Default: **Off** |
| Carrier | From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel.<br>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default.<br>Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format:<br>**ge** *slot*/*port* |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>Range: 1 through 60 seconds<br>Default: 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>Range: 100 through 10000 milliseconds<br>Default: 1000 milliseconds (1 second) |

| Parameter Name | Description |
|---|---|
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>Range: 12 through 60 seconds<br><br>Default: 12 seconds<br><br>The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable. |
| Last Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br><br>**Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br><br>When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br><br>If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| Allow Services | Click **On** or **Off** for each service to allow or disallow the service on the cellular interface. |
| **Encapsulation** | |

| Parameter Name | Description |
|---|---|
| Encapsulation | Enable at least one of the following encapsulation methods:<br>• **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1<br>• **GRE**: Enter a value to set GRE preference for TLOC.<br>Range: 0 through 4294967295<br>• **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295<br>Default: 0<br>• **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255<br>Default: 1 |

### NAT

| Parameter Name | Description |
|---|---|
| UDP Timeout (Minutes) | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 1 minute |

| Parameter Name | Description |
|---|---|
| TCP Timeout (Minutes) | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 60 minutes (1 hour) |

### QoS

| Parameter Name | Description |
|---|---|
| Adaptive QoS | Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values.<br>• **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes.<br>• **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps.<br>• **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps. |
| Shaping Rate (kbps) | Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).<br>Range: 8 through 100000000 |

### ACL

| Parameter Name | Description |
|---|---|
| IPv4 Ingress Access List | Enter the name of an IPv4 access list to packets being received on the interface. |
| IPv4 Egress Access List | Enter the name of an IPv4 access list to packets being transmitted on the interface. |
| IPv6 Ingress Access List | Enter the name of an IPv6 access list to packets being received on the interface. |
| IPv6 Egress Access List | Enter the name of an IPv6 access list to packets being transmitted on the interface. |

### Advanced

| Parameter Name | Description |
|---|---|
| Shutdown | Choose **No** to enable the interface. |
| Tracker / Tracker Group | Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet. |

| Parameter Name | Description |
|---|---|
| Maximum Payload | Enter the maximum receive unit (MRU) value to be negotiated during PPP-over-Ethernet negotiation.<br>Range: 64 through 1792 bytes |
| IP MTU | Enter the maximum MTU size of packets on the interface.<br>Range: 576 through 1804<br>Default: 1500 |
| TCP MSS | Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: 1500 |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface. |
| IP Directed Broadcast | From the drop-down list, select **Global** to enable IP Directed Broadcast.<br>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. |
| Tracker / Tracker Group | Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet. |

## VPN Interface Multilink

Use the VPN Interface Multilink feature to configure multilink interface properties for Cisco IOS XE Catalyst SD-WAN devices.

### Basic Configuration

| Parameter Name | Description |
|---|---|
| Interface Name | Enter the name of the multilink interface. |
| Multilink Group Number * | Enter the number of the multilink group. It must be the same as the number you enter in the multilink interface name parameter.<br>Range: 1 through 65535 |

| Parameter Name | Description |
|---|---|
| PPP Authentication Protocol | Select the authentication protocol used by the multilink interface:<br>• **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP**: Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br>• **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |
| Hostname * | Enter hostname for PPP CHAP Authentication. |
| CHAP Password * | Enter password for PPP CHAP Authentication. |
| IPv4 Address * | To configure a static address, click **Static** and enter an IPv4 address.<br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server.<br>Default: 1 |
| Mask | Choose a value for the subnet mask. |
| IPv6 Address * | To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.<br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses. |

### Multilink

| Parameter Name | Description |
|---|---|
| **Add T1/E1 Interface** | |
| **T1** | |
| Description | Enter a description for the T1controller. |
| Slot* | Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0. |
| Framing | Enter the T1 frame type:<br>• **esf**: Send T1 frames as extended superframes. This is the default.<br>• **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing. |

| Parameter Name | Description |
|---|---|
| Clock Source | Select the clock source:<br>• **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source.<br>• **internal**: Use the controller framer as the primary clock. |
| Line Code | Select the line encoding to use to send T1 frames:<br>• **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes.<br>• **b8zs**: Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouped into extended superframes. |
| Cable Length | Select the cable length to configure the attenuation<br>• **short**: Set the transmission attenuation for cables that are 660 feet or shorter.<br>• **long**: Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet.<br>There is no default length. |
| **E1** | |
| Description | Enter a description for the E1 controller. |
| Slot* | Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0. |
| Framing | Enter the E1 frame type:<br>• **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default.<br>• **no-crc4**: Do no use CRC4. |
| Clock Source | Select the clock source:<br>• **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both E1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source.<br>• **internal**: Use the controller framer as the primary clock. |
| Line Code | Select the line encoding to use to send E1 frames:<br>• **ami**: Use alternate mark inversion (AMI) as the linecode.<br>• **hdb3**: Use high-density bipolar 3 as the linecode. This is the default. |
| **Add Channel Group** | |

| Parameter Name | Description |
|---|---|
| Channel Group | To configure the serial WAN on the interface, enter a channel group number.<br>Range: 0 through 30 |
| Time Slot | To configure the serial WAN on the interface, enter a value for the timeslot.<br>Range: 0 through 31 |
| **Add New A/S Serial Interface** | |
| Interface Name | Enter the name of the serial interface. |
| Description | Enter a description for the serial interface. |
| Bandwidth | For transmitted traffic, set the bandwidth above which to generate notifications. |
| Clock Rate | Specify a value for the clock rate.<br>Range: 1200 through 800000 |

**Tunnel**

| Parameter Name | Description |
|---|---|
| Color | Choose a color for the TLOC. |
| Restrict | Enable this option to drop packets when a tunnel to the service is unreachable. |
| Groups | Enter the list of groups in the field. |
| Border | From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC. |
| Maximum Control Connections | Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>Range: 0 through 8<br>Default: 2 |
| Validator As Stun Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Controller Group List | Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to.<br>Range: 0 through 100 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager.<br>Range: 0 through 8<br>Default: 5 |

| Parameter Name | Description |
|---|---|
| Port Hop | From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface.<br>Default: **On**, which disallows port hopping on tunnel interface |
| Low-Bandwidth Link | Click **On** to set the tunnel interface as a low-bandwidth link.<br>Default: **Off** |
| Network Broadcast | From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template.<br>Default: **Off** |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU.<br>Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes |

### ACL

| Parameter Name | Description |
|---|---|
| Ingress ACL - IPv4 | Enter the name of an IPv4 access list to packets being received on the interface. |
| Egress ACL - IPv4 | Enter the name of an IPv4 access list to packets being transmitted on the interface. |
| Igress ACL - IPv6 | Enter the name of an IPv6 access list to packets being received on the interface. |
| Egress ACL - IPv6 | Enter the name of an IPv6 access list to packets being transmitted on the interface. |

### Advanced

| Parameter Name | Description |
|---|---|
| Shutdown | Click **No** to enable the multilink interface. |
| Description | Enter a description for the multilink interface. |

| Parameter Name | Description |
|---|---|
| PPP Authentication Type | Select the type authentication from one of the following options.:<br>• **Unidirectional**: The server initiates the authentication.<br>• **Bidirectional**: Both the client and the server can initiate the authentication. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco 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.<br>Range: 500 through 1460 bytes<br>Default: 536 |
| Disable Fragmentation | Click **On** to disable fragmentation for PPP Multilink Protocol data units (PDUs). |
| Fragment Max Delay | Configure the delay between the transmission of fragments in a PPP Multilink Protocol link.<br>Range: 0 through 1000<br>Default: No CLI Command |
| Interleaving Fragments | Enable interleave fragmentation for PPP Multilink Protocol data units (PDUs). |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface. |
| IP MTU | Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP.<br>Range: 576 through 1804<br>Default: 1500 bytes |
| IP Directed-Broadcast | Enable the translation of a directed broadcast to physical broadcasts. |
| Shaping Rate (Kbps) | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |

# Service Profile

## Service VPN

This feature helps you configure a service VPN (range 1 – 65527, except 512) or the LAN VPN.

The following table describes the options for configuring the Service VPN feature.

### Basic Configuration

| Field | Description |
|---|---|
| **VPN*** | Enter the numeric identifier of the VPN. |
| **Name*** | Enter a name for the VPN. |
| **OMP Admin Distance IPv4** | Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255. |
| **OMP Admin Distance IPv6** | Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255. |

### DNS

| Field | Description |
|---|---|
| **Add DNS IPv4** | |
| **Primary DNS Address (IPv4)** | Enter the IP address of the primary IPv4 DNS server in this VPN. |
| **Secondary DNS Address (IPv4)** | Enter the IP address of a secondary IPv4 DNS server in this VPN. |
| **Add DNS IPv6** | |
| **Primary DNS Address (IPv6)** | Enter the IP address of the primary IPv6 DNS server in this VPN. |
| **Secondary DNS Address (IPv6)** | Enter the IP address of a secondary IPv6 DNS server in this VPN. |

### Host Mapping

| Field | Description |
|---|---|
| **Add New Host Mapping** | |
| **Hostname*** | Enter the hostname of the DNS server. The name can be up to 128 characters. |
| **List of IP*** | Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas. |

### Advertise OMP

| Field | Description |
|---|---|
| **Add OMP Advertise IPv4** | |

| Field | Description |
|---|---|
| **Protocol** | Choose a protocol to configure route advertisements to OMP, for this VPN:<br>• **bgp**<br>• **ospf**<br>• **ospfv3**<br>• **connected**<br>• **static**<br>• **network**<br>• **aggregate**<br>• **eigrp**<br>• **lisp**<br>• **isis** |
| **Select Route Policy** | Enter the name of the route policy.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Add OMP Advertise IPv6** | |
| **Protocol** | Choose a protocol to configure route advertisements to OMP, for this VPN:<br>• **BGP**<br>• **OSPF**<br>• **Connected**<br>• **Static**<br>• **Network**<br>• **Aggregate** |
| **Select Route Policy** | Enter the name of the route policy.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Protocol Sub Type** | When you choose the OSPF protocol, specify the sub type as external. |

**Route**

| Field | Description |
|---|---|
| **Add IPv4 Static Route** | |
| **Network Address*** | Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN. |

| Field | Description |
|---|---|
| **Subnet Mask*** | Enter the subnet mask. |
| **Next Hop/Null 0/VPN/DHCP** | Choose one of the following options to configure the next hop to reach the static route:<br>• **Next Hop**: When you choose this option, the **IPv4 Route Gateway Next Hop** field appears. Enable this option to add the next hop. You can add a hop with and without a tracker.<br>When you click **Add Next Hop**, the following fields appear:<br>• **Address***: Enter the next-hop IPv4 address.<br>• **Administrative Distance***: Enter the administrative distance for the route.<br>When you click **Add Next Hop with Tracker**, the following fields appear:<br>• **Address***: Enter the next-hop IPv4 address.<br>• **Administrative Distance***: Enter the administrative distance for the route.<br>• **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.<br>• **Null 0**: When you choose this option, the following field appears:<br>• **IPv4 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages.<br>• **VPN**: When you choose this option, the following field appears:<br>• **IPv4 Route VPN***: Selects VPN as the gateway to direct packets to the transport VPN.<br>• **DHCP**: When you choose this option, the following field appears:<br>• **IPv4 Route Gateway DHCP***: Assigns a static route for the default next-hop router when the DHCP server is accessed for an IP address. |
| **Add BGP Routing** | Choose a BGP route. |
| **Add OSPF Routing** | Choose an OSPF route. |
| **Add IPv6 Static Route** | |
| **Prefix*** | Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN. |

| Field | Description |
|---|---|
| **Next Hop/Null 0/NAT** | Choose one of the following options to configure the next hop to reach the static route:<br>• **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear:<br>  • **Address***: Enter the next-hop IPv6 address.<br>  • **Administrative distance***: Enter the administrative distance for the route.<br>• **Null 0**: When you choose this option, the following field appears:<br>  • **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages.<br>• **NAT**: When you choose this option, the following field appears:<br>  • **IPv6 NAT***: Choose NAT64 or NAT66. |

**Service**

| Field | Description |
|---|---|
| **Add Service** | |
| **Service Type** | Choose a service available at the local site and in the VPN.<br>Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**, **TE**, **SIG** |
| **IPv4 Addresses (Maximum: 4)*** | Enter up to four IP address, separated by commas. The service is advertised to the Cisco SD-WAN Controller only if one of the addresses can be resolved locally, at the local site, not via routes learned through OMP. You can configure up to four IP addresses. |
| **Tracking*** | Cisco Catalyst SD-WAN tests each service device periodically to check whether it is operational. Tracking saves the results of the periodic tests in a service log.<br>Tracking is enabled by default. |

**Service Route**

| Field | Description |
|---|---|
| **Add Service Route** | |
| **Prefix*** | Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route. |

| Field | Description |
|---|---|
| **Service*** | Configure routes pointing to any service.<br>Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**. |
| **VPN*** | Destination VPN to resolve the prefix. |

### GRE Route

| Field | Description |
|---|---|
| **Add GRE Route** | |
| **Prefix*** | Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route. |
| **Interface*** | Enter the name of one or two GRE tunnels to use to reach the service. |
| **VPN*** | Enter the number of the VPN to reach the service. This must be VPN 0. |

### IPSEC Route

| Field | Description |
|---|---|
| **Add ipSec Route** | |
| **Prefix*** | Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route. |
| **Interface*** | Enter the name of one or two IPsec tunnel interfaces. If you configure two interfaces, the first is the primary IPsec tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel. |

### NAT

| Field | Description |
|---|---|
| **Nat Pool** | |
| **NatPool Name*** | Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router. |
| **Prefix Length*** | Enter the NAT pool prefix length. |
| **Range Start*** | Enter a starting IP address for the NAT pool. |
| **Range End*** | Enter a closing IP address for the NAT pool. |

| Field | Description |
|---|---|
| **Overload*** | Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured.<br>Default: Enabled |
| **Direction*** | Choose the NAT direction. |
| **Nat64 V4 Pool** | |
| **Nat64 V4 Pool Name*** | Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router. |
| **Nat 64 V4 Pool Range Start*** | Enter a starting IP address for the NAT pool. |
| **Nat 64 V4 Pool Range End*** | Enter a closing IP address for the NAT pool. |
| **Overload*** | Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured.<br>Default: Disabled |

### Route Leak

| Field | Description |
|---|---|
| **Route leak from Global VPN** | |
| **Route Protocol*** | Choose a protocol from the available options to leak routes from global VPN to the service VPN that you are configuring. |
| **Select Route Policy** | Choose a route policy from the drop-down list. |
| **Redistribution (in service VPN)** | |
| **Protocol*** | Choose a protocol from the available options to redistribute the leaked routes. |
| **Select Route Policy** | Choose a route policy from the drop-down list. |
| **Route leak to Global VPN** | |
| **Route Protocol*** | Choose a protocol from the available options to leak routes from the service VPN that you are configuring to the global VPN. |
| **Select Route Policy** | Choose a route policy from the drop-down list. |
| **Redistribution (in global VPN)** | |
| **Protocol*** | Choose a protocol from the available options to redistribute the leaked routes. |

| Field | Description |
|---|---|
| **Select Route Policy** | Enter the name of the route policy. |
| **Route leak from other Service VPN(s)** | |
| **Source VPN** | Enter a value of the source VPN. |
| **Route Protocol*** | Choose a protocol from the available options to leak routes from the source service VPN to the service VPN that you are configuring. |
| **Select Route Policy** | Choose a route policy from the drop-down list. |
| **Redistribution (in Service VPN)** | |
| **Protocol*** | Choose a protocol from the available options to redistribute the leaked routes. |
| **Select Route Policy** | Choose a route policy from the drop-down list. |

### Route Target

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **Import Route Target List: Route Target*** | Configure a route target for IPv4 interfaces. It imports routing information from the target VPN extended community. |
| **Export Route Target List: Route Target*** | Configure a route target for IPv4 interfaces. It exports routing information to the target VPN extended community. |
| **IPv6 Settings** | |
| **Import Route Target List: Route Target*** | Configure a route target for IPv6 interfaces. It imports routing information from the target VPN extended community. |
| **Export Route Target List: Route Target*** | Configure a route target for IPv6 interfaces. It exports routing information to the target VPN extended community. |

## BGP Routing

Use the Border Gateway Protocol (BGP) feature for service-side routing to provide reachability to networks at the local site.

***Table 62: Basic Configuration***

| Field | Description |
|---|---|
| **AS Number** | Enter the local AS number. |
| **Router ID** | Enter the BGP router ID, in decimal four-part dotted notation. |
| **Propagate AS Path** | Enable this option to carry BGP AS path information into OMP. |

| Field | Description |
|---|---|
| **Propagate Community** | Enable this option to propagate BGP communities between Cisco Catalyst SD-WAN sites, across VPNs using OMP redistribution. |
| **External Routes Distance** | Specify the BGP route administrative distance for routes learned from other sites in the overlay network.<br>Range: 1 through 255<br>Default: 20 |
| **Internal Routes Distance** | Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another.<br>Range: 1 through 255<br>Default: 200 |
| **Local Routes Distance** | Specify the BGP route administrative distance for routes within the local AS. By default, a route received locally from BGP is preferred over a route received from OMP.<br>Range: 1 through 255<br>Default: 20 |

*Table 63: Unicast Address Family*

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **Maximum Paths** | Specify the maximum number of parallel internal BGP paths that can be installed into a route table to enable internal BGP multipath load sharing.<br>Range: 0 to 32 |
| **Originate** | Enable this option to allow the default route to be artificially generated and injected into the BGP Route Information Base (RIB), regardless of whether it is present in the routing table. The newly injected default is advertised to all the BGP peers. |
| **Redistribute** | |
| **Protocol*** | Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, **eigrp**, and **nat**.<br>At a minimum, choose **omp**. By default, OMP routes are not redistributed into BGP. |
| **Route Policy** | Enter the name of the route policy to apply to redistributed routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Network** | |

| Field | Description |
|---|---|
| **Network Prefix*** | Enter a network prefix to be advertised by BGP. The network prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0. |
| **Aggregate Address** | |
| **Aggregate Prefix*** | Enter the prefix of the addresses to aggregate for all BGP sessions. The aggregate prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0. |
| **AS Set Path** | Enable this option to generate set path information for the aggregated prefixes. |
| **Summary Only** | Enable this option to filter out more specific routes from BGP updates. |
| **Table Map** | |
| **Policy Name** | Enter the route map that controls the downloading of routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Filter** | When you enable this option, the route map specified in the **Policy Name** field controls whether a BGP route is to be downloaded to the Route Information Base (RIB). A BGP route is not downloaded to the RIB if it is denied by the route map.<br>When you disable this option, the route map specified in the **Policy Name** field is used to set certain properties, such as the traffic index, of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map. |
| **IPv6 Settings** | |
| **Maximum Paths** | Specify the maximum number of parallel internal BGP paths that can be installed into a route table to enable internal BGP multipath load sharing.<br>Range: 0 to 32 |
| **Originate** | Enable this option to allow the default route to be artificially generated and injected into the BGP RIB, regardless of whether it is present in the routing table. The newly injected default is advertised to all the BGP peers. |
| **Redistribute** | |
| **Protocol*** | Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, and **eigrp**.<br>At a minimum, choose **omp**. By default, OMP routes are not redistributed into BGP. |
| **Route Policy** | Enter the name of the route policy to apply to redistributed routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Network** | |

| Field | Description |
|---|---|
| **Network Prefix*** | Enter a network prefix to be advertised by BGP. The IPv6 network prefix is composed of the IPv6 address and the prefix length (1-128). For example, the IPv6 subnet is 2001:DB8:0000:0000:: and the prefix length is 64. |
| **Aggregate Address** | |
| **Aggregate Prefix*** | Enter the prefix of the addresses to aggregate for all BGP sessions. The IPv6 aggregate prefix is composed of the IPv6 address and the prefix length (1-128). For example, the IPv6 subnet is 2001:DB8:0000:0000:: and the prefix length is 64. |
| **AS Set Path** | Enable this option to generate set path information for the aggregated prefixes. |
| **Summary Only** | Enable this option to filter out more specific routes from BGP updates. |
| **Table Map** | |
| **Policy Name*** | Enter the route map that controls the downloading of routes.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Filter** | When you enable this option, the route map specified in the **Policy Name** field controls whether a BGP route is to be downloaded to the Route Information Base (RIB). A BGP route is not downloaded to the RIB if it is denied by the route map.<br>When you disable this option, the route map specified in the **Policy Name** field is used to set certain properties, such as the traffic index, of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map. |

***Table 64: Neighbor***

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **Address*** | Specify the IP address of the BGP neighbor. |
| **Description** | Enter a description of the BGP neighbor. |
| **Remote AS*** | Enter the AS number of the remote BGP peer. |
| **Interface Name** | Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface. |
| **Allowas in Number** | Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used. |

| Field | Description |
|---|---|
| **AS Override** | Enable this option to replace the AS number of the originating router with the AS number of the sending BGP router. |
| **Shutdown** | Disable this option to enable BGP for the VPN. |
| **Advanced Options** | |
| **Next-Hop Self** | Enable this option to configure the router to be the next hop for routes advertised to the BGP neighbor. |
| **Send Community** | Enable this option to send the BGP community attribute of the local router to the BGP neighbor. |
| **Send Extended Community** | Enable this option to send the BGP extended community attribute of the local router to the BGP neighbor. |
| **EBGP Multihop** | Set the time to live (TTL) for BGP connections to external peers.<br>Range: 1 to 255<br>Default: 1 |
| **Password** | Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number. |
| **Keepalive Time (seconds)** | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. Specify the keepalive time for the neighbor, to override the global keepalive time.<br>Range: 0 through 65535 seconds<br>Default: 60 seconds (one-third the hold-time value) |
| **Hold Time (seconds)** | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor, to override the global hold time.<br>Range: 0 through 65535 seconds<br>Default: 180 seconds (three times the keepalive time) |
| **Send Label** | Enable this option to allow the routers advertise to each other so that they can send MPLS labels with the routes. If the routers successfully negotiate their ability to send MPLS labels, the routers add MPLS labels to all the outgoing BGP updates. |
| **Add Neighbor Address Family** | |
| **Family Type*** | Choose the BGP IPv4 unicast address family. |

| Field | Description |
|---|---|
| **In Route Policy** | Specify the name of a route policy to apply to prefixes received from the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Out Route Policy** | Specify the name of a route policy to apply to prefixes sent to the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Maximum Prefix Reach Policy*** | Choose one of the following options:<br>• **Policy Off**: Policy is off.<br>• **Policy On - Restart**: Configure the time interval at which a peering session is re-established by a device when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit.<br>When you choose this option, the following fields appear:<br>• **Maximum Number of Prefixes***: Enter the maximum prefix limit.<br>Range: 1 to 4294967295<br>• **Threshold (percentage)**: Enter the threshold value:<br>Range: 1 to 100<br>Default: 75<br>• **Restart Interval (minutes)***: Enter the time interval.<br>Range: 1 to 65535 minutes<br>• **Policy On - Warning message**: Configure the device to disable the restart capability to allow you to adjust a peer that is sending too many prefixes.<br>• **Policy On - Disable Peer Neighbor**: When the device receives too many prefixes from a peer, and the maximum prefix limit is exceeded, the peering session is disabled or brought down. |
| **IPv6 Settings** | |
| **Address*** | Specify the IP address of the BGP neighbor. |
| **Description** | Enter a description of the BGP neighbor. |
| **Remote AS*** | Enter the AS number of the remote BGP peer. |
| **Interface Name** | Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface. |

| Field | Description |
|---|---|
| **Allowas in Number** | Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used. |
| **AS Override** | Enable this option to replace the AS number of the originating router with the AS number of the sending BGP router. |
| **Shutdown** | Disable this option to enable BGP for the VPN. |
| **Advanced Options** | |
| **Next-Hop Self** | Enable this option to configure the router to be the next hop for routes advertised to the BGP neighbor. |
| **Send Community** | Enable this option to send the BGP community attribute of the local router to the BGP neighbor. |
| **Send Extended Community** | Enable this option to send the BGP extended community attribute of the local router to the BGP neighbor. |
| **EBGP Multihop** | Set the time to live (TTL) for BGP connections to external peers.<br>Range: 1 to 255<br>Default: 1 |
| **Password** | Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number. |
| **Keepalive Time (seconds)** | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. Specify the keepalive time for the neighbor, to override the global keepalive time.<br>Range: 0 through 65535 seconds<br>Default: 60 seconds (one-third the hold-time value) |
| **Hold Time (seconds)** | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor, to override the global hold time.<br>Range: 0 through 65535 seconds<br>Default: 180 seconds (three times the keepalive time) |
| **Add IPv6 Neighbor Address Family** | |
| **Family Type*** | Choose the BGP IPv6 unicast address family. |

| Field | Description |
|---|---|
| **In Route Policy** | Specify the name of a route policy to apply to prefixes received from the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Out Route Policy** | Specify the name of a route policy to apply to prefixes sent to the neighbor.<br>Route policy is not supported in Cisco vManage Release 20.9.1. |
| **Maximum Prefix Reach Policy*** | Choose one of the following options:<br>• **Policy Off**: Policy is off.<br>• **Policy On - Restart**: Configure the time interval at which a peering session is re-established by a device when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit.<br>When you choose this option, the following fields appear:<br>• **Maximum Number of Prefixes***: Enter the maximum prefix limit.<br>Range: 1 to 4294967295<br>• **Threshold (percentage)**: Enter the threshold value:<br>Range: 1 to 100<br>Default: 75<br>• **Restart Interval (minutes)***: Enter the time interval.<br>Range: 1 to 65535 minutes<br>• **Policy On - Warning message**: Configure the device to disable the restart capability to allow you to adjust a peer that is sending too many prefixes.<br>• **Policy On - Disable Peer Neighbor**: When the device receives too many prefixes from a peer, and the maximum prefix limit is exceeded, the peering session is disabled or brought down. |

## OSPF Routing

Open Shortest Path First (OSPF) is a routing protocol for IP networks. It can be used for service-side routing to provide reachability to networks at the local site.

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown.

### Basic Configuration

| Field | Description |
|---|---|
| **Router ID** | Enter the OSPF router ID, in decimal four-part dotted notation. This is the IP address associated with the router for OSPF adjacencies. |
| **Distance for External Routes** | Specify the OSPF route administration distance for routes learned from other domains.<br>Range: 1 through 255<br>Default: 110 |
| **Distance for Inter-Area Routes** | Specify the OSPF route administration distance for routes coming from one area into another.<br>Range: 1 through 255<br>Default: 110 |
| **Distance for Intra-Area Routes** | Specify the OSPF route administration distance for routes within an area.<br>Range: 0 through 255<br>Default: 110 |

### Redistribute

| Field | Description |
|---|---|
| **Add Redistribute** | |
| **Protocol** | Choose the protocol from which to redistribute routes into OSPF.<br>• Static<br>• Connected<br>• BGP<br>• OMP<br>• NAT<br>• EIGRP |

### Maximum Metric (Router LSA)

| Field | Description |
|---|---|
| **Add Router LSA** | |

| Field | Description |
|---|---|
| **Type** | Configure OSPF to advertise a maximum metric so that other routers do not prefer this router as an intermediate hop in their Shortest Path First (SPF) calculation.<br>Choose a type:<br>• **administrative**: Force the maximum metric to take effect immediately, through operator intervention.<br>• **on-startup**: Advertise the maximum metric for the specified time. |

**Area**

| Field | Description |
|---|---|
| **Add Area** | |
| **Area Number*** | Enter the number of the OSPF area.<br>Range: 32-bit number |
| **Set the area type** | Choose the type of OSPF area:<br>• Stub<br>• NSSA |
| **Add Interface** | Configure the properties of an interface in an OSPF area. |
| **Name*** | Enter the name of the interface, in the format **`geslot/port`** or **`loopback number`**. |
| **Hello Interval (seconds)*** | Specify how often the router sends OSPF hello packets.<br>Range: 1 through 65535 seconds<br>Default: 10 seconds |
| **Dead Interval (seconds)*** | Specify how often the router must receive an OSPF hello packet from its neighbor. If no packet is received, the router assumes that the neighbor is down.<br>Range: 1 through 65535 seconds<br>Default: 40 seconds (four times the default hello interval) |
| **LSA Retransmission Interval (seconds)*** | Specify how often the OSPF protocol retransmits LSAs to its neighbors.<br>Range: 1 through 65535 seconds<br>Default: 5 seconds |
| **Interface Cost** | Specify the cost of the OSPF interface.<br>Range: 1 through 65535 |

| Field | Description |
|---|---|
| **Designated Router Priority*** | Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the node with the highest router ID becomes the DR or the backup DR.<br>Range: 0 through 255<br>Default: 1 |
| **OSPF Network Type** | Choose the OSPF network type to which the interface is to connect:<br>• Broadcast network<br>• Point-to-point network<br>• Non-broadcast network<br>• Point-to-multipoint network |
| **Passive Interface*** | Specify whether to set the OSPF interface to be passive. A passive interface advertises its address, but does not actively run the OSPF protocol.<br>Default: Disabled |
| **Authentication Type** | Choose the authentication type:<br>• **simple**: Password is sent in clear text.<br>• **message-digest**: MD5 algorithm generates the password. |
| **Message Digest Key** | Enter the MD5 authentication key, in clear text or as an AES-encrypted key. It can be from 1 to 255 characters. |
| **md5** | Enter the key ID for message digest (MD5 authentication). It can be 1 to 32 characters. |
| **Add Range** | Configure the area range of an interface in an OSPF area. |
| **IP Address*** | Enter the IP address. |
| **Subnet Mask*** | Enter the subnet mask. |
| **Cost** | Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination.<br>Range: 0 through 16777214 |
| **No-advertise*** | Enable this option to not advertise the Type 3 summary LSAs. |

### Advanced

| Field | Description |
|---|---|
| **Reference Bandwidth (Mbps)** | Specify the reference bandwidth for the OSPF auto-cost calculation for the interface.<br>Range: 1 through 4294967 Mbps<br>Default: 100 Mbps |
| **RFC 1583 Compatible** | By default, the OSPF calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328. |
| **Originate** | Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear:<br>• **Always**: Enable this option to always advertise the default route in an OSPF routing domain.<br>• **Default Metric**: Set the metric used to generate the default route.<br>Range: 0 through 16777214<br>Default: 10<br>• **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route. |
| **SPF Calculation Delay (milliseconds)** | Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.<br>Range: 1 through 600000 milliseconds (60 seconds)<br>Default: 200 milliseconds |
| **Initial Hold Time (milliseconds)** | Specify the amount of time between consecutive SPF calculations.<br>Range: 1 through 600000 milliseconds (60 seconds)<br>Default: 1000 milliseconds |
| **Maximum Hold Time (milliseconds)** | Specify the longest time between consecutive SPF calculations.<br>Range: 1 through 600000<br>Default: 10000 milliseconds (60 seconds) |

## Wireless LAN

This feature helps you configure a wireless controller.

The following tables describe the options for configuring the Wireless LAN feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Enable 2.4G*** | Disable this option to shut down the radio type of 2.4 GHz.<br>Default: Enabled |
| **Enable 5G*** | Disable this option to shut down the radio type of 5 GHz.<br>Default: Enabled |
| **Country*** | Choose the country where the router is installed. |
| **Username*** | Specify the username of Cisco Mobility Express. |
| **Password*** | Specify the password of Cisco Mobility Express. |

### ME IP Config

| Field | Description |
|---|---|
| **ME Dynamic IP*** | Enable this option so that the interface receives its IP address dynamically from a DHCP server. |
| **ME IP Address** | Specify the IP address of Cisco Mobility Express. |
| **Subnet Mask** | Specify the subnet mask of Cisco Mobility Express. |
| **Default Gateway** | Specify the default gateway address of Cisco Mobility Express. |

### SSID

| Field | Description |
|---|---|
| **Add SSID** | |
| **SSID Name*** | Enter a name for the wireless SSID.<br>It can be a string from 4 to 32 characters. The SSID must be unique. |
| **Admin State*** | Enable this option to indicate that the interface has been configured. |
| **Broadcast SSID*** | Enable this option if you want to broadcast the SSID. Disable this option if you do not want the SSID to be visible to all the wireless clients. |
| **VLAN (Range 1-4094)*** | Enter a VLAN ID for the wireless LAN traffic. |
| **Radio Type** | Choose one of the following radio types:<br>• **2.4GHz**<br>• **5GHz**<br>• **All** |

| Field | Description |
|---|---|
| **Security Type*** | Choose a security type:<br>• **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server.<br>• **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase.<br>• **Open**: Choose this option to allow access to the wireless network without authentication. |
| **Passphrase*** | This field is available if you choose **WPA2 Personal** as the security type. Set a pass phrase. This pass phrase provides users access to the wireless network. |
| **QoS Profile** | Choose a QoS profile. |

## Switch Port

Use the Switch Port feature to configure bridging for Cisco Catalyst SD-WAN.

The following table describes the options for configuring the Switch Port feature.

| Field | Description |
|---|---|
| **Age Out Time** | Enter how long an entry is in the MAC table before it ages out. Set the value to 0 to prevent entries from timing out.<br>Range: 0, 10 through 1000000 seconds<br>Default: 300 seconds |
| **Configure Interface** | |
| **Interface Name** | Enter the name of the interface to associate with the bridging domain, in the format **`geslot/port`**. |

| Field | Description |
|---|---|
| **Mode** | Choose the switch port mode.<br>• **access**: Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic only for one VLAN. When you choose **access**, the following field appears:<br>**Switchport Access Vlan**: Enter the VLAN number, which can be a value from 1 through 4094.<br>• **trunk**: Configure the interface as a trunk port. You can configure one or more VLANs on a trunk port, and the port can carry traffic for multiple VLANs. When you choose **trunk**, the following fields appear:<br>• **Allowed Vlans**: Enter the number of the VLANs for which the trunk can carry traffic and a description for the VLAN.<br>• **Switchport Trunk Native Vlan**: Enter the number of the VLAN allowed to carry untagged traffic. |
| **Shutdown** | Enable the interface. By default, an interface is disabled. |
| **Speed** | Enter the speed of the interface. |
| **Duplex** | Choose **full** or **half** to specify whether the interface runs in full-duplex or half-duplex mode. |
| **Port Control** | Choose the port control mode to enable IEEE 802.1X port-based authentication on the interface.<br>• **auto**: Enables IEEE 802.1X authentication and starts the port in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The device requests the identity of the supplicant and starts relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the device by using the supplicant MAC address.<br>• **force-unauthorized**: Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The device cannot provide authentication services to the supplicant through the port.<br>• **force-authorized**: Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. |
| **Voice VLAN** | Enter the Voice VLAN ID. |

| Field | Description |
|---|---|
| **Pae Enable** | The Cisco Catalyst SD-WAN device acts as a port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port. |
| **MAC Authentication Bypass** | Enable this option to allow MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-IEEE 802.1X–compliant clients using a RADIUS server. |
| **Host Mode** | Choose whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients).<br>• **single-host**: Grant access only to the first authenticated host. This is the default.<br>• **multi-auth**: Grant access to one host on a voice VLAN and multiple hosts on data VLANs.<br>• **multi-host**: Grant access to multiple hosts.<br>• **multi-domain**: Grant access to both a host and a voice device, such as an IP phone on the same switch port. |
| **Enable Periodic Reauth** | Enable periodic re-authentication. By default, this option is enabled. |
| **Inactivity** | Enter the inactivity timeout time in seconds.<br>Default: 60 seconds |
| **Reauthentication** | Enter the re-authentication interval in seconds. |
| **Control Direction** | Choose **both** (bidirectional) or **in** (unidirectional) authorization mode. |
| **Restricted VLAN** | Enter the restricted VLAN (or authentication-failed VLAN) for IEEE 802.1x-compliant clients. Configure limited services to IEEE 802.1X-compliant clients that failed RADIUS authentication. |
| **Guest VLAN** | Enter the guest VLAN to drop non-IEEE 802.1X enabled clients, if the client is not in the MAB list. |
| **Critical VLAN** | Enter the critical VLAN (or authentication-failed VLAN) for IEEE 802.1x-compliant clients. Configure network access when RADIUS authentication or the RADIUS server fails. |
| **Enable Voice** | Enable the critical voice VLAN. |
| **Configure Static Mac Address** | |
| **MAC Address** | Enter the static MAC address to map to the switch port interface. |
| **Interface Name** | Enter the name of the switch port interface. |
| **VLAN ID** | Enter the number of the VLAN for the switch port. |

## Ethernet Interface

This feature helps you configure the Ethernet interface on a service VPN (range 1 – 65527, except 512).

The following table describes the options for configuring the Ethernet Interface 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. |
| **Associated VPN** | The service VPN. |

### Basic Configuration

| Field | Description |
|---|---|
| **Shutdown** | Enable or disable the interface. |
| **Interface Name** | Enter a name for the interface. Spell out the interface names completely (for example, GigabitEthernet0/0/0).<br>Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured. |
| **Description** | Enter a description for the interface. |
| **IPv4 Settings** | Configure an IPv4 VPN interface.<br>• **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server.<br>• **Static**: Choose **Static** to enter an IP address that doesn't change. |
| **Dynamic DHCP Distance** | Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**.<br>Default: 1 |
| **IP Address** | Enter a static IPv4 address. This option is available when you choose **Static**. |
| **Subnet Mask** | Enter the subnet mask. |
| **Add Secondary IP Address** | Enter up to four secondary IPv4 addresses for a service-side interface.<br>• **IP Address***: Enter the IP address.<br>• **Subnet Mask:** Enter the subnet mask. |

| Field | Description |
|---|---|
| **DHCP Helper** | To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BOOTP (broadcast) DHCP requests that it receives from the specified DHCP servers. |
| **IPv6 Settings** | Configure an IPv6 VPN interface.<br>• **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server.<br>• **Static**: Choose **Static** to enter an IP address that doesn't change.<br>• **None** |
| **IPv6 Address Primary** | Enter a static IPv6 address. This option is available when you choose **Static**. |
| **Add Secondary Ipv6** | Enter up to two secondary IPv6 addresses for a service-side interface. |
| **Add DHCP Helper** | |
| **DHCPv6 Helper*** | To designate the interface as a DHCP helper on a router, enter up to eight IP addresses for DHCP servers in the network. A DHCP helper interface forwards BOOTP (broadcast) DHCP requests that it receives from the specified DHCP servers. |
| **DHCPv6 Helper VPN** | Enter the VPN ID of the VPN source interface for the DHCP helper. |

### NAT

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **NAT** | Enable this option to have the interface act as a NAT device. |
| **NAT Type*** | Choose the NAT translation type for IPv4:<br>• **pool**<br>• **loopback**<br>Default: **pool** |
| **Range Start** | Enter a starting IP address for the NAT pool. |
| **Range End** | Enter a closing IP address for the NAT pool. |
| **Prefix Length** | Enter the NAT pool prefix length. |

| Field | Description |
|---|---|
| **Overload** | Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured.<br>Default: Enabled |
| **NAT Loopback** | Enter the IP address of the loopback interface. |
| **UDP Timeout** | Specify when NAT translations over UDP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 1 minutes |
| **TCP Timeout** | Specify when NAT translations over TCP sessions time out.<br>Range: 1 through 8947 minutes<br>Default: 60 minutes (1 hour) |
| **Add New Static NAT** | |
| **Source IP*** | Enter the source IP address to be translated. |
| **Translate IP*** | Enter the translated source IP address. |
| **Direction** | Choose the direction in which to perform network address translation.<br>• **inside**: Translates the IP address of packets that are coming from the service side of the device and that are destined for the transport side of the router.<br>• **outside**: Translates the IP address of packets that are coming to the device from the transport side device and that are destined for a service-side device. |
| **Source VPN*** | Enter the source VPN ID. |
| **IPv6 Settings** | |
| **NAT** | Enable this option to have the interface act as a NAT device. |
| **Select NAT** | Choose NAT64 or NAT66. When you choose NAT66 and click **Add Static NAT66**, the following fields appear:<br>• **Source Prefix***: Enter the source IPv6 prefix.<br>• **Translated Source Prefix***: Enter the translated source prefix.<br>• **Source VPN ID***: Enter the source VPN ID. |

### VRRP

| Field | Description |
|---|---|
| **IPv4 Settings** | |
| **Add Vrrp Ipv4** | |
| **Group ID*** | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>Range: 1 through 255 |
| **Priority*** | Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router.<br>Range: 1 through 254<br>Default: 100 |
| **Timer*** | Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router .<br>Range: 100 through 40950 seconds<br>Default: 100 seconds |
| **Track OMP*** | When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. |
| **Prefix List** | Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router. |
| **IP Address*** | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP. |
| **Tloc Prefix Change*** | Enable or disable this option to set whether the TLOC preference can be changed or not. |
| **Tloc Prefix Change Value** | Enter the TLOC preference change value.<br>Range: 100 to 4294967295 |
| **Add VRRP IP Address Secondary** | |
| **IP Address*** | Enter an IP address for the secondary VRRP router. |

| Field | Description |
|---|---|
| **Subnet Mask** | Enter the subnet mask. |
| **Add VRRP Tracking Object** | |
| **Tracker ID*** | Enter the interface object ID or object group tracker ID. |
| **Tracker Action*** | Choose one of the options:<br>• **decrement**<br>• **shutdown** |
| **Decrement Value*** | Enter a decrement value.<br>Range: 1-255 |
| **IPv6 Settings** | |
| **Add Vrrp Ipv6** | |
| **Group ID*** | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>Range: 1 through 255 |
| **Priority*** | Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router.<br>Range: 1 through 254<br>Default: 100 |
| **Timer*** | Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router .<br>Range: 100 through 40950 seconds<br>Default: 100 seconds |
| **Track OMP*** | When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. |
| **Track Prefix List** | Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router. |

| Field | Description |
|---|---|
| **Link Local IPv6 Address*** | Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8. |
| **Global IPv6 Prefix** | Enter a virtual global unicast IPv6 address, which represents the global address of the group. The address should be an IPv6 global prefix address that has the same mask as the interface forwarding address on which the VRRP group is configured. For example, 2001::2/124.<br>You can configure up to three global IPv6 addresses. |

### ARP

| Field | Description |
|---|---|
| **Add ARP** | |
| **IP Address*** | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| **MAC Address*** | Enter the MAC address in colon-separated hexadecimal notation. |

### TrustSec

| Field | Description |
|---|---|
| **Enable SGTPropogation** | Enable this option to use the Cisco TrustSec Security Group Tag (SGT) propagation feature. |
| **Propagate** | Enable this option to propagate SGT in Cisco Catalyst SD-WAN. |
| **Security Group Tag** | Enter a value that can be used as a tag. |
| **Enable Enforced Propagation** | Enable this option to start SGT enforcement on the interface. |
| **Enforced Security Group Tag** | Enter a value that can be used as a tag for enforcement. |

### Advanced

| Field | Description |
|---|---|
| **Duplex** | Specify whether the interface runs in full-duplex or half-duplex mode.<br>Default: full |
| **MAC Address** | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |

| Field | Description |
|---|---|
| **IP MTU** | Specify the maximum MTU size of packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **Interface MTU** | Enter the maximum transmission unit size for frames received and transmitted on the interface.<br>Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet)<br>Default: 1500 bytes |
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 500 to 1460 bytes<br>Default: None |
| **Speed** | Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation.<br>Values: 10, 100, 1000, 2500, or 10000 Mbps |
| **ARP Timeout** | ARP timeout controls how long we maintain the ARP cache on a router. Specify how long it takes for a dynamically learned ARP entry to time out.<br>Range: 0 through 2147483 seconds<br>Default: 1200 seconds |
| **Autonegotiate** | Enable this option to turn on autonegotiation. |
| **Media Type** | Specify the physical media connection type on the interface. Choose one of the following:<br>• **auto-select**: A connection is automatically selected.<br>• **rj45**: Specifies an RJ-45 physical connection.<br>• **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media. |
| **Load Interval** | Enter an interval value for interface load calculation. |
| **Tracker** | Static-route tracking for service VPNs enables you to track the availability of the configured endpoint address to determine if the static route can be included in the routing table of a device. 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. |

| Field | Description |
|---|---|
| **ICMP Redirect Disable** | ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway.<br>By default, an interface allows ICMP redirect messages. |
| **XConnect** | Enter the name of a physical interface on the same router that connects to the WAN transport. |
| **IP Directed Broadcast** | An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.<br>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.<br>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet. |

## SVI Interface

This feature helps you configure a switch virtual interface (SVI) to configure a VLAN interface.

For each parameter of the feature 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 to the left of the parameter field and choose one of 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. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template.<br>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 Catalyst SD-WAN device to a device template.<br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br>Examples of device-specific parameters are system IP address, host name, 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.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

The following tables describe the options for configuring the SVI Interface 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. |
| **Associated VPN: VPN*** | Choose a VPN. |

### Basic Configuration

| Field | Description |
|---|---|
| **Shutdown** | Enable or disable the VLAN interface. |
| **VLAN Interface Name*** | Enter a name for the VLAN interface.<br>The name must contain a minimum of five characters. The name must be in the following format:<br>`^Vlan(([1-9]\d\|\d){0,2}(0\|[1-9]\d*)([:\|\.][1-9]\d*)?` |
| **Interface Description** | Enter a description for the interface. |
| **Interface MTU** | Enter the maximum transmission unit size for frames received and transmitted on the interface.<br>Range: 1500 through 9216<br>Default: 1500 bytes |
| **IP MTU** | Enter the maximum transmission unit (MTU) size of IP packets sent on an interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **Configure IPV4 Address** | |
| **IPv4 Address Prefix*** | Enter the IPv4 address for the interface. |
| **List of DHCP helper addresses*** | Enter up to eight IP addresses for DHCP servers in the network to have the interface be a DHCP helper. Separate each address with a comma. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |

| Field | Description |
|---|---|
| **Configure IPV4 Secondary Address** | |
| **Secondary IP Address*** | Enter up to four secondary IP addresses. |
| **Configure IPV6 Address** | |
| **IPV6 address*** | Enter the IPv6 address for the interface. |
| **Configure IPV6 Secondary Address** | |
| **Address*** | Enter up to four secondary IP addresses. |
| **Configure IPV6 DHCP Helper** | |
| **Address*** | Enter an IP address for DHCP servers in the network to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| **VPN** | VPN ID for the DHCP helper address. |

### ACL

| Field | Description |
|---|---|
| **Configure Access List V4** | |
| **Direction*** | Choose a direction of the ACL: **in** or **out**. |
| **Name of ACL*** | Enter the name of the access list. |
| **Configure Access List V6** | |
| **Direction*** | Choose a direction of the ACL: **in** or **out**. |
| **Name of ACL*** | Enter the name of the access list. |

### VRRP

| Field | Description |
|---|---|
| **Configure VRRP** | |
| **Group ID*** | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>Range: 1 through 255 |

| Field | Description |
|---|---|
| **Priority*** | Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router.<br>Range: 1 through 254<br>Default: 100 |
| **Timer*** | Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router .<br>Range: 100 through 40950 seconds<br>Default: 100 seconds |
| **Track OMP** | When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. |
| **Prefix List*** | Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router. |
| **IP Address** | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP. |
| **Add VRRP IP Address Secondary** | |
| **Address*** | Enter an IP address for the secondary VRRP router. |
| **TLOC Preference Change** | Enable or disable this option to set whether the TLOC preference can be changed or not. |
| **Add VRRP Tracking Object** | |
| **Tracker Id*** | Enter the interface object ID or object group tracker ID. |
| **Track Action*** | Choose one of the options:<br>• **decrement**<br>• **shutdown** |

| Field | Description |
|---|---|
| **Decrement Value** | Enter a decrement value.<br>Range: 1-255<br>From Cisco vManage Release 20.10.1, this option is enabled only when you choose **decrement** in **Track Action**. |
| **Configure VRRP IPv6** | |
| **Group ID*** | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>Range: 1 through 255 |
| **Priority*** | Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router.<br>Range: 1 through 254<br>Default: 100 |
| **Timer*** | Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router .<br>Range: 100 through 40950 seconds<br>Default: 100 seconds |
| **Track OMP*** | When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. |
| **Track Prefix List** | Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router. |
| **Add VRRP IPv6 Primary** | |
| **IPv6 Link Local*** | Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8. |
| **Prefix** | Enter the IPv6 address of the primary VRRP router. |

### ARP

| Field | Description |
|---|---|
| **Configure ARP** | |
| **IP Address*** | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| **MAC Address*** | Enter the MAC address in colon-separated hexadecimal notation. |

### Advanced

| Field | Description |
|---|---|
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 to 1960 bytes<br>Default: None |
| **ARP Timeout** | Specify how long it takes for a dynamically learned ARP entry to time out.<br>Range: 0 through 2678400 seconds (744 hours)<br>Default: 1200 (20 minutes) |
| **IP Directed-Broadcast** | An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.<br>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.<br>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet. |
| **ICMP/ICMPv6 Redirect Disable** | ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway.<br>By default, an interface allows ICMP redirect messages. |

## DHCP Server

This feature allows an interface to be configured as a DHCP helper so that it forwards the broadcast DHCP requests that it receives from the DHCP servers.

For each parameter of the feature 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 to the left of the parameter field and choose one of the following:

### Basic Configuration

| Field | Description |
|---|---|
| **Address Pool*** | Enter the IPv4 prefix range, in the format **`prefix/length`**, for the pool of addresses in the service-side network for which the router interface acts as the DHCP server. |
| **Exclude** | Enter one or more IP addresses to exclude from the DHCP address pool. To specify multiple individual addresses, list them separated by a comma. To specify a range of addresses, separate them with a hyphen. |
| **Lease Time(seconds)** | Specify how long a DHCP-assigned IP address is valid.<br>Range: 60 through 31536000 seconds<br>Default: 86400 |

### Static Lease

| Field | Description |
|---|---|
| **Add Static Lease** | |
| **MAC Address*** | Enter the MAC address of the client to which the static IP address is being assigned. |
| **IP*** | Enter the static IP address to assign to the client. |

### DHCP Options

| Field | Description |
|---|---|
| **Add Option Code** | |
| **Code*** | Configure the option code.<br>Range: 1-254 |
| **Type** | Choose one of the three types:<br>• **ASCII**: Specify an ASCII value.<br>• **Hex**: Specify a hex value.<br>• **IP**: Specify IP addresses. You can specify up to eight IP addresses. |

### Advanced

| Field | Description |
|---|---|
| **Interface MTU** | Specify the maximum MTU size of packets on the interface.<br>Range: 68 to 65535 bytes |
| **Domain Name** | Specify the domain name that the DHCP client uses to resolve hostnames. |
| **Default Gateway** | Enter the IP address of a default gateway in the service-side network. |
| **DNS Servers** | Enter one or more IP address for a DNS server in the service-side network. Separate multiple entries with a comma. You can specify up to eight addresses. |
| **TFTP Servers** | Enter the IP address of a TFTP server in the service-side network. You can specify one or two addresses. If two, separate them with a comma. |

## Multicast

The Cisco IOS XE Catalyst SD-WAN multicast overlay software extends Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) over the Cisco Catalyst SD-WAN overlay using Overlay Management Protocol (OMP). Protocol Independent Multicast Sparse-Mode (PIM-SM) is deployed in the customer VPNs, and the Cisco IOS XE MVPN is used to integrate PIM in customer VPNs and OMP in the overlay. The OMP replicator is used in overlay multicast to optimize the multicast distribution tree across the overlay topology. The Cisco IOS XE Catalyst SD-WAN router supports IGMPv2 and IGMPv3 reports and advertises receiver's multicast interest to remote Cisco Catalyst SD-WAN routers using OMP. Depending on the level of optimization required, the Cisco Catalyst SD-WAN routers join or prune to or from the replicators, and replicators use OMP to relay the join or prune to the Cisco Catalyst SD-WAN router providing overlay connectivity to the PIM-RP or source.

The Cisco IOS XE Catalyst SD-WAN overlay multicast network supports the following protocols:

- Protocol Independent Multicast (PIM)
- Internet Group Management Protocol (IGMP)
- MSDP

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

| Parameter Scope | Scope Description |
|---|---|
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the **Enter Key** field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the **Enter Key** field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value is shown for parameters that have a default setting. |

The following tables describe the options for configuring the Multicast 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. |

***Table 65: Basic Configuration***

| Field | Description |
|---|---|
| **SPT Only** | Enable this option to ensure that the Rendezvous Points (RPs) can communicate with each other using the shortest-path tree. |
| **Local Replicator** | Enable this option to configure the Cisco IOS XE Catalyst SD-WAN device as a multicast replicator. |
| **Threshold** | Specify a value.<br>Optional, keep it set to the default value if you are not configuring a replicator. |

***Table 66: PIM***

| Field | Description |
|---|---|
| **Source Specific Multicast (SSM)** | Enable this option to configure SSM. |

| Field | Description |
|---|---|
| **ACL** | Specify an access control list value. An access control list allows you to filter multicast traffic streams using the group and sometimes source IPv4 or IPv6 addresses.<br><br>Configure an IPv4 access control list using a standard or extended access list and attach it to your device before enabling PIM. You must have created a valid standard or extended ACL before using the ACL in your multicast configuration.<br><br>**Note** You cannot configure an ACL for a PIM feature template using Cisco SD-WAN Manager. You must configure the ACL using a CLI add-on template. For information on configuring ACL using the CLI add-on template, see the section **Configure an ACL for Multicast Using a CLI Add-On Template** in chapter **Multicast Overlay Routing** of the Cisco Catalyst SD-WAN Routing Configuration Guide. |
| **SPT Threshold** | Specify the traffic rate, in kbps, at which to switch from the shared tree to the shortest-path tree (SPT). Configuring this value forces traffic to remain on the shared tree and travel via the RP instead of via the SPT. |
| **Add Interface** | |
| **Interface Name** | Enter the name of an interface that participates in the PIM domain, in the format **ge** *slot /port*. |
| **Query Interval(sec)** | Specify how often the interface sends PIM query messages. Query messages advertise that PIM is enabled on the router. |
| **Join/Prune Interval(sec)** | Specify how often PIM multicast traffic can join or be removed from a rendezvous point tree (RPT) or shortest-path tree (SPT). Cisco IOS XE Catalyst SD-WAN device send join and prune messages to their upstream RPF neighbor. |
| **How do you want to configure your Rendezvous Point (RP)**<br><br>Cisco IOS XE SD-WAN supports the following modes: | |
| **Static** | Click this check box to a specify the static IP address of a rendezvous point (RP). |
| **Add Static RP** | |
| **IP Address** | Specify the static IP address of a rendezvous point (RP). |
| **ACL** | Specify an ACL value. |

| Field | Description |
|---|---|
| **Override** | Enable this option for cases when dynamic and static group-to-RP mappings are used together and there is an RP address conflict. In this case, the RP address configured for a static group-to-RP mapping takes precedence.<br>If you do not enable this option, and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings. |
| **Auto RP** | Click this check box to enable reception of PIM group-to-RP mapping updates. This enables reception on the Auto-RP multicast groups, 224.0.1.39 and 224.0.1.40. |
| **RP Announce** | Click this check box to enable transmission of Auto-RP multicast messages. |
| **RP Discovery** | Click this check box to enable Auto-RP automatic discovery of rendezvous points (RPs) in the PIM network so that the router can serve as an Auto-RP mapping agent. An Auto-RP mapping receives all the RPs and their respective multicast groups and advertise consistent group-to-RP mapping updates. |
| **Interface** | Specify the source interface for Auto-RP RP Announcements or RP Discovery messages. |
| **Scope** | Specify the IP header Time-to-Live (TTL) for Auto-RP RP Announcements or RP Discovery messages. |
| **PIM-BSR** | Configure a PIM BSR. |
| **RP Candidate** | |
| **Interface Name** | Choose the interface that you used for configuring the PIM feature template. |
| **Access List** | Add an access list value if you have configured the access list with a value. |
| **Interval** | Add an interval value if you have configured the interval with a value. |
| **Priority** | Specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device. |
| **BSR Candidate (Maximum: 1)** | |
| **Interface Name** | Chose the same interface from the drop-down list that you used for configuring the PIM feature template. |
| **Hash Mask Length** | Specify the hash mask length. Valid values for hash mask length are 0–32. |
| **Priority** | Specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device. |
| **RP Candidate Access List** | Add a value if you have configured the RP candidate access list with a value.<br>An RP candidate uses a standard ACL where you can enter the name for the access list. |

*Table 67: IGMP*

| Field | Description |
|---|---|
| **Add IGMP** | |
| **Interface** | Enter the name of the interface to use for IGMP. To add another interface, click **Add**. |
| **Version** | Specify a version number.<br>Optional, keep it set to the default version number. |
| **Group Address** | Enter a group address to join a multicast group. |
| **Source Address** | Enter a source address to join a multicast group. |
| **Add** | Click **Add** to add the IGMP for the group. |

*Table 68: MSDP*

| Field | Description |
|---|---|
| **Originator-ID** | Specify the ID of the originating device. This ID is the IP address of the interface that is used as the RP address. |
| **Connection Retry Interval** | Configure an interval at which MSDP peers will wait after peering sessions are reset before attempting to re-establish the peering sessions. |
| **Mesh Group** | |
| **Mesh Group Name** | Enter a mesh group name. This configures an MSDP mesh group and indicates that an MSDP peer belongs to that mesh group.<br>**Note** All MSDP peers present on a device that participate in a mesh group must be in a full mesh with all other MSDP peers in the group. Each MSDP peer on each device must be configured as a peer using the **ip msdp peer** command, and as a member of the mesh group using the **ip msdp mesh-group** command. |
| **Peer-IP** | Configure an MSDP peer specified by an IP address. |
| **Advanced Settings** | |
| **Connect-Source Interface** | Enter the primary address of a specified local interface that is used as the source IP address for the TCP connection. |
| **Peer Authentication Password** | Enables MD5 password encryption for a TCP connection between two MSDP peers.<br>**Note** MD5 authentication must be configured with the same password on both MSDP peers. Otherwise, a connection between them cannot be established. |

| Field | Description |
|---|---|
| **Keep Alive** | Configure an interval at which an MSDP peer will send keepalive messages. |
| **Hold-Time** | Configure an interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them as down. |
| **Remote AS** | Specifies the autonomous system number of the MSDP peer. This keyword and argument are used for display purposes only. |
| **SA Limit** | Limits the number of SA messages allowed in the SA cache from the specified MSDP. |
| **Default Peer** | Configure a default peer from which to accept all MSDP SA messages. |

## 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. |
| **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. |
| **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:<br>• Address<br>• AS Path List<br>• Community List<br>• Extended Community List<br>• BGP Local Preference<br>• Metric<br>• Next Hop<br>• OMP Tag<br>• OSPF Tag |
| **Action Type** | Specify the action type. The options are: Accept or Reject. |

| Field | Description |
|---|---|
| **Accept Condition** | Specify the accept condition type. The options are:<br>• AS Path<br>• Community<br>• Local Preference<br>• Metric<br>• Metric Type<br>• Next Hop<br>• OMP Tag<br>• Origin<br>• OSPF Tag<br>• 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. |
| **Condition** | Specify the ACL condition. The options are:<br>• DSCP<br>• Packet Length<br>• PLP<br>• Protocol<br>• Source Data Prefix<br>• Source Port<br>• Destination Data Prefix<br>• Destination Port<br>• TCP<br>• Class<br>• Peer |
| **Action Type** | Specify the action type. The options are: Accept or Reject. |

| Field | Description |
|---|---|
| **Accept Condition** | Specify the accept condition type. The options are:<br>• Counter<br>• DSCP<br>• Log<br>• Next Hop<br>• Mirror List<br>• Class<br>• 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. |
| **Condition** | Specify the ACL condition. The options are:<br>• Next Header<br>• Packet Length<br>• PLP<br>• Protocol<br>• Source Data Prefix<br>• Source Port<br>• Destination Data Prefix<br>• Destination Port<br>• TCP<br>• Class<br>• Traffic Class |
| **Action Type** | Specify the action type. The options are: Accept or Reject. |
| **Accept Condition** | Specify the accept condition type. The options are:<br>• Counter<br>• Log<br>• Next Hop<br>• Traffic Class<br>• Mirror List<br>• Class<br>• 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.

## AppQoE

Use the AppQoE feature to deploy and manage your SD-WAN network more efficiently by optimizing traffic based on sites and applications.

The following table describes the options for configuring the AppQoE feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Device AppQoE Role *** | |
| **Service Node** | Choose the **Service Node** option if you want to configure the device as a service node.<br>**Note** **Service Node** is the default option.<br>Choose both the **Service Node** and **Forwarder** options if you want to configure the device as an integrated service node. |
| **Forwarder:** | Choose **Forwarder** if you want to configure the device as a forwarder. The forwarder redirects traffic to other service nodes.<br>**Note** From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, an AppQoE cluster can either operate on IPv4 protocol or IPv6 protocol in the control plane.<br>• **Forwarder IP Address***: IP address of the device you've configured as a forwarder.<br>• **AppQoE Service VPN***: Choose the service VPN attached to the interface of the forwarder.<br>• **Service Node Group**: Click **Add Service Node Group** and enter the following details for the service node group:<br>  • **Group Name**: Select the AppQoe group name.<br>  • **Add Service Node**: Click **Add Service Node** and enter the IP address of the service nodes to enable the service controllers to communicate with the service nodes.<br>  Click the + icon to add up to 32 service nodes for the group. The starting value for the service node is SNG-APPQOE, following which, you can provide a value in the range SNG-APPQOE1 to SNG-APPQOE31. |

### Advanced

| Field | Description |
|---|---|
| **DRE Optimisation** | Enable DRE optimisation |
| **Resource Profile** | Choose **Global** to choose a profile size from the options available in the drop-down list.<br>Choose **Default**to apply the default DRE profile size for the device.<br>Choose **Device Specific** to enter a value for the profile. |

## VPN Interface GRE

Use the service VPN Interface GRE feature for all Cisco vEdge Cloud and Cisco vEdge router devices.

The following tables describe the options for configuring the service VPN Interface GRE feature.

### Basic Configuration

| Field | Description |
|---|---|
| **Interface Name (1..255)*** | Enter the name of the GRE interface, in the format **grenumber**. The value for **number** can be from 1 through 255. |
| **Interface Description** | Enter a description of the GRE interface. |

### Advanced

| Field | Description |
|---|---|
| **Shutdown** | Click **Off** to enable the interface. |
| **IP MTU** | Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv6 packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **TCP MSS** | Specify the maximum segment size (MSS) of the IPv4 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |

| Field | Description |
|---|---|
| **IPv6 TCP MSS** | Specify the maximum segment size (MSS) of the IPv6 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |

## IPSEC

Use the IPsec feature to configure IPsec tunnels on Cisco IOS XE Catalyst SD-WAN devices, used for Internet Key Exchange (IKE) sessions.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value is shown for parameters that have a default setting. |

The following tables describe the options for configuring the VPN Interface IPsec 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. |

### Basic Configuration

| Field | Description |
|---|---|
| **Interface Name** | Enter the name of the IPsec interface. |
| **Description** | Enter a description of the IPsec interface. |

| Field | Description |
|---|---|
| **Interface Address** | Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list. |
| **Mask** | Enter the subnet mask. |
| **Tunnel Source** | Enter the source of the IPsec interface:<br>• **IP Address**: Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.. This address is on the local router.<br>• **Interface**: Enter the physical interface that is the source of the IPsec tunnel. |
| **Tunnel Destination** | Enter the destination of the IPsec interface:<br>• **Address**: Enter the destination IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list. This address is on a remote device.<br>• **Application**: Choose an application from the drop-down list.<br>• None<br>• Sig |
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |
| **Clear-Dont-Fragment** | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. |
| **IP MTU** | Specify the maximum MTU size of packets on the interface.<br>Range: 576 through 1804<br>Default: 1500 bytes |

### Internet Key Exchange

| Field | Description |
|---|---|
| **IKE Version** | Enter 1 to choose IKEv1.<br>Enter 2 to choose IKEv2.<br>Default: IKEv1 |

| Field | Description |
|---|---|
| **IKE Integrity Protocol** | Choose one of the following modes for the exchange of keying information and setting up IKE security associations:<br>• **Main**: Establishes an IKE SA session before starting IPsec negotiations.<br>• **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties.<br>Default: Main mode |
| **IPsec Rekey Interval (Seconds)** | Specify the interval for refreshing IKE keys.<br>Range: 3600 through 1209600 seconds (1 hour through 14 days)<br>Default: 14400 seconds (4 hours) |
| **IKE Cipher Suite** | Specify the type of authentication and encryption to use during IKE key exchange.<br>Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2<br>Default: aes256-cbc-sha1 |
| **IKE Diffie-Hellman Group** | Specify the Diffie-Hellman group to use in IKE key exchanges.<br>Values: 2, 14, 15, 16, 19, 20, 21, 24<br>Default: 16 |
| **IKE ID for Local End Point** | If the remote IKE peer requires a local endpoint identifier, specify it.<br>Range: 1 through 64 characters<br>Default: Source IP address of the tunnel |
| **IKE ID for Remote End Point** | If the remote IKE peer requires a remote end point identifier, specify it.<br>Range: 1 through 64 characters<br>Default: Destination IP address of the tunnel<br>There is no default option if you have chosen IKEv2. |

### IPSEC

| Field | Description |
|---|---|
| **IPsec Rekey Interval** | Specify the interval for refreshing IKE keys.<br>Range: 3600 through 1209600 seconds (1 hour through 14 days)<br>Default: 3600 seconds |

| Field | Description |
|---|---|
| **IPsec Replay Window** | Specify the replay window size for the IPsec tunnel.<br>Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes<br>Default: 512 bytes |
| **IPsec Cipher Suite** | Specify the authentication and encryption to use on the IPsec tunnel.<br>Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1**<br>Default: **aes256-gcm** |
| **Perfect Forward Secrecy** | Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values:<br>• **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group<br>• **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group<br>• **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group<br>• **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group<br>• **none**: Disable PFS<br>Default: **group-16** |

### Advanced

| Field | Description |
|---|---|
| **Associated VPN** | Select a VPN from the drop-down list to associate with the IPsec tunnel. |
| **Tunnel Route Via** | Specify the tunnel route details to steer the application traffic through.<br>**Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route. |
| **DPD Interval** | Specify the interval for IKE to send Hello packets on the connection.<br>Range: 10 through 3600 seconds (1 hour)<br>Default: 10 seconds |
| **DPD Retries** | Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer.<br>Range: 2 through 60<br>Default: 3 |

| Field | Description |
|---|---|
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 through 1460 bytes<br>Default: None |
| **IP MTU** | Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface.<br>Range: 576 through 9216<br>Default: 1500 bytes |
| **Shutdown** | Click **Off** to enable the interface. |

## Tracker

Use the Tracker feature to track the status of the tracker endpoints.

The following tables describe the options for configuring the Tracker feature.

| Field | Description |
|---|---|
| **Tracker Name*** | Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.<br>From the drop-down list, choose **Global**. From the Tracker Type field drop-down list, choose a value to configure the endpoints. The default value is **static-route**. |
| **Endpoint** | Choose an endpoint type:<br>• **Endpoint IP**: When you choose the **Endpoint IP** option, the following field appears:<br>**Endpoint IP***: IP address of the endpoint. This IP address is the destination on the internet to which the probes are sent to determine the status of an endpoint.<br>• **Endpoint API URL**: When you choose the **Endpoint API URL** option, the following field appears:<br>**API URL of endpoint***: API URL for the endpoint of the tunnel. This URL is the destination on the internet to which probes are sent to determine the status of the endpoint.<br>• **Endpoint TCP/UDP**: When you choose the **Endpoint TCP/UDP** option, the following field appears:<br>**Endpoint IP***: IP address of the TCP/UDP static route endpoint. This IP address is the destination on the internet to which the probes are sent to determine the status of a TCP/UDP endpoint.<br>**Endpoint TCP/UDP***: Choose the TCP or UDP protocol to apply.<br>**Port**: Enter the TCP/UDP port. |

| Field | Description |
|---|---|
| **Interval** | Frequency at which a probe is sent to determine the status of the transport interface. Range: 20 through 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 through 10. Default: 3 |
| **Threshold** | Duration to wait for the probe to return a response before declaring that the transport interface is down. Range: 100 through 1000 milliseconds. Default: 300 milliseconds |

### Tracker Group

Use the Tracker Group feature to track the status of service interfaces.

**Note** Ensure that you have created two trackers to form a tracker group.

The following tables describe the options for configuring the Tracker Group feature.

| Field | Description |
|---|---|
| **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**.<br>**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.<br>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. |

### OSPFv3 IPv4 Routing

Use this feature to configure the Open Shortest Path First version 3 (OSPFv3) IPv4 link-state routing protocol for IPv4 unicast address families.

The following tables describe the options for configuring the OSPFv3 IPv4 Routing feature.

#### Basic Settings

| Field | Description |
|---|---|
| **Router ID** | Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address that is associated with the router for OSPF adjacencies. Default: No Router ID is configured. |
| **Add Redistribute** | |

| Field | Description |
|---|---|
| **Protocol** | Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions.<br>• **Connected**<br>• **Static**<br>• **Nat-route**<br>• **BGP** |
| **Select Route Policy** | Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF. |

### Area

| Field | Description |
|---|---|
| **Area Number*** | Enter the number of the OSPFv3 area.<br>Allowed value: Any 32-bit integer |
| **Area Type** | Choose the type of OSPFv3 area:<br>• **Stub**: No external routes<br>• **NSSA**: Not-so-stubby area, allows external routes<br>• **Normal**<br>**Note** You can't enter a value for **Area type** if you have entered 0 as a value for **Area Number**. |
| **Interface** | |
| **Add Interface** | Configure the properties of an interface in an OSPFv3 area. |
| **Name*** | Enter the name of the interface. Examples of interface names: GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1. |
| **Cost** | Specify a number for the Type 3 summary link-state advertisement (LSA). OSPFv3 uses this metric during its SPF calculation to determine the shortest path to a destination.<br>Range: 0 through 16777215 |
| **Authentication Type** | Specify the SPI and authentication key if you use IPSec SHA1 authentication type.<br>• **no-auth**: Select no authentication.<br>• **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication. |

| Field | Description |
|---|---|
| **SPI** | Specifies the Security Policy Index (SPI) value.<br>Range: 256 through 4294967295 |
| **Authentication Key** | Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long. |
| **Passive Interface** | Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol.<br>Default: Disabled |
| **IPv4 Range** | |
| **Add IPv4 Range** | Configure the area range of an interface in an OSPFv3 area. |
| **Network Address*** | Enter the IPv4 address. |
| **Subnet Mask*** | Enter the subnet mask. |
| **No Advertise*** | Enable this option to not advertise the Type 3 summary LSAs. |
| **Cost** | Specify the cost of the OSPFv3 interface.<br>Range: 1 through 65535 |

### Advanced

| Field | Description |
|---|---|
| **Route Policy** | Enter the name of a localized control policy to apply to routes coming from OSPFv3 neighbors. |
| **Reference Bandwidth (Mbps)** | Specify the reference bandwidth for the OSPFv3 autocost calculation for the interface.<br>Range: 1 through 4294967 Mbps<br>Default: 100 Mbps |
| **RFC 1583 Compatible** | By default, the OSPFv3 calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328. |

| Field | Description |
|---|---|
| **Originate** | Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear:<br>• **Always**: Enable this option to always advertise the default route in an OSPF routing domain.<br>• **Default Metric**: Set the metric used to generate the default route.<br>Range: 0 through 16777214<br>Default: 10<br>• **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route. |
| **Distance** | Define the OSPFv3 route administration distance based on route type.<br>Default: 100 |
| **Distance for External Routes** | Set the OSPFv3 distance for routes learned from other domains.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Inter-Area Routes** | Set the distance for routes coming from one area into another.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Intra-Area Routes** | Set the distance for routes within an area.<br>Range: 0 through 255<br>Default: 110 |
| **SPF Calculation Timers** | Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm. |
| **SPF Calculation Delay (milliseconds)** | Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 200 ms |
| **Initial Hold Time (milliseconds)** | Specify the amount of time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 1000 ms |
| **Maximum Hold Time (milliseconds)** | Specify the longest time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 10000 ms (10 seconds) |

| Field | Description |
|---|---|
| **Maximum Metric (Router LSA)** | Configure OSPFv3 to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation.<br>• **Immediately**: Force the maximum metric to take effect immediately, through operator intervention.<br>• **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up.<br>Range: 5 through 86400 seconds<br>Maximum metric is disabled by default. |

## OSPFv3 IPv6 Routing

Use this feature to configure the Open Shortest Path First version 3 (OSPFv3) IPv6 link-state routing protocol for IPv6 unicast address families.

The following tables describe the options for configuring the OSPFv3 IPv6 Routing feature.

### Basic Settings

| Field | Description |
|---|---|
| **Router ID** | Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address that is associated with the router for OSPF adjacencies. Default: No Router ID is configured. |
| **Add Redistribute** | |
| **Protocol** | Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions.<br>• **Connected**<br>• **Static**<br>• **BGP** |
| **Select Route Policy** | Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF. |

### Area

| Field | Description |
|---|---|
| **Area Number*** | Enter the number of the OSPFv3 area.<br>Allowed value: Any 32-bit integer |

| Field | Description |
|---|---|
| **Area Type** | Choose the type of OSPFv3 area:<br>• **Stub**: No external routes<br>• **NSSA**: Not-so-stubby area, allows external routes<br>• **Normal**<br>**Note** You can't enter a value for **Area type** if you have entered 0 as a value for **Area Number**. |
| **Interface** | |
| **Add Interface** | Configure the properties of an interface in an OSPFv3 area. |
| **Name*** | Enter the name of the interface. Examples of interface names: GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1. |
| **Cost** | Specify a number for the Type 3 summary link-state advertisement (LSA). OSPFv3 uses this metric during its SPF calculation to determine the shortest path to a destination.<br>Range: 0 through 16777215 |
| **Authentication Type** | Specify the SPI and authentication key if you use IPSec SHA1.<br>• **no-auth**: Select no authentication.<br>• **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication. |
| **SPI** | Specifies the Security Policy Index (SPI) value.<br>Range: 256 through 4294967295 |
| **Authentication Key** | Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long. |
| **Passive Interface** | Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol.<br>Default: Disabled |
| **IPv6 Range** | |
| **Add IPv6 Range** | Configure the area range of an interface in an OSPFv3 area. |
| **Network Address*** | Enter the IPv6 address. |
| **Subnet Mask*** | Enter the subnet mask. |
| **No Advertise*** | Enable this option to not advertise the Type 3 summary LSAs. |

| Field | Description |
|---|---|
| **Cost** | Specify the cost of the OSPFv3 interface.<br>Range: 1 through 65535 |

**Advanced**

| Field | Description |
|---|---|
| **Route Policy** | Enter the name of a localized control policy to apply to routes coming from OSPFv3 neighbors. |
| **Reference Bandwidth (Mbps)** | Specify the reference bandwidth for the OSPFv3 autocost calculation for the interface.<br>Range: 1 through 4294967 Mbps<br>Default: 100 Mbps |
| **RFC 1583 Compatible** | By default, the OSPFv3 calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328. |
| **Originate** | Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear:<br>• **Always**: Enable this option to always advertise the default route in an OSPF routing domain.<br>• **Default Metric**: Set the metric used to generate the default route.<br>Range: 0 through 16777214<br>Default: 10<br>• **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route. |
| **Distance** | Define the OSPFv3 route administration distance based on route type.<br>Default: 100 |
| **Distance for External Routes** | Set the OSPFv3 distance for routes learned from other domains.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Inter-Area Routes** | Set the distance for routes coming from one area into another.<br>Range: 0 through 255<br>Default: 110 |
| **Distance for Intra-Area Routes** | Set the distance for routes within an area.<br>Range: 0 through 255<br>Default: 110 |

| Field | Description |
|---|---|
| **SPF Calculation Timers** | Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm. |
| **SPF Calculation Delay (milliseconds)** | Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 200 ms |
| **Initial Hold Time (milliseconds)** | Specify the amount of time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 1000 ms |
| **Maximum Hold Time (milliseconds)** | Specify the longest time between consecutive SPF calculations.<br>Range: 1 through 600000 ms (600 seconds)<br>Default: 10000 ms (10 seconds) |
| **Maximum Metric (Router LSA)** | Configure OSPFv3 to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation.<br>• **Immediately**: Force the maximum metric to take effect immediately, through operator intervention.<br>• **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up.<br>Range: 5 through 86400 seconds<br>Maximum metric is disabled by default. |

## EIGRP Routing

Use the EIGRP routing feature to configure a routing process and specify which networks the protocol should run over.

### Basic Configuration

| Parameter Name | Description |
|---|---|
| Autonomous System ID * | Enter the local autonomous system (AS) number.<br>Range: 1 through 65535<br>Default: None |
| **Network** | |
| IP Address* | Enter the IPv4 address. |
| Mask* | Enter the subnet mask. |

| Parameter Name | Description |
|---|---|
| **Interface** | |
| Add Interface | Provide values for the following fields:<br>• **AF Interface**: Enter a value for the Address Family (AF) interface.<br>• **Shutdown**: Enables the interface to run EIGRP by default.<br>Toggle ON to disable the interface.<br>• **Add Summary Address**: Enter an IPv4 address and choose a subnet mask. |

### IPv4 Unicast Address Family

| Parameter Name | Description |
|---|---|
| Protocol * | Select one of the protocols from which to redistribute routes into EIGRP, for all EIGRP sessions:<br>• **bgp**: Redistribute Border Gateway Protocol (BGP) routes into EIGRP.<br>• **connected**: Redistribute connected routes into EIGRP.<br>• **nat-route**: Redistribute network address translation (NAT) routes into EIGRP.<br>• **omp**: Redistribute Overlay Management Protocol (OMP) routes into EIGRP.<br>• **ospf**: Redistribute Open Shortest Path First (OSPF) routes into EIGRP.<br>**Note** From Cisco IOS XE Catalyst SD-WAN Release 16.12.1b and later, you can set metric values for redistribution by using the CLI add-on feature template. Use the following command:<br>`redistribute ospf 1 metric 1000000 1 1 1 1500`<br>For more information, see CLI Add-on Feature Templates.<br>• **ospfv3**: OSPFv3 routes into EIGRP.<br>• **static**: Redistribute static routes into EIGRP. |
| Route Policy * | Enter the name of the route policy to apply to redistributed routes. |

### Authentication

| Parameter | Description |
|---|---|
| MD5* | **MD5 Key ID**: Enter an MD5 key ID to compute an MD5 hash over the contents of the EIGRP packet using that value. |
| | **MD5 Authentication Key**: Enter an MD5 authentication key to use an encoded MD5 checksum in the transmitted packet. |
| | **Authentication Key**: A 256-byte unique key that is used to compute the Hashed Message Authentication Code (HMAC) and is known both by the sender and the receiver of the message. |
| HMAC-SHA-256 | **Authentication Key**: A 256-byte unique key that is used to compute the HMAC and is known both by the sender and the receiver of the message. |

### Advanced

| Parameter Name | Description |
|---|---|
| Hold Time (seconds) | Set the interval after which EIGRP considers a neighbor to be down. The local router then terminates the EIGRP session to that peer. This acts as the global hold time.<br>Range: 0 through 65535<br>Default: 15 seconds |
| Hello Interval (seconds) | Set the interval at which the router sends EIGRP hello packets.<br>Range: 0 through 65535<br>Default: 5 seconds |
| Route Policy | Enter the name of an EIGRP route policy. |
| Filter | Toggle **ON** to filter routes that do not match the policy. |

## Object Tracker

Use the object tracker feature to configure an object tracker.

### Basic Settings

| Parameter Name | Description |
|---|---|
| **Tracker Type*** | |

| Parameter Name | Description |
|---|---|
| Interface | Configure the following interface values:<br>• **Object tracker ID***: Enter the object tracker ID number.<br>Range: 1-1000<br>• **Interface name***: Enter the global or device-specific tracker interface name. For example, Gigabitethernet1 or Gigabitethernet2. |
| SIG | **Object tracker ID***: Enter the object tracker ID number. |
| Route | Configure the route details:<br>• **Object tracker ID***: Enter the object tracker ID number.<br>Range: 1-1000<br>• **Route IP***: Enter the IPv4 address of the route.<br>• **Route IP Mask***: Select a value for the subnet mask.<br>• **VPN**: Enter a value for the VPN. |

### Object Tracker Group

Use this feature to configure an object tracker group. To ensure accurate tracking, add at least two object trackers before creating an object tracker group.

#### Basic Settings

| Parameter Name | Description |
|---|---|
| Object tracker ID * | Enter an ID for the object tracker group.<br>Range: 1 through 1000 |
| Object tracker * | Select a minimum of two previously created object trackers from the drop-down list. |
| Reachable * | Choose one of the following values:<br>• **Either**: 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.<br>• **Both**: Ensures that the transport interface status is reported as active if both the associated trackers of the tracker group report that the route is active. |

## Security Profile

Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

The following sections describe how to configure a security profile.

### 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:<br>• **Name**: Enter a name for the profile.<br>• **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. |

| Field | Description |
|---|---|
| **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:<br>• NAT<br>• Database URL<br>• Resource Profile: Choose a resource profile priority option:<br>• **Low**<br>• **Medium**<br>• **High**<br>**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

Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

The following sections describe how to configure a policy object profile.

## 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. |
| **Create new** | When you choose this option, the following fields appear:<br>• **Name**: Enter a name for the profile.<br>• **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. |

| Field | Description |
|---|---|
| **Add Standard Community** | Specify the standard community. the options are:<br>• *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.<br>• **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices.<br>• **local-as**: Routes in this community are not advertised outside the local AS number.<br>• **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.<br>• **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:<br>• **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.<br>• **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. |
| **Burst (bytes)** | Specify the maximum traffic burst size. Range is from 15000 to 10000000. |

| Field | Description |
|---|---|
| **Exceed** | Specify an action to take when the burst size or traffic rate is exceeded. The options are:<br>**Drop**—Sets the packet loss priority (PLP) to low.<br>**Remark**—Sets the PLP to high.<br>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. |

## Other Profile

### ThousandEyes

Cisco ThousandEyes is a SaaS application that provides you an end-to-end view across networks and services that impact your business. It monitors the network traffic paths across internal, external, and carrier networks and the internet in real time to provide network performance data. Cisco ThousandEyes provides intelligent insights into your WAN and the cloud and helps you optimize application delivery and end-user experience.

For each parameter of the feature 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 to the left of the parameter field and choose one of 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. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template.<br>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 Catalyst SD-WAN device to a device template.<br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

The following table describes the options for configuring the ThousandEyes 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. |
| **Account Group Token** | Enter the Cisco ThousandEyes Account Group Token. |
| **VPN** | Transport or service VPN. The **Default** setting indicates transport VPN (VPN 0). The **Global** or the **Device Specific** setting indicates service VPN.<br>When you set the VPN configuration as a **Global** or a **Device Specific** setting, enter the ID of the service VPN in which you want to provision the Cisco ThousandEyes Enterprise agent. |
| **Management IP** | Enter an IP address for the Cisco ThousandEyes Enterprise agent. This field is available only when you specify the service VPN. |

| Field | Description |
|---|---|
| **Management Subnet** | Choose a subnet mask from the drop-down list for the Cisco ThousandEyes Enterprise agent. This field is available only when you specify the service VPN.<br>**Note** This IP-prefix address (**Management IP** and **Management Subnet**) must be unique within the fabric and must 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. This field is available only when you specify the service VPN. |
| **Name Server IP** | Enter the IP address of your preferred DNS server.<br>This server can exist within or outside the Cisco Catalyst SD-WAN fabric but must be reachable from the service VPN. |
| **Host Name** | Enter the hostname that the agent must use when registering with the Cisco ThousandEyes portal. By default, the agent uses the hostname of the Cisco IOS XE Catalyst SD-WAN device. |
| **Proxy Type** | If the Cisco ThousandEyes Enterprise agent must use proxy server for external access, choose one of the following as proxy type:<br>• **static**<br>• **pac**<br>• **none**<br>Static proxy settings:<br>• **Proxy Host**: Set the configuration as a **Global** setting and enter the hostname of the proxy server.<br>• **Proxy Port**: Set the configuration as a **Global** setting and enter the port number of the proxy server.<br>PAC settings:<br>• **PAC URL**: Set the configuration as a **Global** setting and enter the URL of the proxy auto-configuration (PAC) file. |

## UCSE

Use the UCSE feature to connect a UCS-E interface with a UCS-E server.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

| Parameter Scope | Scope Description |
|---|---|
| **Global** (Indicated by a globe icon) | Enter a value for the parameter and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

| Parameter Scope | Scope Description |
|---|---|
| **Device Specific** (Indicated by a host icon) | Use a device-specific value for the parameter.<br>Choose **Device Specific** to provide a value for the key in the **Enter Key** field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the **Enter Key** field.<br>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID. |
| **Default** (indicated by a check mark) | The default value is shown for parameters that have a default setting. |

The following tables describe the options for configuring the UCSE feature.

| Field | Description |
|---|---|
| **Type** | Choose a feature from the drop-down list. |
| **Feature Name*** | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| **Description** | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |

### Basic Configuration

| Field | Description |
|---|---|
| **Bay*** | Specify the number for the SAS drive bays. The input value must be an integer. |
| **Slot*** | Specify the slot numbers for the mezzanine adapters. The input value must be an integer. |

### IMC

| Field | Description |
|---|---|
| **Access Port** | Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN.<br>Not all hardware models have a dedicated access port. See the release notes for your Cisco Catalyst SD-WAN release for the supported hardware.<br>Available options:<br>• **Dedicated**<br>• **Shared**<br>Configure the appropriate port (GE or TE) based on the hardware module. |
| **IPv4 Address*** | Provide the UCS-E management port address. |

| Field | Description |
|---|---|
| **Default Gateway*** | Gateway tracking determine, for static routes, whether the next hop is reachable before adding that route to the device's route table.<br>Default: Enabled. |
| **VLAN ID** | Provide the VLAN number, which can be a value from 1 through 4094. |
| **Assign Priority** | Assign the priority. |

**Advanced**

| Field | Description |
|---|---|
| **Interface Name*** | Specify the name of the interface. |
| **Layer** | Specify the layer details necessary for traffic exchange between different VLANs. |
| **UCSE Interface VPN** | Specify the details of the UCS-E interface VPN. |
| **IPv4 Address** | Provide the UCS-E management port address. |

# CLI Profile

The CLI feature profile enables you to specify device configuration in CLI format.

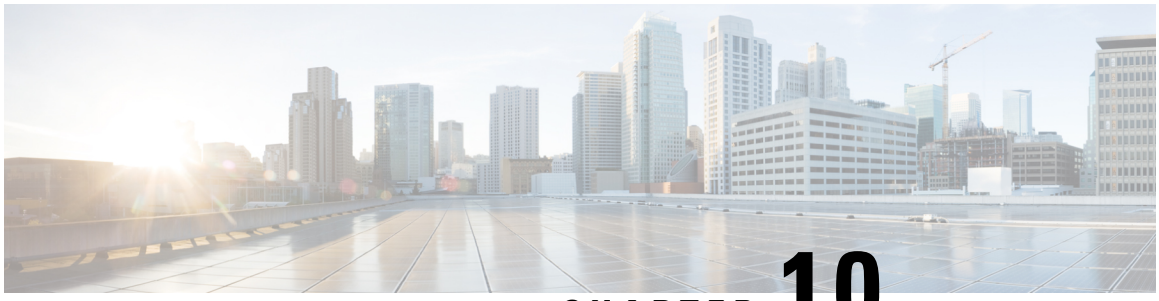
| Field | Description |
|---|---|
| **Choose existing** | Choose an existing profile from the **Profiles** table. |
| **Create new** | When you choose this option, the following fields appear:<br>• **Name**: Enter a name for the profile.<br>• **Description**: Enter a description of the profile. The description can contain any characters and spaces. |

To create or update a CLI add-on profile, you must have appropriate permission for the CLI Add-On Template feature. For more information on different permission settings, see Manage Users.

You can add the route-target CLIs through the CLI add-on profile:

```
vrf definition Mgmt-intf
address-family ipv4
route-target export 119:512
route-target import 119:512
```

You can type the configuration manually in the CLI configuration window, or copy and paste the CLI configuration. To save the configuration, click **Save**.



CHAPTER 10

# Device Tagging

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 69: Feature History*

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


- Information About Device Tagging, on page 454
- Supported Devices for Device Tagging, on page 454
- Prerequisites for Device Tagging, on page 454
- Restrictions for Device Tagging, on page 454

• Add Tags to Devices Using Cisco SD-WAN Manager, on page 455
• Delete Tags, on page 455

# Information About Device Tagging

The Device Tagging feature helps you do the following:

- Add tags to devices: Tagging helps you manage devices more effectively. You can use the tags for grouping, describing, or finding devices. You can add more than one tag to a device.
- Add devices to configuration groups based on tagging: Using tags, you can create rules to define which devices need to be automatically added to a configuration group. For complete information about creating rules, see Add Devices to a Configuration Group Using Rules.

**Note** You can use this feature in both the single-tenant and multitenant deployments.

# Supported Devices for Device Tagging

This feature is supported only on Cisco IOS XE Catalyst SD-WAN devices.

# Prerequisites for Device Tagging

Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Minimum software version for Cisco SD-WAN Manager: Cisco vManage Release 20.8.1

# Restrictions for Device Tagging

- (Cisco vManage Release 20.11.1 and earlier) You can create a maximum of 25 tags in a Cisco SD-WAN Manager instance.
- (Cisco vManage Release 20.11.1 and earlier) You can add a maximum of 25 tags per device.
- (Cisco vManage Release 20.11.1 and earlier) The tag name can be up to 25 characters and can contain only alphanumeric characters, hyphens (–), and underscores (_).
- The tag name cannot contain space or any other special characters.
- The tag name is case-sensitive.
- (Cisco vManage Release 20.11.1 and earlier) You can add only one tag rule to a configuration group.

# Add Tags to Devices Using Cisco SD-WAN Manager

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.

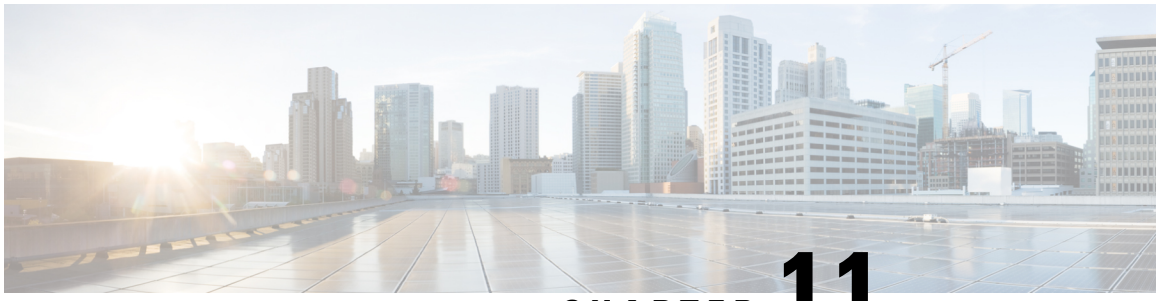
   The specified tag is added to the device.

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

# Delete Tags

You can delete only those tags that are not added to a device or are not a part of a tag rule.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Tag Management**.
2. Choose the tags that you want to delete.
3. Click **Delete Tags**.
4. In the confirmation dialog box, click **Yes**.



CHAPTER 11

# Network Hierarchy and Resource Management

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 70: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Network Hierarchy and Resource Management | Cisco IOS XE Catalyst SD-WAN Release 17.9.1a<br>Cisco vManage Release 20.9.1 | This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco Catalyst SD-WAN.<br>Note that you can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager. |

| Feature Name | Release Information | Description |
|---|---|---|
| Network Hierarchy and Resource Management (Phase II) | Cisco IOS XE Catalyst SD-WAN Release 17.10.1a<br>Cisco vManage Release 20.10.1 | The following enhancements are introduced in the Network Hierarchy and Resource Management feature.<br>• Creation of a system IP pool on the **Configuration** > **Network Hierarchy** page<br>• Automatic assignment of site ID, system IP, and hostname to a device in the Quick Connect workflow<br>• Display of detailed information on the **Configuration** > **Network Hierarchy** page, including site ID pool, region ID pool, and the list of devices associated with a site |
| Support for Software Defined Remote Access Pools | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>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.<br>You can create a software defined remote access pool using the **Configuration** > **Network Hierarchy** page. |
| Support for Traffic Flow Collectors | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a<br>Cisco Catalyst SD-WAN Manager Release 20.13.1 | This feature enables you to configure traffic flow collectors such as the Cflowd server and security logging server. Cflowd monitors service side traffic flowing through devices in the overlay network and exports flow information to the collector. Enable security logging and configure servers for high-speed logging (HSL) and collecting external syslogs.<br>You can configure the traffic flow collectors by navigating to **Configuration** > **Network Hierarchy** > **Collectors**. |


- Information About Network Hierarchy and Resource Management, on page 458
- Supported Devices for Network Hierarchy and Resource Management, on page 459
- Restrictions for Network Hierarchy and Resource Management, on page 460
- Manage a Network Hierarchy, on page 460
- Assign Resource IDs to Devices, on page 467
- Configure Collectors in a Network Hierarchy, on page 470


# Information About Network Hierarchy and Resource Management

### Overview of Network Hierarchy

You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. Your network hierarchy can contain three types of nodes—regions, areas, and sites. The resource IDs assigned to the nodes help you identify where to apply configuration settings later.

By default, there is one node called global in the network hierarchy.

The network hierarchy has a predetermined hierarchy with three types of nodes:

- Region: It represents a region in a multiregion fabric-based Cisco Catalyst SD-WAN deployment. The Multi-Region Fabric feature provides the option to divide the architecture of the Cisco Catalyst SD-WAN overlay network into multiple regional networks that operate distinctly from one another, and a central core-region network for managing inter-regional traffic.

  You can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager. For complete information about the Multi-Region Fabric feature, see the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*.

- Group/Area: A group, also called an area, is a logical grouping of nodes in a network hierarchy. You can group sites, regions, other areas, or any combination of these into an area.

- Site: A site is the lowest level of node or the leaf node in a network hierarchy. You cannot create a child node under a site. You can only associate devices to a site.

For complete information about creating and managing different nodes in a network hierarchy, see Manage a Network Hierarchy.

### Overview of Resource Management

The resource manager in Cisco SD-WAN Manager manages the resource IDs, that is, region IDs and site IDs. It automatically generates a region ID for a region that you create on the **Configuration** > **Network Hierarchy** page. Similarly, it generates a site ID for a site if you do not specify it.

You can assign a site ID and a region ID to a device. For complete information about assigning resource IDs to devices, see Assign Resource IDs to Devices.

If you upgrade from an earlier version of Cisco SD-WAN Manager to Cisco vManage Release 20.9.1, the resource manager in Cisco SD-WAN Manager automatically creates sites based on the site IDs of the existing devices in your setup. Sites are named as SITE_<*id*>. Cisco SD-WAN Manager displays these sites under the global node on the **Network Hierarchy** page. It also associates the existing devices with their sites in the network hierarchy.

## Benefits of Network Hierarchy and Resource Management

- Automates the management of regions and sites.
- Saves the manual effort in an upgrade scenario when Cisco SD-WAN Manager discovers all your existing sites and displays them in the network hierarchy.
- Simplifies the onboarding and configuration of devices.
- Monitors and collects information about traffic flow.

# Supported Devices for Network Hierarchy and Resource Management

This feature is supported on Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices.

# Restrictions for Network Hierarchy and Resource Management

- You can delete a node only if it does not have any child node. For example, you can delete a site only if no devices are associated with it.
- A site is the lowest level of a node or the leaf node in a network hierarchy. You cannot create a child node under a site.
- You cannot create more than one region node between the global node and a site node.
- You cannot create a region in a multitenant deployment.
- The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

# Manage a Network Hierarchy

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

(For Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier) Ensure that the **Multi-Region Fabric** option in Cisco SD-WAN Manager is enabled. See Enable Multi-Region Fabric in the *Cisco Catalyst SD-WAN Multi-Region Fabric Configuration Guide*.

From Cisco Catalyst SD-WAN Manager Release 20.13.1, configuring regions is enabled by default. It does not require enabling Multi-Region Fabric.

### Create a Region, Cisco Catalyst SD-WAN Manager Release 20.13.1 and Later

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to **Global** in the left pane and choose **Add Node**.
3. Do one of the following:
   - If Multi-Region Fabric is not enabled:

     In the **Add Node** pop-up window, check the **Behave as SDWAN Region** checkbox.

     If you do not check this checkbox, this procedure creates a new group within the network hierarchy instead of a region.
   - If Multi-Region Fabric is enabled:

In the **Add Node** pop-up window, choose **Region**.

4. Configure the following:

| Field | Description |
|---|---|
| **Name** | Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). |
| **Description** | Description of the region. |
| **Parent** drop-down list | Choose a parent node. |

5. Click **Add**.

   The new region appears in the left pane.

6. (Optional) You can click a region name or a secondary region name in the left pane to display the automatically assigned region ID number. The region ID number appears above the table in the right pane. The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

### Create a Region, Cisco Catalyst SD-WAN Manager Release 20.12.x or Earlier

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 a Subregion in a Network Hierarchy

### Before You Begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

- From Cisco Catalyst SD-WAN Manager Release 20.13.1, configuring subregions is enabled by default. It does not require enabling Multi-Region Fabric.
- Create a region before creating a subregion. See Create a Region in a Network Hierarchy, on page 460.

- For the maximum combined number of regions and secondary regions, see Restrictions for Network Hierarchy and Resource Management, on page 460.

### Create a Subregion

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a region in the left pane and choose **Add MRF Sub Region**.
3. In the **Add Sub-Region** pop-up window, configure the following:

| Field | Description |
|---|---|
| **Name** | Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). |
| **Description** | Description of the region. |
| **Parent** | This field is automatically populated with the region to which you are adding the subregion, and is not configurable. |

4. Click **Add**.

   The new subregion appears in the left pane.

# Create a Secondary Region in a Network Hierarchy

### Before You Begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

- Create a region before creating a subregion. See Create a Region in a Network Hierarchy, on page 460.
- For the maximum combined number of regions and secondary regions, see Restrictions for Network Hierarchy and Resource Management, on page 460.

### Create a Secondary Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to **Global** in the left pane and choose **Add Node**.
3. In the **Add Node** pop-up window, click **Secondary Region**.
4. Configure the following:

| Field | Description |
|---|---|
| **Name** | Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). |
| **Description** | Description of the region. |

| Field | Description |
|---|---|
| **Parent** | This field shows **Secondary Regions**, and is not configurable. |

5. Click **Add**.

   The new secondary region appears in the left pane, in the **Secondary Regions** section.

6. (Optional) You can click a region name or a secondary region name in the left pane to display the automatically assigned region ID number. The region ID number appears above the table in the right pane. The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

# Create a Group in a Network Hierarchy

### Before You Begin

In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, a group is called an area.

### Create a Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global, region, or group) in the left pane and choose **Add Group**.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, 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 group. 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 group.
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**.

# Edit a Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the region name and choose **Edit MRF Region**.
3. Edit the options as needed. You can edit the name, description, and parent of the region.
4. Click **Save**.

# Delete a Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the region name and choose **Delete MRF Region**.
3. In the confirmation dialog box, click **Yes**.

# Edit a Group

### Before You Begin

In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, a group is called an area.

### Edit a Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the group name and choose **Edit Group**.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, choose **Edit Area**.
3. Edit the options as needed. You can edit the name, description, and parent of the group.
4. Click **Save**.

# Delete a Group

### Before You Begin

In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, a group is called an area.

### Delete a Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the group name and choose **Delete Group**.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, choose **Delete Area**.
3. In the confirmation dialog box, click **Yes**.

## Edit a Site

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the site name and choose **Edit Site**.
3. Edit the options as needed. You can edit only the name, description, and parent of the site.
4. Click **Save**.

## Delete a Site

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the site name and choose **Delete Site**.
3. In the confirmation dialog box, click **Yes**.

## 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.

# Edit 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. The system IP pool is also displayed if you have already created it.

2. Click **…** adjacent to the system IP name and choose **Edit**.
3. Edit the options as needed.

**Note** You can only expand the pool range and cannot enter a lower IP address than the already specified IP address.

4. Click **Save**.

# Create a Remote Access Pool

Minimum supported release: Cisco vManage Release 20.11.1

The resource pool manager supports creation of IPv4 and IPv6 private IP pools for Cisco Catalyst SD-WAN remote access devices. In the remote access configuration you can select the remote access private IP Pool by defining the number of IP addresses.

For more information on Software Defined Remote Access, see Cisco Catalyst SD-WAN Remote Access.

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 Pool**.
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 **Remote Access**.
6. Choose the **IP Type** by clicking the radio button next to **IPv4** or **IPv6**.
7. In the **IP Subnet** field, enter an IP subnet.
8. In the **Prefix Length** field, enter the prefix length of the remote access pool.
9. Click **Add**.

# Edit a Remote Access Pool

Minimum supported release: Cisco vManage Release 20.11.1

You can edit a remote access pool only when you want to expand the pool range.

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. The remote access pool is also displayed if you have already created it.

2. Click **…** adjacent to the remote access pool name and choose **Edit**.
3. Edit the options as needed.

**Note** When you edit a remote access pool, the new pool range cannot be less than the existing pool range

4. Click **Save**.

## Delete a Pool

Minimum supported release: Cisco vManage Release 20.11.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Network Hierarchy**.
2. In the Global page, click **…** adjacent to the pool name and choose **Delete**.
3. In the confirmation dialog box, click **Yes**.

**Note** You can delete a pool only when the pool resources are not in use.

# Assign Resource IDs to Devices

The Network Hierarchy and Resource Management feature enables you to do the following:

- Assign a site ID to a device
- Assign a region ID to a device

## 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**.

# Configure Collectors in a Network Hierarchy

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

Configure Cflowd and security logging servers that help monitor traffic flow and collect information about service-side traffic.

## Information About Collectors

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

Collectors process traffic flowing through routers in the overlay network and export flow information to a server. The collectors maintain information about the flow and data that is extracted from the IP headers of the packets in the traffic flow.

You can configure the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the samples are sent to the collectors (on Cisco SD-WAN Controllers only). You can configure a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN Device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

## Configure Cflowd

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

### Before You Begin

You can configure the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the samples are sent to the collectors (on Cisco SD-WAN Controllers only). You can configure

a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

Ensure that you specify the granular role-based access control (RBAC) for Cflowd and policy groups. With specific permissions to the user group, ensure that you are able to access policy groups from **Configuration** > **Policy Groups**. For more information about configuring RBAC for policy groups, see Configure RBAC for policy groups in Prerequisites for Policy Groups.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.
2. Click **Edit** next to existing roles or click **Add Role** to create a new role.
3. Choose the desired permission for the **Cflowd** feature under **Network Settings** and click **Update**.

### Configure Cflowd

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.
2. Enable Cflowd and configure the values in the following table for the collector server:

| Field | Description |
|---|---|
| **Add Collector Server** | |
| **VPN ID** | VPN ID of the server.<br>Range: 0 through 65536 |
| **IPv4/IPv6 Address** | IPv4 or IPv6 address of the collector server. |
| **UDP Port** | UDP port number of the collector server.<br>Range: 1024 through 65535 |
| **Export Spreading** | Toggle to enable or disable the export spreading configuration. |
| **BFD Metrics Exporting** | Toggle to enable or disable Bidirectional Forwarding Detection (BFD) metrics. |
| **Exporting Interval** | Interval in seconds for sending BFD metrics.<br>**Exporting Interval** appears if you have enabled **BFD Metrics Exporting**.<br>The default BFD export interval is 600 seconds. |
| **Advanced Settings** | |
| **Active Flow Timeout (Seconds)** | Active flow timeout value.<br>Range: 30 through 3600<br>Default: 600 seconds. |
| **Inactive Flow Timeout (Seconds)** | Inactive flow timeout value.<br>Range: 1 through 3600<br>Default: 60 seconds. |

| Field | Description |
|---|---|
| **Flow Refresh Time (Seconds)** | Flow refresh time in seconds.<br>Range: 60 through 86400 seconds.<br>Default: 600 seconds. |
| **Sampling Rate** | Sample duration in seconds.<br>Range: 1 through 65536.<br>Default: 1 second. |
| **Collect TLOC Loopback** | Enable to collect information about the TLOC loopback. |
| **Protocol** | Traffic protocol type to apply the collector to. The options are: **IPv4**, **IPv6**, or **both**.<br>The default protocol is **IPv4**. |
| **TOS** | Type of field in the IPv4 header. |
| **Re-marked DSCP** | Traffic output of the router's data policy. |

You can configure up to four collector servers.

3. Click **Save**.

The Cflowd settings that you configure are applied to the application priority and SLA policy when the policy is deployed to Cisco Catalyst SD-WAN devices. You can monitor application traffic flow over IPv4, IPv6, or both network addresses. For more information about configuring additional settings, see **Monitor traffic flow** in Application Priority and SLA.

# Configure Security Logging

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

### Configure Security Logging

You can set up security logging for Cisco IOS XE Catalyst SD-WAN devices by configuring the location of the destination IP address of the log server. You can configure up to four destination servers along with the source interface to collect the syslogs for High Speed Logging (HSL). The IP address for the destination server can be IPv4, IPv6, or both. For more information about configuring HSL, see Configure Firewall High-Speed Logging Using the CLI Template. You can configure the external syslog server to export UTD logs. For more information about UTD logging, see Create Unified Security Policy Summary page.

### Before You Begin

Ensure that you specify the granular role-based access control (RBAC) for security logging. Ensure that you are able to access policy groups from **Configuration** > **Policy Groups** by configuring specific permissions to the user group. For more information about configuring RBAC for policy groups, see "Configure RBAC for policy groups" in Prerequisites for Policy Groups.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.

2. Click **Edit** adjacent to existing roles or click **Add Role** to create a new role.
3. Choose the permission you wish to configure for the **Security Logging** feature under **Network Settings** and click **Update**.

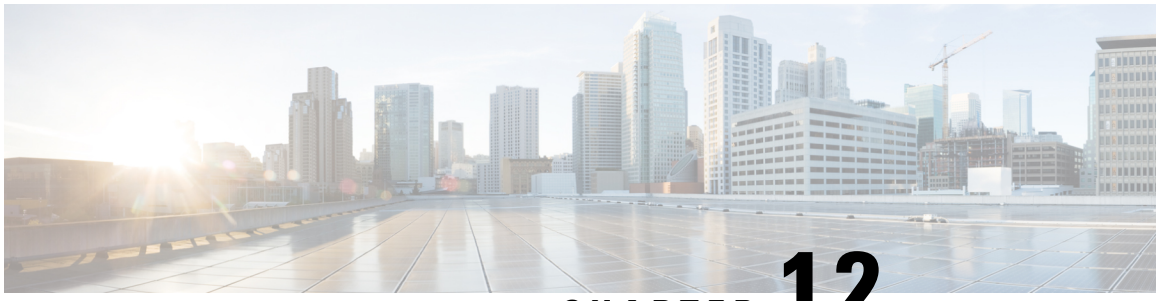
### Configure Security Logging

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.
2. Enable **Security Logging** and configure the values in the following table for the high-speed logging and external syslog servers:

| Field | Description |
|---|---|
| **High Speed Logging** | Configure the following values for the high speed logging server:<br>• **VPN**: VPN name of the high speed logging server.<br>The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager.<br>• **Server IP**: IPv4 or IPv6 address of the log collector server.<br>• **Port**: Port number on which the log collector server is listening for incoming packets. |
| **External Syslog Server** | Configure the following values for the external syslog server:<br>• **VPN**: VPN name of the external syslog server.<br>The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager.<br>• **Server IP**: IPv4 or IPv6 address of the external syslog server. |

   You can configure up to four high speed logging servers.
3. Click **Save**.

The security logging settings that you configure are applied along with the embedded security policy when the policy is deployed to Cisco Catalyst SD-WAN devices. For more information about configuring the embedded security policy, see Configure Embedded Security.



CHAPTER 12

# Cisco Unified Communications Voice Services

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 71: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Integration with Cisco Unified Communications | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | This release adds support for using a feature template to enable Cisco IP-based media services. |
| | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | This feature lets you use feature templates and voice policies to enable Cisco Unified Communications (UC) voice services for supported routers. When Cisco UC voice services are enabled, routers can process calls for various endpoints, including voice ports, POTS dial peers, SIP dial peers, and phone profiles in Cisco Unified SRST mode.<br>You can configure items for UC voice services from the Feature tab and the Voice Policy page for a supported device.<br>Configuring UC voice services for Cisco Unified Communications requires that Cisco SD-WAN Manager runs Cisco Catalyst SD-WAN Release 20.1.1.<br>This feature is supported on Cisco 4000 Series Integrated Services Routers. |
| Cisco Unified Communications Voice Services Configuration through the Workflow Library and Configuration Groups | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a<br>Cisco Catalyst SD-WAN Manager Release 20.13.1 | With this release, you can configure DSP farms for UC voice services by using the Workflow Library and configuration groups |

You can configure feature templates and voice policies to enable Cisco Unified Communications (UC) voice services for supported routers. These templates and policies configure parameters for FXO, FXS, and FXS/DID interfaces on these routers. Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, parameters for PRI ISDN too can be configured. In addition, you can use the DSPFarm feature template to enable Cisco IP-based media services.

When Cisco UC voice services are enabled, routers can process calls for various endpoints, including voice ports for analog interfaces and digital interfaces, POTS dial peers, SIP dial peers, and phone profiles in Cisco Unified SRST mode.

**Note** Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, you also can configure and enable UC voice services by using the Workflow library or configuration groups. See Configure UC Voice Services using the Workflow Library or Configuration Groups.

Configuring UC voice services for Cisco Unified Communications requires that Cisco SD-WAN Manager runs Cisco Catalyst SD-WAN Release 20.3 or later.

For more detailed information about commands to configure and maintain Cisco IOS voice applications, see Cisco IOS Master Command List.

The following describe the general steps that you perform to configure, in various scenarios, voice services for Cisco Unified Communications:

- Workflow for initial configuration of Cisco Catalyst SD-WAN for Cisco Unified Communications.

| | |
|---|---|
| Step 1 | Add a voice card feature template. |
| Step 2 | Add a call routing feature template. |
| Step 3 | (Optional) Add an SRST feature template. |
| Step 4 | (Optional) Add a DSPFarm Feature Template. |
| Step 5 | (Optional) Add a voice policy. |
| Step 6 | Provision a device template for Unified Communications. |

- Workflow for adding a voice port, POTS dial peer, SIP dial peer, or SRST phone profile subpolicy to a voice policy.

| | |
|---|---|
| Step 1 | Detach the device templates that include the UC voice policy and UC-specific feature templates. |
| Step 2 | Add the subpolicy to the voice policy. |
| Step 3 | Map the updated voice policy to endpoints as needed. |
| Step 4 | Attach the feature templates to a device template. |

- Workflow for updating feature templates to add or delete UC endpoints.

| | |
|---|---|
| Step 1 | Detach the device templates that include the voice card UC-specific feature templates and a voice policy. |
| Step 2 | Update the voice card feature templates as needed. |
| Step 3 | Map the updated voice policy to endpoints as needed. |
| Step 4 | Attach the feature templates to a device template. |

- Workflow for updating configuration parameters when the functionality of a voice port changes.

| | |
|---|---|
| Step 1 | Detach the device templates that include the voice card UC-specific feature templates and an associated voice policy mapping. |
| Step 2 | Update the voice card feature template and voice policy as needed. |

| | |
|---|---|
| Step 3 | Map the updated voice policy to endpoints as needed. |
| Step 4 | Attach the feature templates and the voice policy to a device template. |

- Workflow for changing the interface type for a T1/E1 voice module.

| | |
|---|---|
| Step 1 | Detach the device template that includes the voice card feature template that defines the T1/E1 voice module, and detach the associated mapped voice policy. |
| Step 2 | Unmap all voice policies from the PRI ISDN voice ports that are configured for the T1/E1 voice module, and unmap the POTS dial-peers for those ports. |
| Step 3 | In the voice card feature template, delete the PRI ISDN voice ports that are configured for the T1/E1 voice module. |
| Step 4 | Reattach the device template to devices. |
| Step 5 | Reload the devices. |
| Step 6 | Detach the device template from the devices. |
| Step 7 | In the voice card feature template create new PRI ISDN voice ports for the T1/E1 voice module as needed. |
| Step 8 | Map the voice card feature template and voice policy to the device template. |
| Step 9 | Map the updated voice policy to the newly created PRI ISDN voice ports as needed. |
| Step 10 | Reattach the device template to devices. |

- Workflow for updating the clock source configuration for a T1/E1 voice module to change the primary and secondary clock sources.

| | |
|---|---|
| Step 1 | In the voice card feature template for the T1/E1 voice module that you want to update, set the clock source for each PRI ISDN voice port to **Line**, and push the configuration to devices. |
| Step 2 | After the configuration is pushed successfully, in the voice card feature template set the clock source for each PRI ISDN voice port for the T1/E1 voice module to the desired values, and push the configuration to devices. |

• Configure UC Voice Services Using the Workflow Library or Configuration Groups, on page 479
• Add a Voice Card Feature Template, on page 480
• Add a Call Routing Feature Template, on page 490
• Add an SRST Feature Template, on page 494
• Add a DSPFarm Feature Template, on page 496
• Add a Voice Policy, on page 508
• Provision a Device Template for Unified Communications, on page 548
• Dial Peer CSV File, on page 550
• Translation Rules CSV File, on page 552
• Monitoring UC Operations, on page 553
• Cisco Unified Communications FXS and FXO Caller ID Support, on page 560

# Configure UC Voice Services Using the Workflow Library or Configuration Groups

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure and enable certain UC voice service features by using the Workflow library or configuration groups.

To configure and enable UC voice services by using the Workflow Library, choose **Workflows > Configure UC Voice** from the Cisco SD-WAN Manager window and follow the prompts in the workflow.

To configure and enable UC voice services by using configuration groups, see UC Voice Profile.

The following table lists the features that you can configure and enable by using these methods, and shows the first Cisco SD-WAN Manager release that supports these configuration methods.

***Table 72: Supported Releases for Configuring UC Voice Services Using the Workflow Library or Configuration Groups***

| Feature | First Supported Release | |
|---|---|---|
| | Workflow Library Features | Configuration Groups Features |
| DSP Farm | Cisco Catalyst SD-WAN Manager Release 20.13.1 | Cisco Catalyst SD-WAN Manager Release 20.13.1 |

### Supported Devices for Cisco Unified Voice Services using the Workflow Library or Configuration Groups

- Supported platforms:

| Platform | Release |
|---|---|
| Cisco ISR 4451 running Cisco IOS XE 17(12)3a | Cisco IOS XE Catalyst SD-WAN Release 17.12.3 |
| Cisco ISR4431 running Cisco IOS XE 17(12)3a | |
| Cisco ISR 4351 running Cisco IOS XE 17(12)3a | |
| Cisco ISR4331 running Cisco IOS XE 17(12)3a | |
| Cisco ISR4321 running Cisco IOS XE 17(12)3a | |

| Platform | Release |
|---|---|
| Cisco ISR4461 | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and later |
| Cisco C8300-2N2S-4T2x | |
| Cisco C8300-2N2S-6T | |
| Cisco C8300-1N1S-4T2X | |
| Cisco C8300-1N1S-6T | |
| Cisco C8200-1N-4T | |
| Cisco C8200L-1N-4T | |
| Cisco Catalyst 8000V | |

- Supported voice modules for analog interfaces:
  - NIM-2FXO, NIM-4FXO, NIM-2FXSP, NIM-4FXSP, NIM-2FXS/4FXOP
  - SM-X-72FXS, SM-X-24FXS/4FXO, SM-X-16FXS/2FXO, SM-X-8FXS/12FXO
- Supported voice modules for digital interfaces with Packet Voice DSP modules (PVDMs):
  - NIM-1MFT-T1/E1, NIM-2MFT-T1/E1, NIM-4MFT-T1/E1, NIM-8MFT-T1/E1
  - NIM-1CE1T1/PRI-T1/E1, NIM-2CE1T1/PRI-T1/E1, NIM-8CE1T1/PRI-T1/E1
  - PVDM4-32, PVDM4-64, PVDM4-128, PVDM4-256
- Supported PVDM modules for digital signal processor (DSP) farms:
  - NIM-PVDM-32, NIM-PVDM-64, NIM-PVDM-128, NIM-PVDM-256
  - PVDM4-32, PVDM4-64, PVDM4-128, PVDM4-256
  - SM-X-PVDM-500, SM-X-PVDM-1000, SM-X-PVDM-2000, SM-X-PVDM-3000

# 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 73: 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.<br>Using Port Range, you can create analog interfaces as described later in this procedure to configure different ranges of ports. | — |
| 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.<br>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.<br>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}<br>**signal did** {delay-dial \| immediate \| wink-start} |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Caller-ID Enable | Available if you select a signal type of Loopstart or Groundstart.<br>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.<br>Choose the mode for the DID signal type (**Delay Dial**, **Immediate**, or **Wink Start**).<br>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.<br>Default: Off. | **shutdown** |

The following table describes options for configuring a digital interface.

***Table 74: Digital Interface Configuration Options***

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| **Digital Interface Tab**<br>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:<br>• **T1 PRI**—Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding<br>• **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:<br>**1.** Click **Add**. The Port and Clock Selector window displays.<br>**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.<br>**3.** For each port, select the clock source:<br>• **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.<br>• **Primary Clock**—Sets the port to be a primary clock source.<br>• **Secondary Clock**—Sets the port to be a secondary clock source.<br>• **Network**—Sets the backplane clock or the system oscillator clock as the module clock source.<br>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.<br>**4.** Click **Add**. | **controller** {**t1** \| **e1**} *slot*/*sub-slot*/*number*<br>**clock source** {**network** \| **line** \| **line primary** \| **line secondary**} |
| Network Participation | This check box displays after you add an interface.<br>Check this check box to configure the T1/E1 module to participate in the backplane clock.<br>Uncheck this check box to remove the clock synchronization with the backplane clock for the module.<br>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.<br>1. Click **Shutdown Selected**. The Shutdown window displays.<br>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.<br>3. Click **Add**. | **controller e1/t1** *slot*/*sub-slot*/*port* **shutdown**<br>**interface serial** *slot*/*sub-slot*/**port:**{**15** \| **23**} **shutdown**<br>**voice-port** *slot*/*sub-slot*/**port:**{**15** \| **23**} **shutdown** |
| Time Slots | Select the number of time slots of the interface type.<br>Valid ranges:<br>• For T1 PRI—Time slots 1 through 24. The 24th time slot is the D channel.<br>• For E1 PRI— Time slots 1 through 31. The 16th time slot is the D channel. | **controller e1/t1** *slot*/*sub-slot*/*port*<br>**pri-group timeslots** *timeslot-range* [**voice-dsp**] |
| Framing | Select the frame type for the interface type.<br>For a T1 PRI interface type, options are:<br>• **esf**—Extended super frame (default)<br>• **sf**—Super frame<br>For an E1 PRI interface type, options are:<br>• **crc4**—CRC4 framing type (default)<br>• **no-crc4**—No CRC4 framing type | **controller t1** *slot*/*sub-slot*/*port* **framing** [**esf** \| **sf**]<br>**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.<br>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.<br>For a T1 PRI interface type, options are:<br>• **ami**—Use Alternate Mark Inversion as the line code type<br>• **b8zs**—Use binary 8-zero substitution as the line code type (default)<br>For an E1 PRI interface type, options are:<br>• **ami**—Use Alternate Mark Inversion as the line code type<br>• **hdb3**—Use high-density binary 3 as the line code type (default) | **controller t1** *slot/sub-slot/port* **linecode** [**ami** \| **b8zs**]<br>**controller e1** *slot/sub-slot/port* **linecode** [**ami** \| **hdb3**] |
| Line Termination | This check box appears only for an Interface type of E1 PRI.<br>Select the line termination type for the E1 controller:<br>• **75-ohm**—75 ohm unbalanced termination<br>• **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.<br>Select the cable length type for the T1 PRI interface type:<br>• **long**—Long cable length<br>• **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.<br>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.<br>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.<br>By default, this option is disabled (set to **No**). | **interface serial** *slot*/*sub-slot*/**port:**{**15**\| **23**}<br>**isdn protocol-emulate** [**network**\| **user**] |
| Switch Type | Select the ISDN switch type for this interface:<br>• **primary-qsig**—Supports QSIG signaling according tot the Q.931 protocol. Network side functionality is assigned with the isdn protocol-emulate command.<br>• **primary-net5**—NET5 ISDN PRI switch types for Asia, Australia, and New Zealand. ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system.<br>• **primary-ntt**—Japanese NTT ISDN PRI switches.<br>• **primary-4ess**—Lucent (AT&T) 4ESS switch type for the United States.<br>• **primary-5ess**—Lucent (AT&T) 5ESS switch type for the United States.<br>• **primary-dms100**—Nortel DMS-100 switch type for the United States.<br>• **primary-ni**—National ISDN switch type. | **interface serial** *slot*/*sub-slot*/**port:**{**15**\| **23**}<br>**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:<br>**1.** Click **Add**. The ISDN Timer window displays.<br>**2.** Configure the following timers as needed. The values are in milliseconds.<br>• **T200**. Valid range: integers 400 through 400000. Default: 1000.<br>• **T203**. Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations.<br>• **T301**. Valid range: integers 180000 through 86400000. The default value is based on the switch type and network side configurations.<br>• **T303**. Valid range: integers 400 through 86400000. The default value is based on the switch type and network side configurations.<br>• **T306**. Valid range: integers 400 through 86400000. Default: 30000.<br>• **T309**. Valid range: integers 0 through 86400000. The default value is based on the switch type and network side configurations.<br>• **T310**. Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations.<br>• **T321**. Valid range: Integers 0 through 86400000. The default value is based on the switch type and network side configurations.<br>**3.** Click **Add**. | **interface serial** *slot*/*sub-slot*/**port:** {**15**\| **23**}<br>**isdn timer T200** *value*<br>**isdn timer T203** *value*<br>**isdn timer T301** *value*<br>**isdn timer T303** *value*<br>**isdn timer T306** *value*<br>**isdn timer T309** *value*<br>**isdn timer T310** *value*<br>**isdn timer T321** *value* |
| Delay Connect Timer | Select the duration, in milliseconds, to delay connect a PRI ISDN hairpin call.<br>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**<br>Use this tab to configure priority order for the primary and secondary clock sources that you selected for each module.<br>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.<br>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.<br>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.<br>After you configure the priority, this field displays the selected ports in priority order.<br>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.<br>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.<br>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 75: 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.<br>Enter each IPv4 address in CIDR format. For example, 10.1.2.3/32. Separate each address with a comma (,).<br>The router does not communicate with other IPv4 addresses, which prevents fraudulent calls being placed through the router.<br>A Trusted IPv4 Prefix is required for TDM to IP calls. | **voice service voip**<br>**ip address trusted list**<br>**ipv4** *ipv4-address*/*ipv4-network-mask* |
| Trusted IPv6 Prefix List | Enter the IPv6 addresses with which the router can communicate through SIP.<br>Separate each IPv6 address with a comma (,).<br>The router does not communicate with other IPv6 addresses, which prevents fraudulent calls being placed through the router.<br>A Trusted IPv6 Prefix is required for TDM to IP calls. | **voice service voip**<br>**ip address trusted list**<br>**ipv6** *ipv6-prefix*//*prefix-length* |
| Source Interface | Enter the name of the source interface from which the router initiates SIP control and media traffic.<br>This information defines how the return/response to this traffic should be sent. | **voice service voip**<br>**sip**<br>**bind control source-interface** *interface-id*<br>**bind media source-interface** *interface-id* |

The following table describes options for configuring dial peers.

***Table 76: 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:<br>dial-peer voice *number* {pots \| voip}<br>**incoming called-number** *string*<br>Outgoing:<br>dial-peer voice *number* {pots \| voip}<br>**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.<br>Enter the string as an E.164 format regular expression in the form [0-9,A-F#*.?+%()-]*T?. | Incoming:<br>dial-peer voice *number* {pots \| voip}<br>**incoming called-number***string*<br>Outgoing:<br>dial-peer voice *number* {pots \| voip}<br>**destination-pattern** *string* |
| Forward Digits Type | Available if you select the POTS dial peer type and the Outgoing direction.<br>Select how the dial peer transmits digits in outgoing numbers:<br>• **All**—The dial peer transmits all digits<br>• **None**—The dial peer does not transmit digits that do not match the destination pattern<br>• **Some**—The dial peer transmits the specified number of right-most digits<br>Default: None. | All:<br>dial-peer voice *number* pots<br>**forward-digits all**<br>None:<br>dial-peer voice *number* pots<br>**forward-digits 0**<br>Some:<br>dial-peer voice *number* pots<br>**forward-digits** *number* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Forward Digits | Available if you select **Some** for Forward Digits Type.<br>Enter the number of right-most digits in the outgoing number to transmit.<br>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<br>**forward-digits** *number* |
| Prefix | Available if you select the POTS dial peer type and the Outgoing direction.<br>Enter digits to be prepended to the dial string for outgoing calls. | dial-peer voice *number* pots<br>**prefix** *string* |
| Transport Protocol | Available if you select SIP for the Dial Peer Type.<br>Choose the transport protocol (**TCP** or **UDP**) for SIP control signaling. | dial-peer voice *number* voip<br>**session transport** {**tcp** \| **udp**} |
| Preference | Available if you select POTS or SIP for the Dial Peer Type.<br>Select an integer from 0 to 10, where the lower the number, the higher the preference.<br>If dial peers have the same match criteria, the system uses the one with the highest preference value.<br>Default: 0 (highest preference). | dial-peer voice *number* voip<br>**preference** *value*<br>dial-peer voice *number* pots<br>**preference** *value* |
| Voice Port | Available if you select the POTS dial peer type.<br>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**.<br>For an outgoing dial peer, the router sends calls that match the dial peer to this port.<br>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<br>For an analog port:<br>**port** *slot*/*subslot*/*port*<br>For a digital port:<br>**port** *slot*/*subslot*/*port***:15**<br>**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.<br>Enter the network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched.<br>Enter the address in one of these formats:<br>• dns:*hostname.domain*<br>• *sip-server*<br>ipv4:*destination-addres*<br>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 #unique_368.
   - 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 77: 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**<br>**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.<br>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**<br>**max-pool** *max-voice-register-pools* |
| Max Directory Numbers | Enter the number of DNs that the gateway supports when in Cisco Unified SRST mode.<br>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**<br>**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.<br>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**<br>**moh** *filename* |

The following table describes options for configuring Cisco Unified SRST phone profiles.

***Table 78: 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.<br>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.<br>For example, a.b.c.d/24. | **voice register pool** *pool-tag*<br>**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*<br>**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 79: 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*<br>**dsp service dspfarm** |

The following table describes options for configuring DSP farm services.

***Table 80: 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<br>When this check box is unchecked, transcoding is allowed only between the G.711 codec and other codecs.<br>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.<br>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.<br>• For the Transcoder profile type:<br>  • g711alaw<br>  • g711ulaw<br>  • g729abr8<br>  • g729ar8<br>  • g729br8<br>  • g729r8<br>  • g722-64<br>  • ilbc<br>  • iSAC<br>  • pass-through<br>• For the Conference profile type:<br>  • g711alaw<br>  • g711ulaw<br>  • g722r-64<br>  • g729abr8<br>  • g729ar8<br>  • g729br8<br>  • g729r8<br>• For the MTP profile type for software MTP only:<br>  • g711ulaw<br>  • g711alaw | |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| | • g722-64<br>• g729abr8<br>• g729ar8<br>• g729br8<br>• g729r8<br>• ilbc<br>• iSAC<br>• pass-through<br>• For the MTP profile type for hardware MTP only, or for hardware and software MTP:<br>• g711ulaw<br>• g711alaw<br>• pass-through | |
| Conference Maximum Participants | Available if you select Conference for the Profile Type.<br>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.<br>Enter the maximum number of sessions that this profile can support.<br>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.<br>Select the way in which the router performs minor MTP translations such as G.711alaw to G.711ulaw, and DTMF conversions.<br>Options are:<br>• **Hardware**—MTP translations and conversions are performed by the hardware DSP resources<br>• **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.<br>Select the maximum number of hardware sessions that can be used for MTP translations and conversions.<br>Maximum value: 4000 | **maximum session hardware** *number* |
| MTP Maximum Software Sessions | Available if you select Software for the MTP type.<br>Select the maximum number of CPU sessions that can be used for MTP translations and conversions.<br>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 81: SCCP Options*

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| **CUCM Tab**<br>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.<br>Enter the interface in this format:<br>***interface-type/interface-number/port***<br>where:<br>• *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.<br>• *interface-number*—Interface number that the services use to register with Cisco Unified Communications Manager.<br>• *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.<br>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.<br><br>In the first field, enter the IP address or DNS name of the Cisco Unified Communications Manager server.<br><br>In the second field, enter a numerical identifier for the Cisco Unified Communications Manager server.<br><br>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**<br><br>This tab is available when at least one Cisco Unified Communications Manager server is configured in the Cisco Unified Communications Manager tab.<br><br>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.<br><br>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.<br>To do so:<br>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.<br>2. Select the server that you want to be the primary server. This server has the highest priority.<br>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.<br>The servers appear in this field in priority order.<br>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<br><br>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.<br><br>The name must contain from 6 to 15 characters. Characters can be letter, numbers, slashes (/), hyphens (-), and underscores (_). Space characters are not allowed.<br><br>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.<br><br>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.<br><br>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.<br><br>To remove a Cisco Unified Communications Manager media resource name and profile, click its corresponding minus sign (–). | **associate ccm** *profile-identifier*<br>**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:<br>• **graceful**—Switchback occurs after all active sessions terminate gracefully.<br>• **guard**—Switchback occurs either when active sessions are terminated gracefully or when the guard timer expires, whichever happens first.<br>• **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.<br>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:<br>• **graceful**—Switchback occurs after all active sessions terminate gracefully.<br>• **immediate**—Switchover occurs immediately, whether there is an active connection or not.<br>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
   - **POTS Dial Peers**–Configure POTS Dial Peers for a Voice Policy
   - **SIP Dial Peers**–See Configure SIP Dial Peers for a Voice Policy
   - **SRST Phones**–See Configure SRST Phones for a Voice Policy
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 82: 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.<br>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.<br>The name can contain up to 32 characters. | **trunk group** *name* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Hunt-Scheme | | **trunk group** *name*<br>**hunt-scheme least-idle** [**both** \| **even** \| **odd** ]<br>**hunt-scheme least-used** [**both** \| **even** \| **odd** ]<br>**hunt-scheme longest-idle** [**both** \| **even** \| **odd** ]<br>**hunt-scheme round-robin** [**both** \| **even** \| **odd** ]<br>**hunt-scheme sequential** [**both** \| **even** \| **odd** ]<br>**hunt-scheme random** |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| | Select the hunt scheme in the trunk group for outgoing calls:<br>• **least-idle both**—Searches for an idle channel with the shortest idle time<br>• **least-idle even**—Searches for an idle even-numbered channel with the shortest idle time<br>• **least-idle odd**—Searches for an idle odd-numbered channel with the shortest idle time<br>• **least-used both**—Searches for a trunk group member that has the highest number of available channels (applies only to PRI ISDN cards)<br>• **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)<br>• **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)<br>• **longest-idle both**—Searches for an idle odd-numbered channel with the longest idle time<br>• **longest-idle even**—Searches for an idle channel that has the highest number of available even-numbered channels<br>• **longest-idle odd**—Searches for an idle channel that has the highest number of available odd-numbered channels<br>• **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<br>• **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<br>• **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<br>• **sequential-both**—Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk group<br>• **sequential-even**—Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group<br>• **sequential-odd**—Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group<br>• **random**—Searches for a trunk group member at random and selects a channel from the member at random<br>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.<br>If the maximum number of calls is reached, the trunk group becomes unavailable for more calls.<br>• In field—Enter the maximum number of incoming calls that are allowed for this trunk group<br>• Out field— Enter the maximum number of outgoing calls that are allowed for this trunk group<br>Valid range for both fields: integers 0 through 1000. | **trunk group** *name*<br>**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.<br>If you do not enter a value and a call fails, the system does not attempt to make the call again.<br>Valid range: integers 1 through 5. | **trunk group** *name*<br>**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 83: 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.<br>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.<br>The Translation Rules pane displays. | **translate calling** *translation-rule-number* |
| Called | Click to configure translation rules for the number that is being called.<br>The Translation Rules pane displays. | **translate called** *translation-rule-number* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Translation Rules pane | | **voice translation-rule** *number*<br>Match and Replace Rule:<br>**rule** *precedence /match-pattern/ / replace-pattern/*<br>Reject Rule:<br>**rule** *precedence* **reject** */match-pattern/* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| | 1. Click **Add New** to create a translation rule.<br><br>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**.<br><br>2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100.<br><br>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 #unique_376.<br><br>4. Click **Add Rule**.<br><br>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/.<br><br>To include the backslash character (\) in a match string, precede the backslash with a backslash.<br><br>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.<br><br>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.<br>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.<br>**8.** Click **Save**.<br>**9.** Add more translation rules as needed.<br>**10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file.<br>**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 84: Station ID Options***

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Station Name | Enter the name of the station.<br>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.<br>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 85: Line Params Options***

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Gain | Enter the gain, in dB, for voice input.<br>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.<br>Valid range: –6 through 14. Default: 3. | **output attenuation** *decibels* |
| Echo Canceller | Select **Enable** to apply echo cancellation to voice traffic.<br>By default, this option is enabled. | **echo-cancel** *enable* |
| Voice Activity Detection (VAD) | Select **Enable** to apply VAD to voice traffic.<br>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**).<br>Default: U-Law. | **compand-type** {**u-law** \| **a-law**} |
| Impedance | This field does not apply to PRI ISDN cards.<br>Select the terminating impedance for calls.<br>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 86: 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.<br>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:<br>• **Anytone**—Any tone indicates a supervisory disconnect<br>• **Signal**—A disconnect signal indicates a supervisory disconnect<br>• **Dualtone**—A dual-tone indicates a supervisory disconnect<br>Default: Signal. | Anytone:<br>supervisory disconnect **anytone**<br>Signal:<br>supervisory disconnect<br>Dualtone:<br>supervisory disconnect **dualtone** {**mid-call** \| **pre-connect**} |
| Dial Type | Select the dialing method for outgoing calls:<br>• **pulse**—Pulse dialer<br>• **dtmf**—Dual-tone multifrequency dialer<br>• **mf**—Multifrequency dialer<br>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).<br>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.<br>Select **Answer** to configure the port to support answer supervision by detection of battery reversal.<br>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).<br>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**]<br>**battery-reversal-detection-delay** *milliseconds* |
| Timing Hookflash out | Enter the duration, in milliseconds, of hookflash indications that the gateway generates on the FXO interface.<br>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.<br>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.<br>Valid range for minimum duration: 0 through 400. Default minimum value: 50.<br>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**.<br>Default: Yes. | **pulse-digit-detection** |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Loop Length | Select the length for signaling on FXS ports (**Long** or **Short**).<br>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.<br>• **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*<br>**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.<br>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 87: 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:<br>• **Custom CPTone**—Provides options for configuring cptone detection parameters for a supervisory disconnect event<br>• **Dual Tone Detection Params**—Provides options for configuring dual-tone detection parameters for a supervisory disconnect event | **voice class custom-cptone** *cptone-name*<br>**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.<br>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:<br>• Busy<br>• Disconnect<br>• Number Unobtainable<br>• Out of Service<br>• Reorder<br>• 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.<br>Valid range for each tone is 300 through 3600. | **frequency** *frequency-1* [*frequency-2*] |
| Supervisory Number | Applies to Custom Dual Tone Detection Params mode.<br>Enter a unique number to identify dual-tone detection parameters.<br>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.<br>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.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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*<br>**freq-max-deviation** *hertz*<br>**freq-max-power** *dBm0*<br>**freq-min-power** *dBm0*<br>**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 88: 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.<br>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.<br>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.<br>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.<br>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.<br>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 89: 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.<br>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**.<br>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.<br>The name can contain up to 32 characters. | **trunk group** *name* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Hunt-Scheme | | **trunk group** *name*<br>**hunt-scheme least-idle** [**both** \| **even** \| **odd** ]<br>**hunt-scheme least-used** [**both** \| **even** \| **odd** ]<br>**hunt-scheme longest-idle** [**both** \| **even** \| **odd** ]<br>**hunt-scheme round-robin** [**both** \| **even** \| **odd** ]<br>**hunt-scheme sequential** [**both** \| **even** \| **odd** ]<br>**hunt-scheme random** |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| | Select the hunt scheme in the trunk group for outgoing calls:<br>• **least-idle both**—Searches for an idle channel with the shortest idle time<br>• **least-idle even**—Searches for an idle even-numbered channel with the shortest idle time<br>• **least-idle odd**—Searches for an idle odd-numbered channel with the shortest idle time<br>• **least-used both**—Searches for a trunk group member that has the highest number of available channels (applies to only PRI ISDN cards)<br>• **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)<br>• **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)<br>• **longest-idle both**—Searches for an idle odd-numbered channel with the longest idle time<br>• **longest-idle even**—Searches for an idle channel that has the highest number of available even-numbered channels<br>• **longest-idle odd**—Searches for an idle channel that has the highest number of available odd-numbered channels<br>• **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<br>• **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<br>• **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<br>• **sequential-both**—Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk group<br>• **sequential-even**—Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group<br>• **sequential-odd**—Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group<br>• **random**—Searches for a trunk group member at random and selects a channel from the member at random<br>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.<br>If the maximum number of calls is reached, the trunk group becomes unavailable for more calls.<br>• **In field**—Enter the maximum number of incoming calls that are allowed for this trunk group.<br>• **Out field**— Enter the maximum number of outgoing calls that are allowed for this trunk group.<br>Valid range for both fields: integers 0 through 1000. | **trunk group** *name*<br>**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.<br>If you do not enter a value and a call fails, the system does not attempt to make the call again.<br>Valid range: integers 1 through 5. | **trunk group** *name*<br>**max-retry** *attempts* |

- **Translation Profiles**—The following table describes these options.

***Table 90: 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.<br>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.<br>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.<br>The Translation Rules pane displays. | **translate calling** *translation-rule-number* |
| Called | Click to configure translation rules for the number that is being called.<br>The Translation Rules pane displays. | **translate called** *translation-rule-number* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Translation Rules pane | | **voice translation-rule** *number*<br>Match and Replace Rule:<br>**rule** *precedence* /*match-pattern*/ / *replace-pattern*/<br>Reject Rule:<br>**rule** *precedence* **reject** /*match-pattern*/ |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| | 1. Click **Add New** to create a translation rule.<br><br>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**.<br><br>2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100.<br><br>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 #unique_376.<br><br>4. Click **Add Rule**.<br><br>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/.<br><br>To include the backslash character (\) in a match string, precede the backslash with a backslash.<br><br>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.<br><br>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.<br><br>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.<br><br>**8.** Click **Save**.<br><br>**9.** Add more translation rules as needed.<br><br>**10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file.<br><br>**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 91: 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.<br>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.<br>The Translation Rules pane displays. | **translate calling** *translation-rule-number* |
| Called | Click to configure translation rules for the number that is being called.<br>The Translation Rules pane displays. | **translate called** *translation-rule-number* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Translation Rules pane | | **voice translation-rule** *number*<br>Match and Replace Rule:<br>**rule** *precedence /match-pattern/ / replace-pattern/*<br>Reject Rule:<br>**rule** *precedence* **reject** */match-pattern/* |

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| | 1. Click **Add New** to create a translation rule.<br><br>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**.<br><br>2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100.<br><br>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 #unique_376.<br><br>4. Click **Add Rule**.<br><br>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/.<br><br>To include the backslash character (\) in a match string, precede the backslash with a backslash.<br><br>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.<br><br>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.<br>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.<br>**8.** Click **Save**.<br>**9.** Add more translation rules as needed.<br>**10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file.<br>**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 92: 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.<br>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.<br>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*<br>**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.<br>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.<br>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 93: 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.<br>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:<br>• **None**—Modem pass-through is disabled on the device<br>• **NSE G.711ulaw**—Uses named signaling events (NSEs) to communicate G.711ulaw codec switchover between gateways<br>• **NSE G.711alaw**—Uses named signaling events (NSEs) to communicate G.711alaw codec switchover between gateways | None:<br>**no modem passthrough**<br>NSE G.711 ulaw:<br>**modem passthrough nse codec g711ulaw**<br>NSE G.711 alaw:<br>**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 94: 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.<br>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.<br>For a detailed description of each bundle, see the “Primary Fax Protocol Command Bundles” table<br>The descriptions of the bundles include the following components:<br>• **nse**—Uses NSEs to switch to T.38 fax relay mode<br>• **force**—Unconditionally uses Cisco Network Services Engines (NSE) to switch to T.38 fax relay<br>• **version**—Specifies a version for configuring fax speed:<br>  • **0**—Configures version 0, which uses T.38 version 0 (1998–G3 faxing)<br>  • **3**—Configures version 3, which uses T.38 version 3 (2004–V.34 or SG3 faxing)<br>• **none**—No fax pass-through or T.38 fax relay is attempted<br>• **Pass-through**—The fax stream uses one of the following high-bandwidth codecs:<br>  • **g711ulaw**—Uses the G.711 ulaw codec<br>  • **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.”<br>Select the fallback mode for fax transmissions. This fallback mode is used if the primary fax protocol cannot be negotiated between device endpoints.<br>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."<br>Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol.<br>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."<br>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.<br>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 95: 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.<br>Options for selecting the low-speed and high-speed redundancy values are available. | **fax protocol t38 version 3**<br>**ls-redundancy** *value*<br>**hs-redundancy** *value*<br>**no fax-relay sg3-to-g3** |
| T.38 Fax Relay Version 0 | Primary fax protocol is T.38 fax relay version 0.<br>Options for selecting the low-speed and high-speed redundancy values are available. | **fax protocol t38 version 0**<br>**ls-redundancy** *value*<br>**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.<br>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*<br>**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.<br>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*<br>**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.<br>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.<br>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.<br>Options for selecting the low-speed and high-speed redundancy values are available. | **fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value*<br>**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.<br>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*<br>**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.<br>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*<br>**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.<br>Options for selecting the low-speed and high-speed redundancy values are available. | **fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value*<br>**fax-relay ecm disable**<br>**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.<br>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*<br>**fax-relay ecm disable**<br>**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.<br>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*<br>**fax-relay ecm disable**<br>**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<br>Options for selecting the low-speed and high-speed redundancy values are available. | **fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value*<br>**fax-relay ecm disable**<br>**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.<br>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*<br>**fax-relay ecm disable**<br>**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.<br>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*<br>**fax-relay ecm disable**<br>**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.<br>Options for selecting the low-speed and high-speed redundancy values are available. | **fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value*<br>**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.<br>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*<br>**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.<br>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*<br>**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.<br>Options for selecting the low-speed and high-speed redundancy values are available. | **fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value*<br>**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.<br>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*<br>**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.<br>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*<br>**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**<br>**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**<br>**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 96: 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**<br>**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 97: SRST Phones Configuration Options*

| Option | Description | Cisco IOS CLI Equivalent |
|---|---|---|
| Medial Profile Number | Enter a number for this Cisco Unified SRST media profile.<br>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.<br>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*<br>**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.<br>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.<br>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 98: Generated CLI Commands for Subpolicies to Endpoints Mapping***

| Endpoint | Subpolicy | Cisco IOS CLI Application Mapping | Remarks |
|---|---|---|---|
| Voice Port FXO<br>Voice Port FXS<br>Voice Port FXS DID<br>Voice Port PRI ISDN<br>POTS Dial Peer<br>SIP Dial Peer | Translation profile | **translation-profile incoming** *profile-name*<br>**translation-profile outgoing** *profile-name* | A translation profile policy is applied to a dial peer or a voice profile. |
| SRST Phone<br>SIP Dial Peer | Media profile | voice register pool *number*<br>**voice-class codec** *number*<br>**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*<br>**supervisory custom-cptone** *cptone-name*<br>**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<br>Voice Port FXS<br>Voice Port FXS DID<br>Voice Port PRI ISDN<br>POTS Dial Peer | Trunk group | **trunk-group name** [*preference-num*]<br>**voice-port** *number*<br>*trunk-group name* [*preference-num*]<br>**interface serial** *slot*/*sub-slot*/**port:** {**15** \| **23**}<br>**dial-peer voice** *tag* **pots**<br>**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.<br>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:<br>**no modem passthrough**<br>G.711 ulaw:<br>**modem passthrough nse codec g711ulaw**<br>G.711 alaw:<br>**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**}}]} | — |

# Dial Peer CSV File

A dial peer CSV file includes information for one or more incoming and outgoing SIP and POTS dial peers. The file must be comma delimited, and each record in the file must include each field that the following table describes, in the order shown.

*Table 99: Dial Peer CSV Files Fields*

| Field | Description |
|---|---|
| Dial Peer Tag | Number that is used to reference the dial peer. |
| Dial Peer Type | Type of dial peer that you are creating (**pots** or **voip**). |
| Direction | Direction of traffic on the dial peer (**Incoming** or **Outgoing**). |
| Description | Description of the dial peer. |
| Forward Digits | How the dial peer transmits digits in outgoing numbers:<br>• **All**—The dial peer transmits all digits in the number.<br>• **None**—The dial peer does not transmit digits in the number that do not match the destination pattern.<br>• *n*—The dial peer transmits the number of right-most digits in the number that the integer *n* represents. For example, if *n* is 7 and the outgoing number is 1112223333, the dial peer transmits 2223333. |
| Preference | For POTS dial peers, a unique numeric value for the dial peer. If dial peers have the same match criteria, the system uses the one with the highest preference value. |
| Prefix | Digits to be prepended to outgoing POTS dial peer calls. |
| Numbering Pattern | String that the router uses to match incoming calls to the dial peer. |
| Dest. Address | Network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched. |
| Voice Port | Voice port that the router uses to match calls to the dial peer.<br>For an outgoing dial peer, the router sends the calls that match the dial peer to this port.<br>For an incoming dial peer, this port serves as an additional match criterion. The dial peer is matched only if a call comes in on this port. |

| Field | Description |
|---|---|
| Transport Protocol | For SIP dial peers, transport protocol (**TCP** or **UDP**) for SIP control signaling. |

Example dial peer CSV file:

```
Tag,type,Direction,Description,Forward Digits,Preference,Prefix,Pattern,Dest. Address,Voice
 Port,Transport
6545,voip,Outgoing,description To Voice Gateway,,1,,23456,ipv4:166.2.121.17,,udp
6756,voip,Outgoing,description ***Fax Number 6362-6362***,,0,,34567,ipv4:166.2.121.16,,tcp
768,voip,Outgoing, description Fire Alarm Dialer,,8,,5678,ipv4:166.2.121.19,,udp
10,pots,Incoming,,,5,,0115T,,1/0/1,
54,pots,Outgoing,,,6,,.T,,1/0/3,
23,pots,Incoming,,all,0,,76..,,1/0/4,
26,pots,Incoming,,5,1,55,9800.......,,1/0/5,
27,pots,Incoming,,5,1,55,9800.......,,0/1/5:15,
```

# Translation Rules CSV File

When you configure translation rules for a translation profile, POTS dial peer, or SIP dial peer you can either create new translation rules or import existing translation rule information from a CSV file.

The file must be comma delimited, and each record in the file must include each field that the following table describes, in the order shown:

***Table 100: Translation Rules CSV Files Fields***

| Field | Description |
|---|---|
| Match | String that you want the translation rule to affect. The string must be in regular expression format beginning and ending with a slash (/). For example, /^9/. |
| Action | Action that the system performs for calls that match the string in the Match field. Valid values are:<br>• **reject**—Causes the system to reject the call<br>• **replace**—Causes the system to replace the match string with the value in the Replace field |
| Replace | If the Action field contains **replace**, this field contains 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.<br>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. |

Example translation rules CSV file:

```
Match,Action,Replace
/34/,replace,/34/
/23/,reject,
/56/,replace,/100/
/16083652563/,replace,/6083652563/
```

# 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 101: 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 102: 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 |

| Field | Description |
|---|---|
| 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 103: Voice Phone Info Monitoring Information***

| Field | Description |
|---|---|
| Pool Tag | Tag number that is assigned to the Cisco Unified SRST phone pool on the device |
| 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 104: 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. |

| Field | Description |
|---|---|
| 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. |
| 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 105: 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. |

| Field | Description |
|---|---|
| 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. |
| 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 106: 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 107: 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 |
| 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 108: 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. |

| Field | Description |
|---|---|
| Operation | Status of the registration of the profile with Cisco Unified Communications Manager:<br>• ACTIVE IN PROGRESS—Profile is in the process of registering with Cisco Unified Communications Manager<br>• DOWN—Profile is unable to register with Cisco Unified Communications Manager<br>• ACTIVE— Profile is registered with Cisco Unified Communications Manager |
| 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:<br>• app-assoc-done—Profile is associated with Cisco Unified Communications Manager<br>• 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 109: 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 |

| Field | Description |
|---|---|
| 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 110: Voice DSPFarm Active Monitoring Information***

| Field | Description |
|---|---|
| DSP | Identifier of the DSP for an active call that uses this DSP farm service |
| 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 |

# Cisco Unified Communications FXS and FXO Caller ID Support

***Table 111: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Unified Communications FXS and FXO Caller ID Support | Cisco IOS XE Catalyst SD-WAN Release 17.8.1a<br>Cisco vManage Release 20.8.1 | This feature lets you configure Foreign Exchange Station (FXS) and Foreign Exchange Office (FXO) caller ID features by using Cisco SD-WAN Manager CLI add-on feature templates. |

## Information About Adding Voice Features with a CLI Add-On Feature Template

You can configure FXS and FXO caller ID features in Cisco IOS XE Catalyst SD-WAN devices by using CLI add-on feature templates. For detailed information about CLI add-on feature templates, see CLI Add-On-Feature Templates.

Caller ID is an analog service by which a telephone central office switch sends digital information about an incoming call. The Caller ID feature for analog FXS ports is configurable on a per-port basis to phones that

are connected to analog FXS voice ports. Caller ID also is available on analog FXO ports. Caller ID-related features are based on the identity of the calling party.

If an FXS voice port has caller-id commands configured, remove all the caller-id configurations before changing the signaling type from loop-start or ground-start to Direct Inward Dialing (DID).

If you remove a voice port from a device after a caller ID command is configured, remove the caller ID configuration from the device. Otherwise, a voice port configuration mismatch occurs between the Cisco IOS configuration and the Cisco Catalyst SD-WAN configuration.

# Supported Devices for Adding Voice Features with a CLI Add-On Feature Template

- Cisco NIM-2FXO network interface module
- Cisco NIM-4FXO network interface module
- Cisco NIM-2FXSP network interface module
- Cisco NIM-4FXSP network interface module
- Cisco NIM-2FXS/4FXOP network interface module
- Cisco SM-X-72FXS double-wide service module
- Cisco SM-X-24FXS/4FXO single-wide service module
- Cisco SM-X-16FXS/2FXO single-wide service module
- Cisco SM-X-8FXS/12FXO single-wide service module

# Restrictions for Adding Voice Features with a CLI Add-On Feature Template

- Caller ID must be enabled with the **caller-id enable** command before you use any of the **caller-id** commands.
- When the **caller-id alerting dsp-pre-allocate** command is used or disabled, the FXO voice port is automatically shut down and then brought up to allocate or deallocate the DSP voice channel if the FXO port is in the Idle state.

# Configure Voice Features with a CLI Add-On Feature Template

The following commands provide configuration options for caller ID features:

- **caller-id alerting dsp-pre-allocate**: Statically allocates a digital signal processor (DSP) voice channel for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving FXO voice port.
- **caller-id alerting line-reversal**: Sets the line-reversal alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending FXS voice port and for an on-hook caller ID at a receiving FXO voice port.
- **caller-id alerting pre-ring**: Sets a 250-millisecond pre-ring alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending FXS and a receiving FXO voice port.

- **caller-id alerting ring**: Sets the ring-cycle method for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving FXO or a sending FXS voice port.
- **caller-id block**: Requests blocking of caller ID information display at the far end of a call that originates from an FXS port.
- **caller-id format e911**: Specifies the caller ID message type that should be the enhanced 911 format for calls that are sent on FXS voice ports.
- **caller-id mode**: Specifies a noncountry, standard caller ID mode for a receiving FXO or a sending FXS voice port.
- **clid dtmf-codes**: Specifies global caller ID DTMF start, redirect, and end codes.

# Examples of Adding Voice Features with a CLI Add-On Feature Template

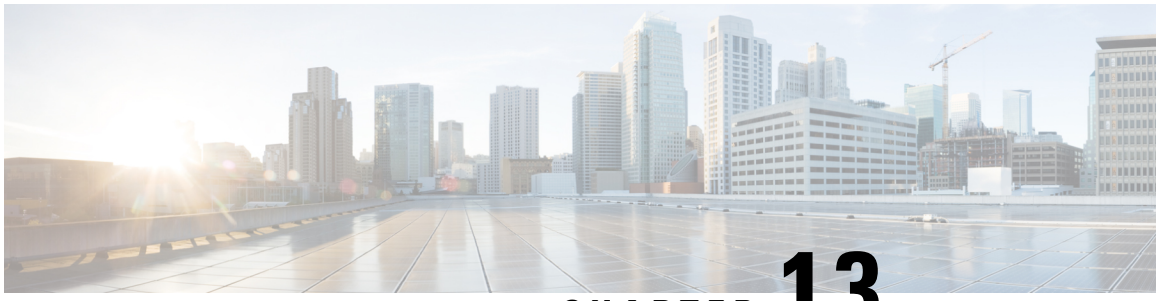
The following example shows caller ID configuration for FXS ports:

```
voice service pots
    clid dtmf-codes ABC
!
voice-port 1/0/0
   caller-id enable
   caller-id alerting ring 3
    station name West Wing
   station number 4085550100
!
voice-port 1/0/1
   caller-id enable
    caller-id mode DTMF start * end #
    caller-id alerting line-reversal
    station name East Wing
    station number 4085550101
!
voice-port 1/0/2
   caller-id enable
    caller-id mode BT
    caller-id alerting pre-ring
    station name Jose
    station number 4085550102
!
voice-port 1/0/3
    caller-id enable
    caller-id block
    station name a-sample
    station number 4085552000
!
voice-port 1/0/4
    caller-id enable
    caller-id format e911
    station name sample-2
    station number 4085552222
```

The following example shows caller ID configuration for FXO ports:

```
voice service pots
    clid dtmf-codes ABC
!
voice-port 2/0/0
    cptone BR
```

```
    caller-id enable
    caller-id alerting line-reversal
    caller-id alerting dsp-pre-allocate
!
voice-port 2/0/1
    caller-id enable
    caller-id alerting ring 2
!
voice-port 2/0/2
    caller-id enable
    caller-id BT FSK
    caller-id alerting pre-ring
```



CHAPTER 13

# CUBE Configuration

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 112: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Unified Border Element Configuration | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a<br>Cisco vManage Release 20.7.1 | This feature lets you configure Cisco Unified Border Element (CUBE) functionality by using Cisco IOS XE Catalyst SD-WAN device CLI templates or CLI add-on feature templates. |
| Secure SRST Support on Cisco Catalyst SD-WAN | Cisco IOS XE Catalyst SD-WAN Release 17.10.1a<br>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. |

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Unified Border Element Configuration | Cisco IOS XE Catalyst SD-WAN Release 17.14.1a<br>Cisco Catalyst SD-WAN Manager Release 20.14.1 | This feature provides support for the following commands:<br>• **cipher (voice class)**<br>• **nat media-keepalive**<br>• **secure-ciphersuite**<br>• **transport tcp tls (sip-ua)**<br>• **voice-class sip nat media-keepalive** |
| Survivable Remote Site Telephony (SRST) commands | Cisco IOS XE Catalyst SD-WAN Release 17.14.1a<br>Cisco Catalyst SD-WAN Manager Release 20.14.1 | This feature provides support for the following commands:<br>• **http client secure-ciphersuite**<br>• **transport-tcp-tls (call-manager-fallback)** |

This chapter provides information about configuring devices for Cisco Unified Border Element (CUBE).


- Information About CUBE, on page 566
- Supported Devices for CUBE Configuration, on page 567
- Restrictions for CUBE Configuration, on page 567
- Use Cases for CUBE, on page 567
- Configure CUBE, on page 568
- CUBE Commands, on page 569
- SRST Commands, on page 577


# Information About CUBE

CUBE bridges voice and video connectivity between two VoIP networks. It is similar to a traditional voice gateway, except for the replacement of physical voice trunks with IP-based voice trunks. Traditional gateways connect VoIP networks to telephone companies by using a circuit-switched connection, such as PRI. CUBE connects VoIP networks to other VoIP networks and enterprise networks to Internet telephony service providers (ITSPs).

CUBE provides conventional Session Border Controller (SBC) functions and a wide variety advanced features.

You can configure Cisco IOS XE Catalyst SD-WAN devices for CUBE by using device CLI templates or CLI add-on feature templates.

For more information about the CUBE setup, functionality, usage, configuration, and related topics, see the *Cisco Unified Border Element Configuration Guide*.

# Supported Devices for CUBE Configuration

- Cisco 1000 Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8000v Software Router
- Cisco ASR 1001-X Router
- Cisco ASR 1002-X Router
- Cisco ASR 1006-X Router with the Cisco ASR1000-RP3 Module, and the Cisco ASR1000-ESP100 or ASR1000-ESP100-X Embedded Services Processor
- Cisco ASR 1004 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006-X Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor

# Restrictions for CUBE Configuration

High-availability configuration is not supported for CUBE.

# Use Cases for CUBE

CUBE can be used to configure session border controller elements for a wide variety of applications, including the following:

- Enterprise premises-based collaboration capabilities using Cisco Unified Communications Manager (or another call control application) with centralized or local PSTN breakouts
- A local breakout gateway for Cisco Unified Communications Manager Cloud, which is a Cisco-hosted cloud service for large enterprises
- A local gateway to enable the Bring Your Own PSTN (BYoPSTN) option for Cisco Webex Calling
- Edge audio for Cisco Webex meetings with a direct VoIP route to the Cisco Webex cloud or through existing PSTN services

# Configure CUBE

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
```

# CUBE Commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for CUBE configuration. Click a command name in the **Command** column to view information about the command, its syntax, and its use.

***Table 113: Cisco Catalyst SD-WAN CLI Template Commands for CUBE Configuration***

| Command | Description |
|---|---|
| address-hiding | Hides signaling and media peer addresses from endpoints other than the gateway. |
| anat | Enables Alternative Network Address Types (ANAT) on a SIP trunk. |
| answer-address | Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call. |
| application (global) | Enters application configuration mode to configure applications. |
| asserted-id | Enables support for the asserted ID header in incoming SIP requests or response messages, and to send the asserted ID privacy information in outgoing SIP requests or response messages. |
| asymmetric payload | Configures SIP asymmetric payload support. |
| audio forced | Allows only audio and image (for T.38 Fax) media types, and drops all other media types). |
| authentication | Enables SIP digest authentication. |
| bind | Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface. |
| block | Configures global settings to drop (not pass) specific incoming SIP provisional response messages on a CUBE. |
| call spike | Configures the limit on the number of incoming calls received in a short period (a call spike). |
| call threshold global | Enables the global resources of a gateway. |
| call treatment action | Configures the action that the router takes when local resources are unavailable. |
| call treatment cause-code | Specifies the reason for the disconnection to the caller when local resources are unavailable. |
| call treatment isdn-reject | Specifies the rejection cause code for ISDN calls when all ISDN trunks are busied out, but the switch ignores the busyout trunks and still sends ISDN calls into the gateway. |

| Command | Description |
|---|---|
| call treatment on | Enables call treatment to process calls when local resources are unavailable. |
| callmonitor | Enables the call monitoring messaging functionality on a SIP endpoint in a VoIP network. |
| call-route | Enables header-based routing at the global configuration level. |
| cipher (voice class) | Configures the cipher setting, and associates it to a TLS profile. |
| clid | Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, and removes the calling party name and number from the calling-line identifier in voice service voip configuration mode. Alternatively, allows the presentation of the calling number by substituting for the missing **Display Name** field in the Remote-Party-ID and From headers. |
| codec preference | Specifies a list of preferred codecs to use on a dial peer. |
| codec profile | Defines audio and video capabilities that are needed for video endpoints. |
| codec transparent | Enables codec capabilities to be passed transparently between endpoints in a CUBE. |
| conn-reuse | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Reuses the TCP connection of a SIP registration for an endpoint behind a firewall. |
| connection-reuse | Uses global listener port for sending requests over UDP. |
| contact-passing | Configures pass-through of the contact header from one leg to the other leg for 302 pass-through. |
| cpa | Enables the call progress analysis (CPA) algorithm for outbound VoIP calls and to set CPA parameters. |
| credentials | Configures a SIP TDM gateway or CUBE to send a SIP registration message when in the UP state. |
| crypto signaling | Identifies the **trustpoint** *trustpoint-name* keyword and argument that is used during the Transport Layer Security (TLS) handshake that corresponds to the remote device address. |
| dial-peer cor custom | Specifies that named class of restrictions (COR) apply to dial peers. |
| dial-peer cor list | Defines a class of restrictions (COR) list name. |

| Command | Description |
|---|---|
| disable-early-media 180 | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies which call treatment, early media or local ringback, is provided for 180 responses with 180 responses with Session Description Protocol (SDP). |
| dspfarm profile | Enters DSP farm profile configuration mode and defines a profile for DSP farm services. |
| dtmf-interworking | Enables a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets sent from CUBE, and generates RFC 4733 compliance RTP Named Telephony Event (NTE) packets from CUBE. |
| early-media update block | Blocks the UPDATE requests with the Session Description Protocol (SDP) in an early dialog. |
| early-offer | Forces CUBE to send a SIP invite with Early Offer on the Out Leg. |
| emergency | Configures a list of emergency numbers. |
| error-code-override | Configures the SIP error code to be used at the dial peer. |
| error-passthru | Enables the passage of error messages from the incoming SIP leg to the outgoing SIP leg. |
| g729-annexb override | Configures the settings for G.729 codec interoperability and overrides the default value if the annexb attribute is not present. |
| gcid | Enables Global Call ID (GCID) for every call on an outbound leg of a VoIP dial peer for a SIP endpoint. |
| gw-accounting | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables an accounting method for collecting call detail records (CDRs). |
| handle-replaces | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a Cisco IOS device to handle SIP INVITE with Replaces header messages at the SIP protocol level. |
| header-passing | Enables the passing of headers to and from SIP INVITE, SUBSCRIBE, and NOTIFY messages. |
| host-registrar | Populates the sip-ua registrar domain name or IP address value in the host portion of the diversion header and redirects the contact header of the 302 response. |
| http client connection idle timeout | Sets the number of seconds for which the HTTP client waits before terminating an idle connection. |

| Command | Description |
|---|---|
| http client connection persistent | Enables HTTP persistent connections so that multiple files can be loaded by using the same connection. |
| http client connection timeout | Sets the number of seconds for which the HTTP client waits for a server to establish a connection before abandoning its connection attempt. |
| ip qos dscp | Configures the DSCP value for QoS. |
| localhost | Globally configures CUBE to substitute a DNS hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages. |
| max-conn | Specifies the maximum number of incoming or outgoing connections for a particular VoIP dial peer. |
| max-forwards | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Globally sets the maximum number of hops, that is, proxy or redirect servers that can forward the SIP request. |
| media | Enables media packets to pass directly between endpoints without the intervention of CUBE, and enables signaling services. |
| media disable-detailed-stats | Disables the collection of detailed call statistics. |
| media profile asp | Creates a media profile to configure acoustic shock-protection parameters. |
| media profile nr | Creates a media profile to configure noise-reduction parameters. |
| media profile stream-service | Enables stream service on CUBE. |
| media profile video | Creates a media profile video. |
| media-address voice-vrf | Associates an RTP port range with VRF. |
| media-inactivity-criteria | Specifies the mechanism for detecting media inactivity (silence) on a voice call. |
| midcall-signaling | Configures the method that is used for signaling messages. |
| min-se | Changes the minimum session expiration (Min-SE) header value for all the calls that use the SIP session timer. |
| nat | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Uses SIP Network Address Translation (NAT) global configuration. |
| nat media-keepalive | Enables media keepalive packet transmission for the specified interval of time. |

| Command | Description |
|---|---|
| notify redirect | Enables application handling of redirect requests for all VoIP dial peers. |
| notify ignore substate | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies Ignoring the Subscription-State header in a Notify message. |
| notify telephone-event | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the maximum interval between two consecutive NOTIFY messages for a particular telephone event. |
| num-exp | Defines how to expand a telephone extension number into a particular destination pattern. |
| options-ping | Enables in-dialog options. |
| outbound-proxy | Configures a SIP outbound proxy for outgoing SIP messages globally. |
| pass-thru content | Enables the pass-through of SDP from in-leg to the out-leg. |
| permit hostname | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Stores hostnames used during validation of initial incoming INVITE messages. |
| privacy | Sets privacy support at the global level as defined in RFC 3323. |
| privacy-policy | Configures the privacy header policy options at the global level. |
| progress_ind | Configures an outbound dial peer on a CUBE to override and remove or replace the default progress indicator in specified call messages. |
| protocol mode | Configures the Cisco IOS SIP stack. |
| random-contact | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Populates an outgoing INVITE message with random-contact information instead of clear-contact information. |
| reason-header override | Enables cause code passing from one SIP leg to another. |
| redirect ip2ip | Redirects SIP phone calls to SIP phone calls globally on a gateway. |
| redirection | Enables the handling of 3*xx* redirect messages |
| referto-passing | Disables dial peer lookup and modification of the Refer-To header when the CUBE passes across a REFER message during a call transfer. |

| Command | Description |
|---|---|
| registrar | Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar. |
| rel1xx | Enables SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint. |
| remote-party-id | Enables translation of the Remote-Party-ID SIP header. |
| requri-passing | Enables pass-through of the host part of the Request-URI and To SIP headers. |
| retry bye | Configures the number of times that a BYE request is retransmitted to the other user agent. |
| retry invite | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the number of times that a SIP INVITE request is retransmitted to the other user agent. |
| rtcp all-pass-through | Passes through all the RTCP packets in the datapath. |
| rtcp keepalive | Configures RTCP keepalive report generation and generates RTCP keepalive packets. |
| rtp payload-type | Identifies the payload type of an RTP packet. |
| rtp-media-loop count | Configures the number of media loops before RTP voice and video media packets are dropped. |
| rtp-port | Configures the real-time protocol range. |
| rtp-ssrc multiplex | Multiplexes RTCP packets with RTP packets and sends multiple synchronization source in RTP headers (SSRCs) in an RTP session. |
| secure-ciphersuite | Configures the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE. |
| session refresh | Enables SIP session refresh globally. |
| session transport | Configures a VoIP dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages. |
| set pstn-cause | Maps an incoming PSTN cause code to a SIP error status code. |
| set sip-status | Maps an incoming SIP error status code to a PSTN cause code. |
| signaling forward | Configures global settings for transparent tunneling of QSIG, Q.931, H.225, and ISUP messages. |
| silent discard untrusted | Discards SIP requests from untrusted sources in an incoming SIP trunk. |

| Command | Description |
|---|---|
| sip-server | Configures a network address for the SIP server interface. |
| srtp | Specifies that SRTP be used to enable secure calls and call fallback. |
| srtp negotiate | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables the Cisco IOS Session Initiation Protocol (SIP) gateway to accept and send a Real-Time Transport Protocol (RTP) Audio/Video Profile (AVP) at the global configuration level. |
| stun | Enters STUN configuration mode for configuring firewall traversal parameters. |
| stun flowdata shared-secret | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a secret shared on a call control agent. |
| stun usage firewall-traversal flowdata | Enables firewall traversal using STUN. |
| supplementary-service media-renegotiate | Globally enables midcall media renegotiation for supplementary services. |
| timers | Configures SIP-signaling timers. |
| transport | Configures the SIP user agent (gateway) for SIP signaling messages in inbound calls through the SIP TCP, TLS over TCP, or UDP socket.<br>This command supports TLS version 1.3 and all associated ciphers. |
| uc secure-wsapi | Configures a secure Cisco Unified Communication IOS services environment for a specific application. |
| uc wsapi | Configures a nonsecure Cisco Unified Communication IOS services environment for a specific application. |
| update-callerid | Enables sending updates for caller IDs. |
| url (SIP) | Configures URLs to either the SIP, SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls. |
| vad | Enables VAD for calls using a specific dial peer. |
| video codec | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies a video codec for a voice class. |
| voice cause code | Sets the internal Q850 cause code mapping for, voice and enters voice cause configuration mode. |
| voice class codec | Enters voice-class configuration mode and assigns an identification tag number for a codec voice class. |

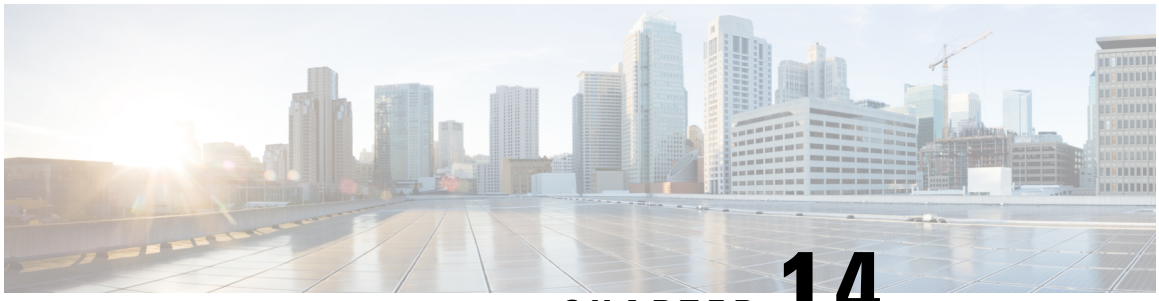
| Command | Description |
|---|---|
| voice class dpg | Creates a dial-peer group for grouping multiple outbound dial peers. |
| voice class e164-pattern-map | Creates an E.164 pattern map that specifies multiple destination E.164 patterns in a dial peer. |
| voice class media | Configures media control parameters for voice. |
| voice class server-group | Enters voice-class configuration mode and configures server groups (groups of IPv4 and IPv6 addresses) that can be referenced from an outbound SIP dial peer. |
| voice-class sip options-keepalive | Monitors connectivity between CUBE VoIP dial peers and SIP servers. |
| voice class sip-copylist | Configures a list of entities to be sent to the peer call leg. |
| voice class sip-event-list | Configures a list of SIP events to be passed through. |
| voice class sip-hdr-passthrulist | Configures a list of headers to be passed through the route string. |
| voice-class sip nat media-keepalive | Configures media keepalive to enable media keepalive packets to be transmitted for the interval specified. |
| voice class sip-profiles | Configures SIP profiles for a voice class. |
| voice class srtp-crypto | Enters voice class configuration mode and assigns an identification tag for an **srtp-crypto voice class** command. |
| voice class uri | Creates or modifies a voice class for matching dial peers to a SIP or TEL URI. |
| voice class tls-cipher | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures an ordered set of TLS cipher suites. |
| voice class tls-profile | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables voice class configuration mode, and assigns an identification tag for a TLS profile. |
| voice iec syslog | Enables viewing of internal error codes as they are encountered in real time. |
| voice statistics iec | Enables collection of internal error code statistics. |
| xfer target | Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Routes the INVITE to the refer-to destination in the REFER consume case. The routing decision is made based on the xfer target destination. |

# SRST Commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for SRST. Click a command name in the **Command** column to view information about the command, its syntax, and its use.

***Table 114: Cisco Catalyst SD-WAN CLI Template Commands for SRST***

| Command | Description |
|---|---|
| http client secure-ciphersuite | Sets the secure encryption cipher suite for the HTTP client. |
| transport-tcp-tls (call-manager-fallback) | Configures a specific TLS version for Unified Secure SCCP SRST, in call-manager-fallback mode. |



CHAPTER 14

# Configure Network Interfaces

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

In the Cisco Catalyst SD-WAN overlay network design, interfaces are associated with VPNs. The interfaces that participate in a VPN are configured and enabled in that VPN. Each interface can be present only in a single VPN.

At a high level, for an interface to be operational, you must configure an IP address for the interface and mark it as operational (**no shutdown**). In practice, you always configure additional parameters for each interface.

You can configure up to 512 interfaces on a Cisco IOS XE Catalyst SD-WAN device. This number includes physical interfaces, loopback interfaces, and subinterfaces.

**Note** To maximize the efficiency of the load-balancing among Cisco Catalyst SD-WAN Controllers, use sequential numbers when assigning system IP addresses to the Cisco IOS XE Catalyst SD-WAN devices in the domain. Example of a sequential numbering schemes is 172.16.1.1, 172.16.1.2, 172.16.1.3, and so on.

**Note** Ensure that any network interface configured on a device has a unique IP address.


- Configure VPN, on page 580
- Configure Interfaces in the WAN Transport VPN (VPN 0), on page 584
- Configure the System Interface, on page 591
- Configure Control Plane High Availability, on page 592
- Configure Other Interfaces, on page 592
- Configure Interface Properties, on page 599

- Enable DHCP Server using Cisco SD-WAN Manager, on page 615
- Configuring PPPoE, on page 618
- Configure PPPoE Over ATM, on page 622
- Configuring VRRP , on page 624
- Configuring Dynamic Interfaces, on page 626
- Configure VPN Ethernet Interface, on page 628
- VPN Interface Bridge, on page 638
- VPN Interface DSL IPoE, on page 643
- VPN Interface DSL PPPoA, on page 654
- VPN Interface DSL PPPoE, on page 662
- VPN Interface Ethernet PPPoE, on page 672
- Cisco VPN Interface GRE, on page 680
- GRE-in-UDP, on page 683
- VPN Interface IPsec , on page 684
- VPN Interface Multilink, on page 692
- Configure VPN Interface SVI using Cisco SD-WAN Manager, on page 700
- VPN Interface T1/E1, on page 704
- Cellular Interfaces, on page 712


# Configure VPN

## VPN

Use the VPN template for all Cisco Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

To configure VPNs using Cisco SD-WAN Manager templates, follow this general workflow:

1. Create VPN feature templates to configure VPN parameters. You create a separate VPN feature template for each VPN. For example, create one feature template for VPN 0, a second for VPN 1, and a third for VPN 512.

   For Cisco SD-WAN Manager Network Management Systems and Cisco Catalyst SD-WAN Controllers, you can configure only VPNs 0 and 512. Create templates for these VPNs only if you want to modify the default settings for the VPN. For Cisco IOS XE Catalyst SD-WAN devices, you can create templates for these two VPNs and for additional VPN feature templates to segment service-side user networks.

   - **VPN 0**—**Transport VPN**, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
   - **VPN 512**—**Management VPN**, which carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices. For controller devices, by default, VPN 512 is not configured.
   - **VPNs 1**–**511**, **513**–**65530**—**Service VPNs,** for service-side data traffic on Cisco IOS XE Catalyst SD-WAN devices.

2. Create interface feature templates to configure the interfaces in the VPN.

# Create a VPN Template

**Note** Cisco IOS XE Catalyst SD-WAN devices use VRFs for segmentation and network isolation. However, the following steps still apply if you are configuring segmentation for Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. When you complete the configuration, the system automatically converts the VPNs to VRFs for Cisco IOS XE Catalyst SD-WAN devices.

**Note** You can configure a static route through the VPN template.

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

**Step 2** Click **Device Templates**, and click **Create Template**.

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

**Step 3** From the **Create Template** drop-down list, choose **From Feature Template**.

**Step 4** From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.

**Step 5** To create a template for VPN 0 or VPN 512:

**a.** Click **Transport & Management VPN**, or scroll to the **Transport & Management VPN** section.

**b.** From the VPN 0 or VPN 512 drop-down list, click **Create Template**. The VPN template form appears.

The form contains fields for naming the template, and fields for defining VPN parameters.

**Step 6** To create a template for VPNs 1 through 511, and 513 through 65527:

**a.** Click **Service VPN**, or scroll to the **Service VPN** section.

**b.** Click the **Service VPN** drop-down list.

**c.** From the **VPN** drop-down list, click **Create Template**. The VPN template form displays.

The form contains fields for naming the template, and fields for defining VPN parameters.

**Step 7** In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

**Step 8** In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

# Changing the Scope for a Parameter Value

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

| Parameter Name | Description |
|---|---|
| Device Specific | 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.<br>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 Create a Template Variables Spreadsheet<br>**Note** When you are using a CSV file for configuring device-specific variables in the device attach flow, ensure to fill all the mandatory fields before uploading.<br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global | Enter a value for the parameter, and apply that value to all devices.<br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

Once you have created and named the template, enter the following values. Parameters marked with an asterisk are required.

# Configure Basic VPN Parameters

To configure basic VPN parameters, choose **Basic Configuration** and then configure the following parameters. Parameters marked with an asterisk are required to configure a VPN.

| Parameter Name | Description |
|---|---|
| VPN | Enter the numeric identifier of the VPN.<br>Range for Cisco IOS XE Catalyst SD-WAN devices: 0 through 65527<br>Values for Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager devices: 0, 512 |

| Parameter Name | Description |
|---|---|
| Name | Enter a name for the VPN.<br>**Note** For Cisco IOS XE Catalyst SD-WAN devices, you can't enter a device-specific name for the VPN. |
| Enhance ECMP keying | Click **On** to enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source, and destination IP addresses, as the ECMP hash key.<br>ECMP keying is **Off** by default. |

**Note** To complete the configuration of the transport VPN on a router, you must configure at least one interface in VPN 0.

To save the feature template, click **Save**.

### Configure Load-Balancing Algorithm Using the CLI

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, you need CLI template to configure the **src-only** load-sharing algorithm for IPv4 and IPv6 Cisco Catalyst SD-WAN and non Cisco Catalyst SD-WAN traffic. For complete details on the load-sharing algorithm CLI, see IP Commands list.

This following provides CLI configurations for selecting a Cisco Express Forwarding load-balancing algorithm for non Cisco Catalyst SD-WAN IPv4 and IPv6 traffic. You can enable ECMP keying to send the configurations for both IPv4 and IPv6.

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm {universal [id] | include-ports [ source [id]
 | destination [id]] |
src-only [id]}

Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm {universal [id] | include-ports [ source
[id] | destination [id]] |
src-only [id]}
```

This following provides CLI configurations for enabling load balancing algorithm on an interface for Cisco Catalyst SD-WAN IPv4 and IPv6 traffic. You can enable ECMP keying to send the configurations for both IPv4 and IPv6.

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}

Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

# Configure DNS and Static Hostname Mapping

To configure DNS addresses and static hostname mapping, click **DNS** and configure the following parameters:

| Parameter Name | Options | Description |
|---|---|---|
| **Primary DNS Address** | Click either **IPv4** or **IPv6**, and enter the IP address of the primary DNS server in this VPN. | |
| **New DNS Address** | Click **New DNS Address** and enter the IP address of a secondary DNS server in this VPN. This field appears only if you have specified a primary DNS address. | |
| | **Mark as Optional Row** | Check the **Mark as Optional Row** check box to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. |
| | **Hostname** | Enter the hostname of the DNS server. The name can be up to 128 characters. |
| | **List of IP Addresses** | Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas. |
| To save the DNS server configuration, click **Add**. | | |

To save the feature template, click **Save**.

### Mapping Host Names to IP Addresses

```
! IP DNS-based host name-to-address translation is enabled
  ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
  ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
  ip domain name cisco.com
```

# Configure Interfaces in the WAN Transport VPN (VPN 0)

This topic describes how to configure the general properties of WAN transport and service-side network interfaces. For information about how to configure specific interface types and properties—including cellular interfaces, DHCP, PPPoE, VRRP, and WLAN interfaces.

VPN 0 is the WAN transport VPN. This VPN handles all control plane traffic, which is carried over OMP sessions, in the overlay network. For a Cisco IOS XE Catalyst SD-WAN device device to participate in the overlay network, at least one interface must be configured in VPN 0, and at least one interface must connect to a WAN transport network, such as the Internet or an MPLS or a metro Ethernet network. This WAN transport interface is referred to as a tunnel interface. At a minimum, for this interface, you must configure an IP address, enable the interface, and set it to be a tunnel interface.

To configure a tunnel interface on a Cisco Catalyst SD-WAN Controller or a Cisco SD-WAN Manager, you create an interface in VPN 0, assign an IP address or configure the interface to receive an IP address from DHCP, and mark it as a tunnel interface. The IP address can be either an IPv4 or IPv6 address. To enable dual stack, configure both address types. You can optionally associate a color with the tunnel.

**Note** You can configure IPv6 addresses only on transport interfaces in VPN 0 and but not supported in VPN 512.

Tunnel interfaces on Cisco IOS XE Catalyst SD-WAN devices must have an IP address, a color, and an encapsulation type. The IP address can be either an IPv4 or IPv6 address. To enable dual stack in releases before Cisco IOS XE Catalyst SD-WAN Release 17.3.2, configure both address types.

To use dual stack with Cisco IOS XE Catalyst SD-WAN devices from Cisco IOS XE Catalyst SD-WAN Release 17.3.2, configure all controllers with both IPv4 and IPv6 addresses. In addition, configure DNS for the Cisco Catalyst SD-WAN Validator interface to resolve IPv4 and IPv6 address types so that controllers can reach the Cisco Catalyst SD-WAN Validator through either IP address type.

**Note** Starting from Cisco vManage Release 20.6.1, in case of a dual-stack configuration, if an IPv4 address or the fully qualified domain name (FQDN) is not available, but an IPv6 address is available, then the IPv6 address is used to connect to the Cisco Catalyst SD-WAN Validator.

For the tunnel interface, you can configure a static IPv4 or IPv6 address, or you can configure the interface to receive its address from a DHCP server. To enable dual stack, configure both an IPv4 and an IPv6 address on the tunnel interface.

From Cisco IOS XE Catalyst SD-WAN Release 17.3.2, Cisco IOS XE Catalyst SD-WAN devices do not support dual stack on the same TLOC or interface. Only one address type can be provisioned for a TLOC or interface. Using a second address type requires a second TLOC or interface on which it can be provisioned.

On Cisco Catalyst SD-WAN Controllers and Cisco Catalyst SD-WAN Controller NMSs, *interface-name* can be either **eth** *number* or **loopback** *number*. Because Cisco Catalyst SD-WAN Controllers and Cisco Catalyst SD-WAN Controller NMSs participate only in the overlay network's control plane, the VPNs that you can configure on these devices are VPN 0 and VPN 512. Hence, all interfaces are present only on these VPNs.

To enable the interface, include the **no shutdown** command.

Color is a Cisco Catalyst SD-WAN software construct that identifies the transport tunnel. It can be **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. The colors **metro-ethernet**, **mpls**, and **private1** through **private6** are referred to as *private colors*, because they use private addresses to connect to the remote side Cisco IOS XE Catalyst SD-WAN device in a private network. You can use these colors in a public network provided that there is no NAT device between the local and remote Cisco IOS XE Catalyst SD-WAN devices.

To limit the remote TLOCs that the local TLOC can establish BFD sessions with, mark the TLOC with the **restrict** option. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color.

**Note** When a WAN edge device is configured with two IPv6 TLOCs, one with static default route and the other one with IPv6 address autoconfig default which is the IPv6 neighbor discovery default route, the IPv6 neighbor discovery default route is not installed in the routing table. In this case, the IPv6 TLOC with IPv6 neighbor discovery default route does not work.

For IPv6 TLOC with IPv6 neighbor discovery default route to work, you can configure the static route for TLOC with IPv6 neighbor discovery to overwrite the IPv6 neighbor discovery default route and ensure that both the static routes are installed into the routing table. You can also use the IPv6 neighbor discovery default route on all interfaces.

On a Cisco Catalyst SD-WAN Controller or Cisco Catalyst SD-WAN Controller NMS, you can configure one tunnel interface. On a Cisco IOS XE Catalyst SD-WAN device, you can configure up to eight tunnel interfaces.

On Cisco IOS XE Catalyst SD-WAN devices, you must configure the tunnel encapsulation. The encapsulation can be either IPsec or GRE. For IPsec encapsulation, the default MTU is 1442 bytes, and for GRE it is 1468 bytes, These values are a function of overhead required for BFD path MTU discovery, which is enabled by default on all TLOCs. (For more information, see Configuring Control Plane and Data Plane High Availability Parameters.) You can configure both IPsec and GRE encapsulation by including two **encapsulation** commands under the same **tunnel-interface** command. On the remote Cisco IOS XE Catalyst SD-WAN device, you must configure the same tunnel encapsulation type or types so that the two routers can exchange data traffic. Data transmitted out of an IPsec tunnel can be received only by an IPsec tunnel, and data sent on a GRE tunnel can be received only by a GRE tunnel. The Cisco Catalyst SD-WAN software automatically selects the correct tunnel on the destination Cisco IOS XE Catalyst SD-WAN device.

A tunnel interface allows only DTLS, TLS, and, for Cisco IOS XE Catalyst SD-WAN devices, IPsec traffic to pass through the tunnel. To allow additional traffic to pass without having to create explicit policies or access lists, enable them by including one **allow-service** command for each service. You can also explicitly disallow services by including the **no allow-service** command. Note that services affect only physical interfaces. You can allow or disallow these services on a tunnel interface:

| Service | Cisco Catalyst SD-WAN Controller | Cisco Catalyst SD-WAN Controller |
|---|---|---|
| **all** (Overrides any commands that allow or disallow individual services) | X | X |
| **bgp** | — | — |
| **dhcp** (for DHCPv4 and DHCPv6) | — | — |
| **dns** | — | — |
| **https** | X | — |
| **icmp** | X | X |
| **netconf** | X | — |
| **ntp** | — | — |
| **ospf** | — | — |

| Service | Cisco Catalyst SD-WAN Controller | Cisco Catalyst SD-WAN Controller |
|---|---|---|
| **sshd** | X | X |
| **stun** | X | X |

The **allow-service stun** command pertains to allowing or disallowing a Cisco IOS XE Catalyst SD-WAN device to generate requests to a generic STUN server so that the device can determine whether it is behind a NAT and, if so, what kind of NAT it is and what the device's public IP address and public port number are. On a Cisco IOS XE Catalyst SD-WAN device that is behind a NAT, you can also have tunnel interface to discover its public IP address and port number from the Cisco Catalyst SD-WAN Validator.

With this configuration, the Cisco IOS XE Catalyst SD-WAN device uses the Cisco Catalyst SD-WAN Validator as a STUN server, so the router can determine its public IP address and public port number. (With this configuration, the router cannot learn the type of NAT that it is behind.) No overlay network control traffic is sent and no keys are exchanged over tunnel interface configured to the the Cisco Catalyst SD-WAN Validator as a STUN server. However, BFD does come up on the tunnel, and data traffic can be sent on it. Because no control traffic is sent over a tunnel interface that is configured to use the Cisco Catalyst SD-WAN Validator as a STUN server, you must configure at least one other tunnel interface on the Cisco IOS XE Catalyst SD-WAN device so that it can exchange control traffic with the Cisco Catalyst SD-WAN Controller and the Cisco Catalyst SD-WAN Controller NMS.

You can log the headers of all packets that are dropped because they do not match a service configured with an **allow-service** command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

# TLOC Extension

There are scenarios when Cisco IOS XE Catalyst SD-WAN devices cannot connect to a single transport directly and only one device can connect to a single transport. A switch is connected to each transport and the devices connect to each transport through the switches. To have a set-up with the switch option at a branch increases the cost of the solution and result in managing another device. TLOC extension enables a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.

## TLOC Extension Over IPv6

***Table 115: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| TLOC Extension Over IPv6 | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>Cisco vManage Release 20.11.1 | This feature enables the support of TLOC extension for IPv6. In the previous releases, TLOC extension was supported only for IPv4. |

### Information About TLOC Extension Over IPv6

In the earlier releases, TLOC extension was supported only over IPv4 interfaces.

This feature supports the following requirements:

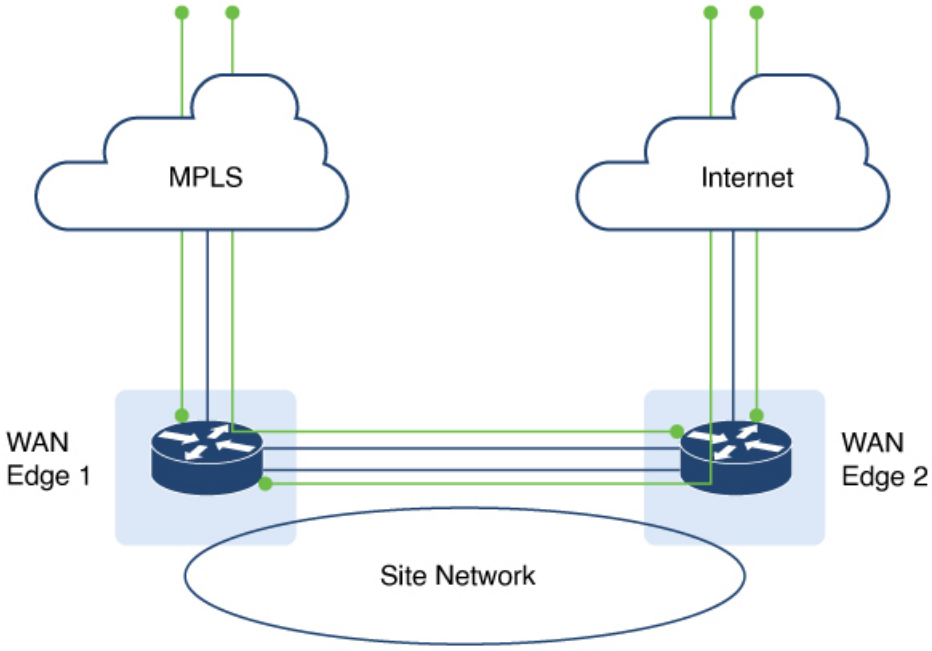
- TLOC extension over IPv6 works only if the underlay supports IPv6 addressing on both the Cisco IOS XE Catalyst SD-WAN devices connecting each other.
- Implicit IPv6 ACL on TLOC tunnel interface is supported.
- IPv6 TLOC has dual stack support. When both IPv4 and IPv6 are configured, the tunnel is built on top of either IPv4 or IPv6, based on the configuration.
- TLOC interface supports NAT66. The limitations of NAT66 also applies to the TLOC extended interface.
- The following interface types supports IPv6 TLOC extension:
  - Physical interface
  - Physical sub-interface
  - Loopback interface

**Note** Only the Layer 2 setup supports IPv6 TLOC extension.

- This feature is supported for both private and public color TLOC interfaces.
- This feature supports the loopback TLOC interface that is bound to either:
  - The WAN transport circuit.
  - An extended WAN interface between two Cisco IOS XE Catalyst SD-WAN devices.

### Use Case for TLOC Over IPv6 Extension

*Figure 4: TLOC Extension*




The TLOC extension allows each Cisco IOS XE Catalyst SD-WAN device to access the opposite transport through a TLOC-extension interface on the neighboring SD-WAN device. In the diagram, SD-WAN device 1 can access the internet through the SD-WAN device 2 TLOC extension interface in addtion to the direct MPLS connection. SD-WAN device 2 can access the MPLS transport through the SD-WAN device 1 TLOC extension interface in addition to the direct internet connetion. TLOC extension over IPv6 achieves redundancy in a dual-device deployment scenario with only one circuit connection on each device.

### Limitations for TLOC Extension Over IPv6

- SIG is not supported on the IPv6 TLOC extension.
- NAT64 is not supported for IPv6 TLOC extension.
- TLOC extension over IPv6 is not supported for Layer 3 connections.

When a TLOC configuration is extended to a peer interface and then to ISP, the extended control connections are still up on the peer interface, even after removing TLOC Extension configuration.

In TLOC-Extension, the extender interface is part of the Cisco Catalyst SD-WAN. However, the tunnel-interface configuration under the extender interface is optional.

## Configure TLOC Extension

1. Enter global configuration mode, and configure an interface.

   ```
   Device# config-transaction
   ```

2. Enter SD-WAN configuration mode.

```
Device(config)# sdwan
```

3. In the SD-WAN configuration mode, configure an interface type such as, Gigabit Ethernet.

```
Device(config-sdwan)# interface GigabitEthernet3
```

4. Configure tunnel interface.

```
Device(config-interface-GigabitEthernet3)# tunnel-interface
```

5. Configure encapsulation, color, allowed services for TLOC.

```
Device(config-interface-GigabitEthernet3)# tunnel-interface
Device(config-interface-GigabitEthernet3)# encapsulation ipsec
Device(config-interface-GigabitEthernet3)# color color
Device(config-interface-GigabitEthernet3)# exit
```

6. In the global configuration mode, configure an interface.

```
Device# config-transaction
Device(config)# ip route 0.0.0.0 0.0.0.0 ip-address
```

7. On device 2, the LTE WAN connection is on GigabitEthernet1 and this transport is extended to device 1 GigabitEthernet3 TLOC interface.

```
Device(config-sdwan)# tloc-extension GigabitEthernet1
```

8. Configure NAT routes on GigabitEthernet1 for data traffic to reach back to device 1 through device 2 for GigabitEthernet3 subnet.

The following example describes how TLOC extension is configured on a network interface.

```
On Device1,
Configure TLOC interface on VPN 0
sdwan
interface GigabitEthernet3
  tunnel-interface
   encapsulation ipsec
   color custom1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no 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

  Configure default route via this TLOC interface with nexthop
  to L2 connected interface of the peer (ED2 Gig3).

  ip route 0.0.0.0 0.0.0.0 10.1.19.16

 On Device2,
LTE WAN connection is on Gig1 and this transport is extended to ED1 Gig3 TLOC
interface(custom1).
 sdwan
 int GigabitEthernet3
 tloc-extension GigabitEthernet1
```

```
Configure NAT routes on Gig1 or appropriate routes for data traffic to reach back to ED1
via ED2 for Gig3 subnet.
```

## Verify TLOC Extension

The following is a sample output of the commands to verify if TLOC extension is configured on a network interface.

```
Device# show sdwan control connections
PEER                                        PEER
  CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                  PRIV
  PEER
PUB                                         GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                            PORT
  PUBLIC IP
PORT  ORGANIZATION             LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------------
vsmart  dtls 172.16.255.19   100        1      2001:a0:5::13
12455 2001:a0:5::13                           12455 vIPtela Inc Regression  custom1
      No    up
0:01:23:06 0
vsmart  dtls 172.16.255.20   200        1      2001:a0:c::14                          12456
2001:a0:c::14                             12456 vIPtela Inc Regression  custom1
No    up
0:01:23:06 0
```

```
Device# show sdwan bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
DST PUBLIC                        DST PUBLIC         DETECT      TX
  SYSTEM IP        SITE ID     STATE       COLOR            COLOR             SOURCE IP
IP                                          PORT        ENCAP  MULTIPLIER  INTERVAL(msec
  UPTIME
TRANSITIONS
-------------------------------------------------------------------------------------------------
172.16.255.14    400         up          custom1            lte             2001:a0:15::10
2001:a1:e::e                                12346       ipsec  7           1000
0:00:05:50  3
```

# Configure the System Interface

For each Cisco IOS XE Catalyst SD-WAN device, you configure a system interface with the **system system-ip** command. The system interface's IP address is a persistent address that identifies the Cisco IOS XE Catalyst SD-WAN device. It is similar to a router ID on a regular router, which is the address used to identify the router from which packets originated.

Specify the system IP address as an IPv4 address in decimal four-part dotted notation. Specify just the address; the prefix length (/32) is implicit.

The system IP address can be any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, and 224.0.0.0/4, and 240.0.0.0/4 and later. Each device in the overlay network must have a unique system IP address. You cannot use this same address for another interface in VPN 0.

The system interface is placed in VPN 0, as a loopback interface named **system**. Note that this is not the same as a loopback address that you configure for an interface.

To display information about the system interface, use the **show interface** command. For example:

The system IP address is used as one of the attributes of the OMP TLOC. Each TLOC is uniquely identified by a 3-tuple comprising the system IP address, a color, and an encapsulation. To display TLOC information, use the **show omp tlocs** command.

For device management purposes, it is recommended as a best practice that you also configure the same system IP address on a loopback interface that is located in a service-side VPN that is an appropriate VPN for management purposes. You use a loopback interface because it is always reachable when the router is operational and when the overlay network is up. If you were to configure the system IP address on a physical interface, both the router and the interface would have to be up for the router to be reachable. You use a service-side VPN because it is reachable from the data center. Service-side VPNs are VPNs other than VPN 0 (the WAN transport VPN) and VPN 512 (the management VPN), and they are used to route data traffic.

# Configure Control Plane High Availability

A highly available Cisco Catalyst SD-WAN network contains two or more Cisco Catalyst SD-WAN Controllers in each domain. A Cisco Catalyst SD-WAN domain can have up to eight Cisco Catalyst SD-WAN Controllers, and each Cisco IOS XE Catalyst SD-WAN device, by default, connects to two of them. You change this value on a per-tunnel basis:

# Configure Other Interfaces

### Configure Interfaces in the Management (VRF mgmt-intf)

On all Cisco Catalyst SD-WAN devices, VPN 512 is used for out-of-band management, by default as part of the factory-default configuration. On Cisco IOS XE Catalyst SD-WAN devices the management VPN is converted to VRF Mgmt-Intf.

Cisco XE SD-WAN devices use VRFs in place of VPNs.

```
Device# show sdwan running-config | sec vrf definition Mgmt-intf

vrf definition Mgmt-intf
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
============
interface GigabitEthernet0
 no shutdown
 vrf forwarding Mgmt-intf
 negotiation auto
exit
============
config-t
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0

vrf definition Mgmt-intf
 rd 1:512
 !
 address-family ipv4
  route-target export 1:512
  route-target import 1:512
 exit-address-family
```

```
 !
 address-family ipv6
 exit-address-family
!
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 192.168.20.11 255.255.255.0
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0
!
```

To display information about the configured management interfaces, use the **show interface** command. For example:

```
Device# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 8000 bits/sec, 12 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     4839793 packets input, 415574814 bytes, 0 no buffer
     Received 3060073 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     82246 packets output, 41970224 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

**Note** VPN 512 is not advertised in the overlay. It is local to the device. If you need a management VPN that is reachable through the overlay, create a VPN with a number other than 512.

# Configure Loopback Interfaces

Use the interface name format **loopback** *string*, where *string* can be any alphanumeric value and can include underscores (_) and hyphens (–). The total interface name, including the string "loopback", can be a maximum of 16 characters long. (Note that because of the flexibility of interface naming in the CLI, the interfaces **lo0** and **loopback0** are parsed as different strings and as such are not interchangeable. For the CLI to recognize as interface as a loopback interface, its name must start with the full string **loopback**.)

One special use of loopback interfaces is to configure data traffic exchange across private WANs, such as MPLS or metro Ethernet networks. To allow a router that is behind a private network to communicate directly over the private WAN with other edge routers, you direct data traffic to a loopback interface that is configured as a tunnel interface rather than to an actual physical WAN interface.

# Implicit ACL on Loopback Interfaces

*Table 116: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Implicit ACL on Loopback Interfaces | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1 | This feature allows you to enable implicit ACL on loopback TLOC interfaces.<br>When a loopback TLOC interface has its own implicit ACL, ACL rules are applied on the traffic destined for the interface. With implicit ACL enabled on the loopback TLOC interface, only limited services can be allowed, thereby enhancing your network security.<br>When a loopback TLOC interface is bound to a physical interface on a Cisco IOS XE Catalyst SD-WAN device, the physical interface is treated like a physical TLOC interface. |

## Information About Implicit ACL on Loopback Interfaces

Access lists that you configure using localized data policy are called Explicit ACLs. Router tunnel interfaces also have implicit ACLs, which are also referred to as Services. Some of these are present by default on the tunnel interface, and they are in effect until you disable them. Through configuration, you can also enable other implicit ACLs. On Cisco IOS XE Catalyst SD-WAN devices, the following services are enabled by default: DHCP, DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

You can configure and modify implicit ACLs with the **allow-service** command to allow a service. Use the **no allow-service** command to disallow a service. If both implicit ACL and explicit ACL are configured, explicit ACL takes precedence over the implicit ACL.

When Cisco IOS XE Catalyst SD-WAN device loopback interfaces are configured with a Transport Location (TLOC), implicit ACL rules are applied to the traffic destined for it. Implicit ACL on loopback interfaces are applied both in a bind mode and in an unbind mode. A bind mode is where a loopback interface is bound to a physical interface on a Cisco IOS XE Catalyst SD-WAN device to send data. In an unbind mode, a loopback interface is not bound to any physical interface.

### Loopback TLOC Interface Bound to a Physical WAN Interface

When a loopback interface is a TLOC and is bound to a physical WAN interface, the corresponding implicit ACL rules are applied based on where the traffic is destined:

- If the traffic that is destined to the loopback TLOC interface is received on a physical WAN interface, the implicit ACL rules configured on the loopback TLOC interface is applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured with a TLOC, then routing decisions apply.

**Note** Use this command **implicit-acl-on-bind-intf** to enable implicit ACL protection on a physical interface in cases where a physical interface is not configured with a TLOC and bound to the loopback TLOC interface.

Forwarded or passthrough packets are dropped when a loopback TLOC interface is bound to a physical WAN interface—the same behavior as when a physical interface is configured as a TLOC. Therefore, explicit ACL must be configured on the bound physical interface to forward packets.

An explicit ACL is necessary to allow passthrough packets in the following sample scenarios:

- **Branch edge routers accessing controllers hosted in on-premises data centers**: This scenario presumes that the branch edge routers access the controllers through the data center hub, which is configured with a loopback interface bound to a physical WAN interface.
- **Branch routers accessing cloud-hosted controllers through data center internet circuits**: This scenario presumes that the branch routers are connected to the data center edge using an MPLS network. Such branch routers then access the cloud-hosted controllers through the data canter edge router, which is configured with a loopback interface bound to a physical WAN interface.

- If a physical WAN interface is configured with TLOC, implicit ACL rules of the physical TLOC interface apply. In both these scenarios explicit ACLs on the bound physical WAN interface are necessary to allow passthrough traffic.

### Loopback TLOC Interface Not Bound to a Physical WAN Interface

When a loopback interface is a TLOC, and is not bound to a physical WAN interface, implicit ACL rules are applied based on where the traffic is destined for:

- If the traffic that is destined for the loopback TLOC interface is received on a physical WAN interface, implicit ACL rules of the loopback TLOC are applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the input physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured for TLOC, then routing decisions apply.

- If the physical WAN interface is configured for TLOC, the configured implicit ACL rules apply.

The difference between the bind mode and the unbind mode for loopback TLOC is that in a bind mode the passthrough traffic is dropped because the bound physical interface is treated as a TLOC by itself. In an unbind mode, the passthrough traffic is allowed.

#### Example Using Bind Mode and Unbind Mode

**Bind Mode**

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 and Loopback2 configured as TLOCs and bound to the physical interface GigabitEthernet1. The device also has another interface, Loopback3, which is not configured as a TLOC.

Physical interface GigabitEthernet1 will be treated as a TLOC interface for incoming VPN 0.

To enable implicit ACL protection on physical interface GigabitEthernet1 for incoming VPN 0 traffic use the command **implicit-acl-on-bind-intf** .

In this example:

- If the traffic is destined for Loopback1, implicit ACL rules of Loopback1 are applied.
- If the traffic is destined for Loopback2, implicit ACL rules of Loopback2 are applied.
- If the traffic is destined for Loopback3 on GigabitEthernet1, traffic is allowed.
- If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

If the bound interface, GigabitEthernet1, is also configured as a TLOC, the traffic to Loopback3 will be subjected to implicit ACL rules on GigabitEthernet1.

**Unbind Mode**

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 configured as a TLOC and is in unbind mode. Loopback2 is not configured as a TLOC. The device also has GigabitEthernet1 interface, which is configured as a TLOC, and GigabitEthernet4 interface, which is not configured as a TLOC.

In this example:

- If the traffic destined for Loopback1 arrives at GigabitEthernet1, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied.
- If the traffic destined for Loopback1 arrives at GigabitEthernet4, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet4, traffic is allowed.
- If the traffic destined for Loopback2 arrives on GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied. If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

  If the traffic is destined for another device passing through GigabitEthernet4, the traffic is forwarded.

## Benefits of Implicit ACL on Loopback Interfaces

Implicit ACL on a loopback TLOC interface protects against denial of service (DoS) attacks by allowing only limited services. This enhances your network security.

# Configure Implicit ACL on Loopback Interfaces

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 Implicit ACL on Loopback Interfaces Using CLI

By default DNS, DHCP, ICMP and HTTPS services are permitted, and other services are denied.

To permit all the services, use the **allow-service** *all* command.

To permit a specific service, use the **allow-service** *service name* command.

To deny a service, use the **no allow-service** *service name* command.

### Example

The following example shows implicit ACL configured on a loopback interface.

```
sdwan interface Loopback100
  tunnel-interface
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
```

# Configuration Examples for Implicit ACL Configured on a Loopback Interface in Bind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in bind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# bind GigabitEthernet1
Device (config-tunnel-interface)# implicit-acl-on-bind-intf
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
```

```
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

## Configuration Examples for Implicit ACL Configured on a Loopback Interface in unbind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in unbind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

## Monitor Implicit ACL on Loopback Interfaces

Use the **show platform hardware qfp active statistics drop** command to monitor implicit ACL configuration on loopback interfaces.

### Example

The following is a sample output from the **show platform hardware qfp active statistics drop** command:

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never


-------------------------------------------------------------------------

Global Drop Stats                          Packets                 Octets

-------------------------------------------------------------------------

Disabled                                         4                    266

Ipv4EgressIntfEnforce                           15                  10968

Ipv6NoRoute                                      6                    336

Nat64v6tov4                                      6                    480

SVIInputInvalidMac                             244                  15886

SdwanImplicitAclDrop                           160                  27163

UnconfiguredIpv4Fia                         942525               58524580
```

```
UnconfiguredIpv6Fia                      77521               9587636
```

## Configure Subinterfaces

When you create a subinterface that does not specify an IP MTU value, the subinterface inherits the IP MTU value from the parent interface. If you want the subinterface to have a different IP MTU value, use the **ip mtu** command in the subinterface configuration to set the IP MTU for the sub interface.

For example:

```
interface GigabitEthernet0/0/0
 mtu 1504
 no ip address
!
interface GigabitEthernet0/0/0.9
 encapsulation dot1Q 9
 no shutdown
 ip address 192.168.9.32 255.255.255.0
!
interface Tunnel9
 no shutdown
 ip unnumbered GigabitEthernet0/0/0.9
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0.9
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0.9
 tunnel mode sdwan
!
sdwan
 interface GigabitEthernet0/0/0.9
  tunnel-interface
   encapsulation ipsec
   color private1
  !
 !
```

# Configure Interface Properties

## Set the Interface Speed

When a Cisco IOS XE Catalyst SD-WAN device comes up, the Cisco Catalyst SD-WAN software autodetects the SFPs present in the router and sets the interface speed accordingly. The software then negotiates the interface speed with the device at the remote end of the connection to establish the actual speed of the interface. To display the hardware present in the router, use the **show hardware inventory** command:

To display the actual speed of each interface, use the **show interface** command. Here, interface **ge0/0**, which connects to the WAN cloud, is running at 1000 Mbps (1Gbps; it is the 1GE PIM highlighted in the output above), and interface **ge0/1**, which connects to a device at the local site, has negotiated a speed of 100 Mbps.

For non-physical interfaces, such as those for the system IP address and loopback interfaces, the interface speed is set by default to 10 Mbps.

To override the speed negotiated by the two devices on the interface, disable autonegotiation and configure the desired speed:

For Cisco Catalyst SD-WAN Controllers and Cisco SD-WAN Manager systems, the initial interface speeds are 1000 Mbps, and the operating speed is negotiated with the device at the remote end of the interface. The controller interface speed may vary depending upon the virtualization platform, the NIC used, and the drivers that are present in the software.

# Set the Interface MTU

By default, all interfaces have an MTU of 1500 bytes. You can modify this on an interface:

For releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.4.1a the MTU can range from 576 through 2000 bytes.

Starting from release Cisco IOS XE Catalyst SD-WAN Release 17.4.1a the MTU can range from 576 through 9216 bytes on 1 GE interfaces. This MTU range is also supported on 10 GE and 100 GE interfaces starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a.

To display an interface's MTU, use the **show interface** command.

For Cisco Catalyst SD-WAN Validator, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller devices, you can configure interfaces to use ICMP to perform path MTU (PMTU) discovery. When PMTU discovery is enabled, the device to automatically negotiates the largest MTU size that the interface supports in an attempt to minimize or eliminate packet fragmentation:

On Cisco IOS XE Catalyst SD-WAN device, the Cisco Catalyst SD-WAN BFD software automatically performs PMTU discovery on each transport connection (that is, for each TLOC, or color). BFD PMTU discovery is enabled by default, and it is recommended that you use it and not disable it. To explicitly configure BFD to perform PMTU discovery, use the **bfd color pmtu-discovery** configuration command. However, you can choose to instead use ICMP to perform PMTU discovery:vEdge Cloud router

BFD is a data plane protocol and so does not run on Cisco Catalyst SD-WAN Validator, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller devices.

# VFR and Underlay Fragmentation

*Table 117: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| VFR and Underlay Fragmentation | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br>Cisco Catalyst SD-WAN Manager Release 20.12.1 | In Cisco Catalyst SD-WAN networks, the VFR (Virutal Fragmentation Reassembly) actively fragments and reassembles packets. The packets undergo fragmentation to improve transportation efficiency while passing through a VFR-enabled Cisco IOS XE Catalyst SD-WAN device. The VFR reassembles the fragmented packets to match the original incoming packet. The reassembled packet contains critical Layer 4 or Layer 7 information necessary for proper reception by the destination device.<br>Underlay fragmentation refers to the process of breaking down a large data packet into smaller fragments at the network layer. Underlay fragmentation allows the successful transmission of packets that exceed the MTU limitations by breaking them down into manageable fragments and ensuring their reliable delivery. |

# Information About VFR and Underlay Fragmentation

While transmitting data across a network, due to various network constraints, the original data packets fragment into smaller fragments to facilitate seamless transmission. While the packets travel through the Cisco IOS XE Catalyst SD-WAN device, they are fragmented . VFR allows fragmented packets to be reassembled efficiently before reaching their destination.

In Cisco Catalyst SD-WAN network, data packets undergo reassembly in two modes: the default mode and the reassembly mode.

In the default mode, packets are virtually reassembled by default. Upon the delivery of the first fragment, each feature in the network receives the entire payload of the virtually reassembled packet. When the last fragment is received, the remaining features reassemble the packet. The original packet is fragmented, and the internal fragment information structure is shared. The fragments are then queued for refragmentation based on the fragment-offset sequence. The VFR mechanism reconstructs the packets using information from the fragment headers, such as fragment identifiers, sequence numbers, and offsets.

On the other hand, in the reassembly mode, the packets undergo physical reassembly, and fragment header information isn't saved. Upon receiving the last fragment, the fragments reassemble via a metapacket, and the internal fragment information structure is released.

**Note**

- If the packets were originally fragmented using the default mode, they undergo reassembly as if they were the original incoming packets. On the other hand, when the reassembly mode is utilized to virtually fragment the packets, they experience fragmentation based on the MTU of the egress interface before reassembly.
- Some features (such as NAT, Cisco IOS XE Firewall, IPSec) automatically enable VFR to obtain Layer 4 or Layer 7 information.
- When a particular interface enables VFR, it overrides the existing firewall or NAT's VFR mode configuration by default, ensuring interoperability with the firewall or NAT.

# Information About Underlay Fragmentation

Underlay fragmentation processes large data packets that exceed the MTU (Maximum Transmission Unit) size supported by the Cisco Catalyst SD-WAN network infrastructure. Each data packet has a maximum size that can transmit over the network without being fragmented. This maximum size is defined by the MTU. The process of breaking down a large data packet into smaller fragments at the network layer is known as underlay fragmentation. The underlay fragmentation enables the transmission of packets that exceed the MTU limitations by breaking them down into smaller fragments and ensuring their successful delivery.

# Prerequisites For Configuring VFR and Underlay Fragmentation

The Maximum Transmission Unit (MTU) size needs to be properly configured on the network devices. The MTU defines the maximum size of a packet that can be transmitted without fragmentation. It is essential to ensure that the MTU is set appropriately on all devices involved in the network path to avoid underlay fragmentation unless it is intentionally desired.

# Restrictions For Configuring VFR and Underlay Fragmentation

- The VFR process requires all fragments within an IP datagram. If fragments within an IP datagram are sent to different devices due to load balancing, VFR may fail and fragments may be dropped.
- VFR is designed to work with any feature that requires fragment reassembly (such as Cisco Catalyst SD-WAN NAT, and IPsec). By default, NAT, Crypto-based IPSec, and NAT64 enable and disable VFR internally; that is, when these features are enabled on an interface, VFR is enabled on that interface. If more than one feature attempts to enable VFR on an interface, VFR maintains a reference count to keep track of the number of features that have enabled VFR. When the reference count is zero, VFR is automatically disabled.
- The underlay fragmentation mechanism is limited to the network layer and is specific to the underlying network infrastructure. It does not handle fragmentation and reassembly across multiple network segments or end-to-end connections.

- If any of the fragments in a series of fragmented packets are lost or arrive out of order, the reassembly process may fail. This can result in incomplete or corrupted packets.
- The VFR CLIs are unavailable under port-channel sub-interfaces.

# Benefits of VFR and Underlay Fragmentation

- VFR enables the Cisco IOS XE Firewall to create appropriate dynamic access control lists (ACLs) to protect the network from various fragmentation attacks.
- VFR is responsible for detecting and preventing various types of fragment attacks.
- VFR drops all fragments within a fragment chain if an overlap of a fragment is detected.

# Use Cases For VFR and Underlay Fragmentation

Networks such as long-distance connections such as a connection between an airplane and aiport signal towers, can experience interruptions, due to the time it takes for large packets to traverse these links. When VFR is enabled, the fragments will reassemble into a complete datagram, then are fragmented within the Cisco Catalyst SD-WAN tunnel interface. With this, the first fragment will be sent out first and there is no interruption in receiving the packets.

Underlay fragmentation helps in fragmenting large packets into smaller sizes, and reconstruct the packet back into the original one. This improves the overall application performance.

# Enable Boost Mode

The boost mode helps in resolving one of the identified bottlenecks related to the memory management of fragments within the data plane of the network. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the memory allocation to reassembly of fragments occured from a global chunk, necessitating a lock in period for the memory until the reassembly is complete. This leads to potential competition among multiple threads for the same global chunk and results in waiting for the same memory. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the boost mode enhances performance by utilizing CVLA, an alternative data plane memory infrastructure. Unlike the chunk mechanism, CVLA is lock-free and is an efficient memory management mechanism within Cisco IOS XE devices.

**Note** The boost mode is disabled by default on Cisco IOS XE Catalyst SD-WAN devices.

### Enable Boost Mode Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to enable the boost mode.

1. Enable the boost mode:

**platform** *ipreass* **boost-mode**

Here is the complete configuration example to enable the boost mode:

```
platform ipreass boost-mode
```

# Configure VFR Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure VFR.

### Enable VFR for IPv4 packets on Inbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   **interface** *interface-type interface-number*
2. Enable VFR on the interface and specify the maximum threshold values:

   **ip virtual-reassembly** [**max-reassemblies** number ] [**max-fragments** number ] [**timeout** seconds ] [**mode** modes][**drop-fragments** ]

Here is the complete configuration example to enable VFR for IPv4 packets:

```
interface GigabitEthernet5
ip virtual-reassembly max-reassemblies 64 max-fragments 16 mode default timeout 5
```

### Enable VFR for IPv4 packets on Outbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   **interface** *interface-type interface-number*
2. Enable VFR for outbound interface traffic on the interface and specify the maximum threshold values:

   **ip virtual-reassembly-out** [**max-reassemblies** number ] [**max-fragments** number ] [**timeout** seconds ] [**mode** modes][**drop-fragments** ]

Here is the complete configuration example to enable VFR for IPv4 packets:

```
interface GigabitEthernet 5
ip virtual-reassembly-out mode default max-fragments 64
```

### Enable VFR for IPv6 packets on Inbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   **interface** *interface-type interface-number*
2. Enable VFR for IPv6 packets on inbound interface traffic

   **ipv6 virtual-reassembly [in | out]**[**max-reassemblies** number ] [**max-fragments** number ] [**timeout** seconds ] [**mode** modes][**drop-fragments** ]

Here is the complete configuration example to enable VFR for IPv6 packets:

```
interface GigabitEthernet 5
ipv6 virtual-reassembly in mode default max-fragments 25
max-reassemblies 1024
```

### Enable VFR for IPv6 packets on Outbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   **interface** *interface-type interface-number*
2. Enable VFR for IPv6 packets on outbound interface traffic

   **ipv6 virtual-reassembly [in | out]**[**max-reassemblies** number ] [**max-fragments** number ] [**timeout** seconds ] [**mode** modes][**drop-fragments** ]

Here is the complete configuration example to enable VFR for IPv6 packets:

```
interface GigabitEthernet 5
ipv6 virtual-reassembly out mode default max-fragments 25
```

# Configure Underlay Fragmentation Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure underlay fragmentation.

1. Enter the config-sdwan mode:

   **sdwan**
2. Configure an interface type and enter interface configuration mode:

   **interface** *interface-name interface-number*
3. Configure the tunnel interface:

   **tunnel-interface**
4. Skip Layer 3 fragmentation and clear overlay DF bit:

   **inner-fragmentation-disable**
5. Perform the encapsulation for the GRE interface of the TLOC:

   **encapsulation** *gre*

**Note** Only GRE encapsulation is supported for underlay fragmentation in Cisco IOS XE Catalyst SD-WAN Release 17.12.1a.

Here is the complete configuration example to enable underlay fragmentation:

```
sdwan
interface GigabitEthernet1
tunnel-interface
inner-fragmentation-disable
encapsulation gre
```

# Verify Boost Mode

The following is a sample output from the **show platform hardware qfp active infrastructure cvla client handles** command:

```
Device# show platform hardware qfp active infrastructure cvla client handles
Handles for cpp 0:

---------------------

Entity name: IPREASS_CVLA_0

Handle: 0xeea45000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF_AOR

Handle: 0xeea0d000

Number of allocations: 0

Memory allocated: 0


Entity name: NBAR_CVLA_ENTITY

Handle: 0xee946000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF Chunk 2

Handle: 0xef929000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF Chunk 1

Handle: 0xef928000

Number of allocations: 0

Memory allocated: 0
```

```
--------------------
```

**Note** If there is no entity for **IPREASS_CVLA_*** displayed, the boost mode is disabled. Once the boost mode is disabled, the **IPREASS_CVLA_*** disappears after 64 seconds.

# Monitor VFR and Underlay Fragments Using the CLI

### Monitor VFR for IPv4 packets

The following is a sample output from the **show ip virtual-reassembly** command:

```
Device# show ip virtual-reassembly GigabitEthernet 5
GigabitEthernet5:

   Virtual Fragment Reassembly (VFR) is ENABLED [out]

   Concurrent reassemblies (max-reassemblies): 16

   Fragments per reassembly (max-fragments): 32

   Reassembly timeout (timeout): 3 seconds

   Drop fragments: OFF


   Current reassembly count:0

   Current fragment count:0

   Total reassembly count:12

   Total reassembly timeout
```

The example shows if VFR for IPv4 is enabled or not. **Virtual Fragment Reassembly (VFR) is ENABLED [out]** signifies that VFR is enabled. The total packets that underwent reassembly are also displayed.

### Monitor VFR for IPv6 packets

The following is a sample output from the **show ipv6 virtual-reassembly** command:

```
Device# show ipv6 virtual-reassembly GigabitEthernet 5
GigabitEthernet5:

   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [out]

   IPv6 configured concurrent reassemblies (max-reassemblies): 64

   IPv6 configured fragments per reassembly (max-fragments): 16

   IPv6 configured reassembly timeout (timeout): 3 seconds

   IPv6 configured drop fragments: OFF
```

```
   IPv6 current reassembly count:0

   IPv6 current fragment count:0

   IPv6 total reassembly count:12

   IPv6 total reassembly timeout count:0
```

The example shows if VFR for IPv6 is enabled or not. **Virtual Fragment Reassembly (VFR) is ENABLED [out]** signifies that VFR is enabled. The total packets that underwent reassembly are also displayed.

### Monitor Underlay Fragmentation

The following is a sample output from the **show ip traffic interface GigabitEthernet 1** command:

```
Device# show ip traffic interface GigabitEthernet 1
GigabitEthernet 1 statistics :

  Rcvd:  11048818 total, 749458331 total_bytes

         0 format errors, 0 hop count exceeded

         0 bad header, 0 no route

         0 bad destination, 0 not a router

         0 no protocol, 0 truncated

         0 forwarded

         0 fragments, 0 total reassembled

         0 reassembly timeouts, 0 reassembly failures

         0 discards, 0 delivers

  Sent:  0 total, 0 total_bytes 0 discards

         0 generated, 0 forwarded

         0 fragmented into, 0 fragments, 0 failed

  Mcast: 0 received, 0 received bytes

         0 sent, 0 sent bytes

  Bcast: 0 received, 1256 sent
```

The example shows the number of packets that were sent and received, including the total number of packets. A change from the previous number of packet tranfer indicates that underlay fragmentation is enabled.

The following is a sample output from **show sdwan ftm** *tloc-list* command:

```
Device# show sdwan ftm tloc-list

--- LOCAL  TLOC LIST ---




Id: 32775 (binosId=0xf808007f), Tenant Id: 0      LocalTLOC, num-nhops: 0   ,hash: 0, ref:
 1    SLA 0x0:0x0 Inner-fragmentation
-disable: No
```

```
[TOTAL-LOCAL-TLOC:1]



--- REMOTE TLOC LIST ---



Id: 32768 (binosId=0xf808000f), Tenant Id: 0       SLAClass, num-nhops: 0   ,hash: 0, ref:
 1    SLA 0x0:0x0
 num-active-nhops: 0


Id: 32774 (binosId=0xf808006f), Tenant Id: 0       SLAClass, num-nhops: 1   ,hash: 0, ref:
 1    SLA 0x1:0x0
 [nhop1] nhop-Id: 19   , Type: IPsec     , Encap: IPSEC SLA 0x1:0x0hw_record_index:   5
198.100.1.5/12366->198.100.1.6/12346 pr
oto 0x800 hash 0x13 wan-if 3 tloc 32774 R-color mpls local-tloc 32775 L-color mpls BFD UP
tloc-capability 0 SLA 0x1:0x0 weight
1   pref 0

 num-active-nhops: 1


[TOTAL-REMOTE-TLOC:2]


--- PENDING TLOC LIST (is_pending_updates:FALSE)---



[TOTAL-PENDING-TLOC:0]



--- UNMATCHED TLOC LIST (is_pending_updates:FALSE)---



[TOTAL-UNMATCHED-TLOC:0]



--- TENANT LOCAL  TLOC LIST ---
```

The example displays all the local TLOCs in the network.

The following is a sample output from **show platform software sdwan** *R0 next-hop overlay all* command:

```
Device# show platform software sdwan R0 next-hop overlay all

Show sdwan next-hop oce all :


OCE ID: 0xf800013f, OCE Type: SDWAN_NH_OVERLAY

Overlay: client_handle (nil), ppe addr (nil)

  overlay encap: ipsec

  src-ip: 198.100.1.5, src-port: 12366

  dst-ip: 198.100.1.6, dst-port: 12346

  flags: 0x0, linktype: MCP_LINK_IP, ifhandle: 15, encap type: MCP_ET_NULL

  encap rewrite: 00

 mtu: 1446, fixup: 0x0, fixup_flags_2: 0x0, color: mpls, phy_oce_handle: 31, nh_overlay_h:
0xf800013f
    Overlay_CFG:

    encap type: ipsec

    src-ip: 198.100.1.5, src-port: 12366

    dst-ip: 198.100.1.6, dst-port: 12346

    local_system_ip: 1.1.1.1

    remote_system_ip: 2.2.2.2

    local_color: 2 [mpls], remote_color: 2 [mpls]

    wan_ifindex: 8 [GigabitEthernet2], tun_ifindex: 15 [Tunnel0]

    tun_adj_id: 0, l2_adj_id: 0x1f, tunnel_qos_dpidx: 0x0

    bfd-ld: 20005, ipsec_flow_id: 603979786, session_id: 5

    Inner-fragmentation-disable: yes
```

The example demonstrates whether the inner fragmentation is disabled or enabled in a particular next-hop overlay.

The following is a sample output from **show platform software sdwan** *F0 next-hop overlay all* command:

```
Device# show platform software sdwan F0 next-hop overlay all

OCE ID: 0xf800013f, OCE Type: SDWAN_NH_OVERLAY

Overlay: client_handle 0x63d321350ba0, ppe addr db910710

  overlay encap: ipsec

  src-ip: 198.100.1.5, src-port: 12366

  dst-ip: 198.100.1.6, dst-port: 12346

  flags: 0x0, linktype: MCP_LINK_SDWAN, ifhandle: 15, encap type: MCP_ET_ARPA

  encap rewrite: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  mtu: 1446, fixup: 0x0, fixup_flags_2: 0x800000, color: mpls, phy_oce_handle: 31,
nh_overlay_h: 0xf800013f
    Overlay_CFG:

    encap type: ipsec

    src-ip: 198.100.1.5, src-port: 12366

    dst-ip: 198.100.1.6, dst-port: 12346

    local_system_ip: 1.1.1.1

    remote_system_ip: 2.2.2.2

    local_color: 2 [mpls], remote_color: 2 [mpls]

    wan_ifindex: 8 [GigabitEthernet2], tun_ifindex: 15 [Tunnel0]

    tun_adj_id: 0, l2_adj_id: 0x1f, tunnel_qos_dpidx: 0x0

    bfd-ld: 20005, ipsec_flow_id: 603979786, session_id: 5

    Inner-fragmentation-disable: yes
```

The example demonstrates whether the inner fragmentation is disabled or enabled in all the available overlays.

# Configure TCP MSS and Clear Dont Fragment

***Table 118: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Configure TCP MSS | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>Cisco vManage Release 20.5.1 | This feature adds support for TCP MSS adjustment 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<br>Cisco vManage Release 20.5.1 | This feature provides the option to clear the Don't Fragment bit in the IPv4 packet header for packets being sent out on a Cisco Catalyst SD-WAN tunnel . When you clear the Don't Fragment configuration, packets larger than the interface MTU are fragmented before being sent. |

TCP maximum segment size (MSS) is a parameter that specifies the largest amount of data, in bytes, that a communications device can receive in a single TCP segment, without counting the TCP header or the IP header. The MSS is specified as TCP MSS, initially in the TCP SYN packet during TCP handshake. Small MSS values reduces or eliminates IP fragmentation resulting in higher overhead.

You can configure the MSS of TCP SYN packets passing through a device. By default, the MSS is dynamically adjusted based on the interface or tunnel maximum transmission unit (MTU) such that TCP SYN packets are

never fragmented. For data sent over an interface, the MSS is calculated by adding the interface MTU, the IP header length, and the maximum TCP header length.

### Limitations

- TCP MSS values can be adjusted for Cisco Catalyst SD-WAN tunnel interfaces only.

**Note** Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, you can adjust the TCP MSS value for a service VPN or for Network Address Translation (NAT) Direct Internet Access (DIA) use cases. Adjusting the TCP MSS value helps prevent TCP sessions from being dropped.

For more information on NAT DIA, see the *Cisco Catalyst SD-WAN NAT Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

- The option **Clear Dont Fragment** is available for Cisco Catalyst SD-WAN tunnel interfaces only.

## Configure TCP MSS and Clear Dont Fragment

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 TCP MSS Using CLI

Use the following command to configure TCP MSS on the CLI:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip tcp adjust-mss 1460
```

### Verify TCP MSS Configuration

The following is sample output of the **show platform hardware qfp active feature sdwan datapath session summary** command:

```
Device#show platform hardware qfp active feature sdwan datapath session summary
Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU

------          ------          -------- -------    ------   -------  ----------- -----

10.1.15.25      10.1.14.14      12347    12346      IPSEC    65526    10007       1446

10.1.15.25      10.0.5.21       12347    12357      IPSEC    65526    10009       1446

10.1.15.25      10.0.5.11       12347    12347      IPSEC    65526    10008       1446

10.1.15.25      10.1.16.16      12347    12366      IPSEC    65526    10006       1446
```

## Configure Clear Dont Fragment on the CLI

Use the following command to configure **Clear Dont Fragment** option using the CLI:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment
```

### Verify Dont Fragment Configuration on the CLI

The following is sample output of the **show platform software interface rp active name Tunnel1** command to verify if **Clear-dont-fragment** is enabled or not.

```
Device# show platform software interface rp active name Tunnel1 | include dont
IP Clear-dont-fragment: TRUE
```

The following is sample output of the **show running-config interface Tunnel1** command that displays the running configuration when **Clear-dont-fragment** is enabled.

```
Device# show running-config interface Tunnel1
Building configuration...

Current configuration : 132 bytes
!
interface Tunnel1
ip unnumbered GigabitEthernet1
ip clear-dont-fragment
tunnel source GigabitEthernet1
tunnel mode sdwan
end
```

# Monitoring Bandwidth on a Transport Circuit

You can monitor the bandwidth usage on a transport circuit, to determine how the bandwidth usage is trending. If the bandwidth usage starts approaching a maximum value, you can configure the software to send a notification. Notifications are sent as Netconf notifications, which are sent to the Cisco SD-WAN Manager NMS, SNMP traps, and syslog messages. You might want to enable this feature for bandwidth monitoring, such as when you are doing capacity planning for a circuit or when you are gathering trending information about bandwidth utilization. You might also enable this feature to receive alerts regarding bandwidth usage, such as if you need to determine when a transport interface is becoming so saturated with traffic that a customer's traffic is impacted, or when customers have a pay-per-use plan, as might be the case with LTE transport.

To monitor interface bandwidth, you configure the maximum bandwidth for traffic received and transmitted on a transport circuit. The maximum bandwidth is typically the bandwidth that has been negotiated with the circuit provider. When bandwidth usage exceeds 85 percent of the configured value for either received or transmitted traffic, a notification, in the form of an SNMP trap, is generated. Specifically, interface traffic is sampled every 10 seconds. If the received or transmitted bandwidth exceeds 85 percent of the configured value in 85 percent of the sampled intervals in a continuous 5-minute period, an SNMP trap is generated. After the first trap is generated, sampling continues at the same frequency, but notifications are rate-limited to once per hour. A second trap is sent (and subsequent traps are sent) if the bandwidth exceeds 85 percent of the value in 85 percent of the 10-second sampling intervals over the next 1-hour period. If, after 1 hour, another trap is not sent, the notification interval reverts to 5 minutes.

You can monitor transport circuit bandwidth on Cisco IOS XE Catalyst SD-WAN devices and on Cisco SD-WAN Manager NMSs.

To generate notifications when the bandwidth of traffic received on a physical interface exceeds 85 percent of a specific bandwidth, configure the downstream bandwidth:

To generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds 85 percent of a specific bandwidth, configure the upstream bandwidth:

In both configuration commands, the bandwidth can be from 1 through 2147483647 ($2^{32}$ / 2) – 1 kbps.

To display the configured bandwidths, look at the bandwidth-downstream and bandwidth-upstream fields in the output of the **show interface detail** command. The rx-kbps and tx-kbps fields in this command shows the current bandwidth usage on the interface.

# Enable DHCP Server using Cisco SD-WAN Manager

*Table 119: Feature History*

| Feature Name | Release Information | Feature Description |
|---|---|---|
| DHCP Option Support | Cisco IOS XE Catalyst SD-WAN Release 16.12.1b | This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges. |

Use the DHCP-Server template for all Cisco Catalyst SD-WANs.

You enable DHCP server functionality on a Cisco Catalyst SD-WAN device interface so it can assign IP addresses to hosts in the service-side network.

To configure a Cisco Catalyst SD-WAN device to act as a DHCP server using Cisco SD-WAN Manager templates:

1. Create a DHCP-Server feature template to configure DHCP server parameters, as described in this topic.
2. Create one or more interface feature templates, as described in the VPN-Interface-Ethernet and the VPN-Interface-PPP-Ethernet help topics.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

To configure a Cisco IOS XE Catalyst SD-WAN device interface to be a DHCP helper so that it forwards broadcast DHCP requests that it receives from DHCP servers, in the DHCP Helper field of the applicable interfaces template, enter the addresses of the DHCP servers.

### Navigate to the Template Screen and Name the Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then 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, choose **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Service VPN** or scroll to the **Service VPN** section.
6. Click **Service VPN** drop-down list.
7. From **Additional VPN Templates**, click **VPN Interface**.
8. From the **Sub-Templates** drop-down list, choose **DHCP Server**.
9. From the **DHCP Server** drop-down list, click **Create Template**. The DHCP-Server template form is displayed.

This form contains fields for naming the template, and fields for defining the DHCP Server parameters.

10. In **Template Name**, enter a name for the template.

    The name can be up to 128 characters and can contain only alphanumeric characters.

11. In **Template Description**, 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.

### Minimum DHCP Server Configuration

To configure DHCP server functionality, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk as required to configure DHCP servers.

***Table 120:***

| Parameter Name | Description |
|---|---|
| Address Pool* | Enter the IPv4 prefix range, in the format *prefix/length*, for the pool of addresses in the service-side network for which the router interface acts as DHCP server. |
| Exclude Addresses | Enter one or more IP addresses to exclude from the DHCP address pool. To specify multiple individual addresses, list them separated by a comma. To specify a range of addresses, separate them with a hyphen. |
| Maximum Leases | Specify the number of IP addresses that can be assigned on this interface.*Range:* 0 through 4294967295 |
| Lease Time | Specify how long a DHCP-assigned IP address is valid.*Range:* 0 through 4294967295 seconds |
| Offer Time | Specify how long the IP address offered to a DHCP client is reserved for that client. By default, an offered IP address is reserved indefinitely, until the DHCP server runs out of addresses. At that point, the address is offered to another client.*Range:* 0 through 4294967295 seconds*Default:* 600 seconds |
| Administrative State | Select Up to enable or Down to disable the DHCP functionality on the interface. By default, DHCP server functionality is disabled on an interface. |

To save the feature template, click **Save**.

### Configure Static Leases

To configure a static lease to assign a static IP address to a client device on the service-side network, click **Static Lease**, and click **Add New Static Lease** and configure the following parameters:

*Table 121:*

| Parameter Name | Description |
|---|---|
| MAC Address | Enter the MAC address of the client to which the static IP address is being assigned. |
| IP Address | Enter the static IP address to assign to the client. |
| Hostname | Enter the hostname of the client device. |

To edit a static lease, click **pencil** icon.

To remove a static lease, click **trash** icon.

To save the feature template, click **Save**.

### Configure Advanced Options

To configure a advanced DHCP server options, click **Advanced** and then configure the following parameters:

*Table 122:*

| Parameter Name | Description |
|---|---|
| Interface MTU | Specify the maximum MTU size of packets on the interface.*Range:* 68 to 65535 bytes |
| Domain Name | Specify the domain name that the DHCP client uses to resolve hostnames. |
| Default Gateway | Enter the IP address of a default gateway in the service-side network. |
| DNS Servers | Enter one or more IP address for a DNS server in the service-side network. Separate multiple entries with a comma. You can specify up to eight addresses. |
| TFTP Servers | Enter the IP address of a TFTP server in the service-side network. You can specify one or two addresses. If two, separate them with a comma. |

To save the feature template, click **Save**.

### Configure DHCP server using CLI

```
Device# config-transaction
Device(dhcp-config)# ip dhcp pool DHCP-POOL
Device(dhcp-config)# network 10.1.1.1 255.255.255.0
Device(dhcp-config)# default-router 10.1.1.2
Device(dhcp-config)# dns-server 172.16.0.1
Device(dhcp-config)# domain-name DHCP-DOMAIN
Device(dhcp-config)# exit
Device(config)ip dhcp excluded-address 10.1.1.2 10.1.1.10
Device(
```

### Release Information

Introduced in Cisco SD-WAN Manager in Release 15.2.

# Configuring PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) connects multiple users over an Ethernet local area network to a remote site through common customer premises equipment. PPPoE is commonly used in a broadband aggregation, such as by digital subscriber line (DSL). PPPoE provides authentication with the CHAP or PAP protocol. In the Cisco Catalyst SD-WAN overlay network, Cisco Catalyst SD-WAN devices can run the PPPoE client. The PPPoE server component is not supported.

It is recommended that you configure quality of service (QoS) and shaping rate on a PPPoE Dialer interface. Queuing based QoS policies on both Dialer interface and PPPoE-enabled physical interface at the same time, is not supported.

PPPoE-enabled physical interfaces are supported on ATM PVCs and Ethernet interfaces. A dialer interface must be used for cloning virtual access. Multiple PPPoE client sessions can be configured on an Ethernet interface, but each session must use a separate dialer interface and a separate dialer pool.

The Cisco Catalyst SD-WAN implementation of PPPoE does not support the Compression Control Protocol (CCP) options, as defined in RFC 1962.

This example shows configuring PPPoE server on IPv4 interfaces:

```
!
interface Dialer100
 mtu 1492
 ip address negotiated
 encapsulation ppp
 ip tcp adjust-mss 1460
 dialer pool 100
 dialer down-with-vInterface
 ppp authentication chap callin
 ppp chap hostname cisco
 ppp chap password 7 1511021F07257A767B
 ppp ipcp route default
```

**Note** Follow these steps to replace a template configured with PPPoE as WAN interface with a regular interface in Dialer100:

1. Remove the IP address assigned to the dialer interface using the command:

   ```
   no ip address <ip> <mask>
   ```

2. Add a new IP address for the dialer interface.

# Configure PPPoE from Cisco SD-WAN Manager Templates

To use Cisco SD-WAN Manager templates to configure PPPoE on Cisco IOS XE Catalyst SD-WAN device, you create three feature templates and one device template:

- Create a VPN-Interface-PPP feature template to configure PPP parameters for the PPP virtual interface.
- Create a VPN-Interface-PPP-Ethernet feature template to configure a PPPoE-enabled interface.
- Optionally, create a VPN feature template to modify the default configuration of VPN 0.

- Create a device template that incorporates the VPN-Interface-PPP, VPN-Interface-PPP-Ethernet, and VPN feature templates.

Create a VPN-Interface-PPP feature template to configure PPP parameters for the PPP virtual interface:

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. Choose Cisco IOS XE Catalyst SD-WAN device Cloud or a router model.
4. Choose the **VPN-Interface-PPP** template.
5. In the template, configure the following parameters:

***Table 123:***

| Parameter Field | Procedure |
|---|---|
| Template Name | Enter a name for the template. It can be up to 128 alphanumeric characters. |
| Description | Enter a description for the template. It can be up to 2048 alphanumeric characters. |
| Shutdown | Click **No** to enable the PPP virtual interface. |
| Interface Name | Enter the number of the PPP interface. It can be from 1 through 31. |
| Description (optional) | Enter a description for the PPP virtual interface. |
| Authentication Protocol | Select either CHAP or PAP to configure one authentication protocol, or select PAP and CHAP to configure both. For CHAP, enter the hostname and password provided by your ISP. For PAP, enter the username and password provided by your ISP. If you are configuring both PAP and CHAP, to use the same username and password for both, click Same Credentials for PAP and CHAP. |
| AC Name (optional) | Select the PPP tab, and in the AC Name field, enter the name of the the name of the access concentrator used by PPPoE to route connections to the Internet. |
| IP MTU | Click **Advanced**, and in the IP MTU field, ensure that the IP MTU is at least 8 bytes less than the MTU on the physical interface. The maximum MTU for a PPP interface is 1492 bytes. If the PPPoE server does not specify a maximum receive unit (MRU), the MTU value for the PPP interface is used as the MRU.<br>Starting from Cisco vManage Release 20.9.1, there is 8 bytes overheads deduced based on the specified IP MTU value when configuration is pushed to the device. |
| Save | To save the feature template, click **Save**. |

To create a VPN-Interface-PPP-Ethernet feature template to enable the PPPoE client on the physical interfaces:

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. Choose Cloud or a router model.
4. Choose the **VPN-Interface-PPP-Ethernet** template.
5. In the template, configure the following parameters:

| Parameter Field | Procedure |
|---|---|
| Template Name | Enter a name for the template. It can be up to 128 alphanumeric characters. |
| Description | Enter a description for the template. It can be up to 2048 alphanumeric characters. |
| Shutdown | Click **No** to enable the PPPoE-enabled interface. |
| Interface Name | Enter the name of the physical interface in VPN 0 to associate with the PPP interface. |
| Description (optional) | Enter a description for the PPPoE-enabled interface. |
| IP Confguration | Assign an IP address to the physical interface:<br>• To use DHCP, select Dynamic. The default administrative distance of routes learned from DHCP is 1.<br>• To configure the IP address directly, enter of the IPv4 address of the interface. |
| DHCP Helper (optional) | Enter up to four IP addresses for DHCP servers in the network. |
| Save | To save the feature template, click **Save**. |

To create a VPN feature template to configure the PPPoE-enabled interface in VPN 0, the transport VPN:

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. Choose Cloud or a router model.
4. Choose the **VPN** template.
5. In the template, configure the following parameters:

| Parameter Field | Procedure |
|---|---|
| Template Name | Enter a name for the template. It can be up to 128 alphanumeric characters. |

| Parameter Field | Procedure |
|---|---|
| Description | Enter a description for the template. It can be up to 2048 alphanumeric characters. |
| VPN Identifier | Enter VPN identifier 0. |
| Name | Enter aname for the VPN. |
| Other interface parameters | Configure the desired interface properties. |
| Save | To save the feature template, click **Save**. |

To create a device template that incorporates the VPN-Interface-PPP, VPN-Interface-PPP-Ethernet, and VPN feature templates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then 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, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose the type of device for which you are creating the device template.

   Cisco SD-WAN Manager displays the feature templates for the device type you selected. Required templates are indicated with an asterisk (*).
5. Enter a name and description for the device template. These fields are mandatory. The template name cannot contain special characters.
6. In **Transport & Management VPN**, under **VPN 0**, from the drop-down list of available templates, select the desired feature template. The list of available templates are the ones that you have previously created.
7. In **Additional VPN 0 Templates**, click the plus sign (+) next to **VPN Interface PPP**.
8. From **VPN-Interface-PPP** and **VPN-Interface-PPP-Ethernet** fields, select the feature templates to use.
9. To configure multiple PPPoE-enabled interfaces in VPN 0, click the plus sign (+) next to Sub-Templates.
10. To include additional feature templates in the device template, in the remaining sections, select the feature templates in turn, and from the drop-down list of available templates, select the desired template. The list of available templates are the ones that you have previously created. Ensure that you select templates for all mandatory feature templates and for any desired optional feature templates.
11. To create the device template, click **Create**.

To attach a device template to a 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. Choose a template.
4. Click **…**, and click **Attach Device**.
5. Search for a device or select a device from the Available Device(s) column to the left.
6. Click the arrow pointing right to move the device to the Selected Device(s) column on the right.
7. Click **Attach**.

# Configure PPPoE Over ATM

***Table 124: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Configure PPPoE over ATM | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a<br>Cisco vManage Release 20.4.1 | This feature provides support for configuring PPPoEoA on Cisco IOS XE Catalyst SD-WAN devices. PPPoEoA uses AAL5MUX encapsulation which delivers better efficiency compared to other encapsulation methods. |

You can configure PPPoE over ATM interfaces (PPPoEoA) on Cisco IOS XE Catalyst SD-WAN devices that support ADSL. PPPoEoA uses ATM Adaptation Layer 5 Multiplexed Encapsulation (AAL5MUX) encapsulation to carry PPPoE over ATM permanent virtual circuits (PVCs), providing efficiency gain over AAL5 LLC/SNAP encapsulation.

PPPoEoA over AAL5MUX reduces Subnetwork Access Protocol (SNAP) encapsulation bandwidth usage, using multiplexed (MUX) encapsulation to reduce the number of cells needed to carry voice packets. Deploying the PPPoEoA over ATM AAL5MUX feature in a VoIP environment results in improved throughput and bandwidth usage.

## Supported Platforms for PPPoE Over ATM

The following platforms support PPPoE over ATM:

- Cisco 1100 4G/6G Series Integrated Services routers.
- Cisco1100 Series Integrated Service routers.
- Cisco1109 Series Integrated Service routers.
- Cisco111x Series Integrated Service routers.
- Cisco1111x Series Integrated Service routers.

- Cisco1120 Series Integrated Service routers.
- Cisco1160 Series Integrated Service routers.

# Configure PPPoE Over ATM using Cisco SD-WAN Manager

You can configure PPPoE using in Cisco SD-WAN Manager using the device CLI template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. From **Device Templates**, 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 **CLI Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
6. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
7. Choose **Device configuration**. Using this option, you can provide IOS-XE configuration commands that appear in the output of the `show sdwan running-config` command.
8. (Optional) To load the running config of a connected device, select it from the Load Running config from reachable device list and click **Search**.
9. In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file. The configuration for PPPoEoA is available in the Configure PPPoE Over ATM on the CLI section.
10. 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}}.
11. Click **Add**. The new device template is displayed in the Device Template table. The **Type** column shows **CLI** to indicate that the device template was created from CLI text.

# Configure PPPoE Over ATM on the CLI

This section provides example CLI configurations to configure PPoE over ATM on the CLI.

```
Device(config)# interface atm number
Device(config)# no ip address
Device(config)# interface atm number point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# encapsulation aal5mux  pppoe-client
Device(config)# pppoe-client dial-pool-number number
Device(config)# interface Dialer dialer-rotary-group-number
```

```
Device(config)# mtu bytes
Device(config)# ip address negotiated
Device(config-if)# encapsulation encapsulation-type
Device(config)# load-interval seconds
Device(config)# dialer pool number
Device(config)# dialer-group group-number
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname hostname
Device(config)# ppp chap password secret
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
```

## Configuration Example for Configuring PPPoE Over ATM Interfaces

This example shows configuring PPPoE over ATM interfaces.

```
Device(config)# interface ATM0/1/0
Device(config)# no ip address
Device(config)# no atm enable-ilmi-trap
!
Device(config)# interface ATM0/1/0.10 point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# cdp enable
Device(config)# pvc 22/62
Device(config)# ubr 1045
Device(config-if)# encapsulation aal5mux pppoe-client
Device(config)# pppoe-client dial-pool-number 120
!
!
Device(config)# interface Dialer 120
Device(config)# mtu 1492
Device(config)# ip address negotiated
Device(config)# ip nat outside
Device(config-if)# encapsulation ppp
Device(config)# load-interval 30
Device(config)# dialer pool 120
Device(config)# dialer-group 1
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname test@cisco.com
Device(config)# ppp chap password 0 cisco
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
!
```

# Configuring VRRP

**Note** The x710 NIC must have the **t->system-> vrrp-advt-with-phymac** command configured, for VRRP to function.

The Virtual Router Redundancy Protocol (VRRP) is a LAN-side protocol that provides redundant gateway service for switches and other IP end stations. In the Cisco Catalyst SD-WAN software, you configure VRRP on an interface, and typically on a subinterface, within a VPN.

VRRP is only supported with service-side VPNs (VPN 0 and 512 reserved) and if sub-interfaces are used, then the VRRP physical interface must be configured in VPN 0.

For each VRRP interface (or subinterface), you assign an IP address and you place that interface in a VRRP group.

The group number identifies the virtual router. You can configure a maximum of 512 groups on a router. In a typical VRRP topology, two physical routers are configured to act as a single virtual router, so you configure the same group number on interfaces on both these routers.

For each virtual router ID, you must configure an IP address.

Within each VRRP group, the router with the higher priority value is elected as primary VRRP. By default, each virtual router IP address has a default primary election priority of 100, so the router with the higher IP address is elected as primary. You can modify the priority value, setting it to a value from 1 through 254.

The primary VRRP periodically sends advertisement messages, indicating that it is still operating. If backup routers miss three consecutive VRRP advertisements, they assume that the primary VRRP is down and elect a new primary VRRP. By default, these messages are sent every second. You can change the VRRP advertisement time to be a value from 1 through 3600 seconds.

By default, VRRP uses the state of the interface on which it is running, to determine which router is the primary virtual router. This interface is on the service (LAN) side of the router. When the interface for the primary VRRP goes down, a new primary VRRP virtual router is elected based on the VRRP priority value. Because VRRP runs on a LAN interface, if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, you can configure one of the following:

- Track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router.

If all OMP sessions are lost on the primary VRRP router, VRRP elects a new default gateway from among all the gateways that have one or more active OMP sessions even if the gateway chosen has a lower VRRP priority than the current primary VRRP router. With this option, VRRP failover occurs once the OMP state changes from up to down, which occurs when the OMP hold timer expires. (The default OMP hold timer interval is 60 seconds.) Until the hold timer expires and a new primary VRRP is elected, all overlay traffic is dropped. When the OMP session recovers, the local VRRP interface claims itself as primary VRRP even before it learns and installs OMP routes from the Cisco Catalyst SD-WAN Controllers. Until the routers are learned, traffic is also dropped.

- Track both the OMP session and a list of remote prefixes.

If all OMP sessions are lost, VRRP failover occurs as described for the **track-omp** option. In addition, if reachability to all the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the router determines the primary VRRP.

As discussed above, the IEEE 802.1Q protocol adds 4 bytes to each packet's length. Hence, for packets to be transmitted, either increase the MTU size on the physical interface in VPN 0 (the default MTU is 1500 bytes) or decrease the MTU size on the VRRP interface.

# Configuring Dynamic Interfaces

*Table 125: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Configuring Dynamic Interfaces | Cisco IOS XE Catalyst SD-WAN Release 17.3.2<br>Cisco vManage Release 20.3.2 | This feature allows you to configure dynamic interfaces for supported devices. A dynamic interface allows a device to select optimum paths in real-time.<br>This feature applies only to the Cisco C8500-12X4QC router. |

You can configure dynamic interfaces for supported devices. A dynamic interface allows a device to select optimum paths in real-time.

Configuring dynamic interfaces consists of these general steps:

1. Create a dynamic interface mode feature template. As part of this step, you define modes for the bays in a device.
2. Configure an Interface for Control Connections.
3. Associate the dynamic interface mode feature template with a device template.

### Create a Dynamic Interface Mode Feature Template

When you create a dynamic interface mode feature template, you create a template that defines the modes for the bays in a device.

You can configure the mode for bay 1, bay 2, or both.

The mode for bay 0 is configured automatically and cannot be changed. If you configure the mode for bay 1 as 100G, bay 0 is disabled because the 10G interfaces on bay 0 do not apply in this case.

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 choose **Feature Template**.
4. From the **Device Model** drop-down list, choose the device for which you wish to create the template.
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 of the template.

This field can contain any characters and spaces.

7. From **Additional Templates**, choose the **Dynamic Interface Mode** drop-down list and click **Create Template**.
8. In **Template Name**, enter a name for the template.

   This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
9. In **Description**, enter a description of the template.

   This field can contain any characters and spaces.
10. Configure the mode for bay 1, bay 2, or both bays by choosing the desired value in the **Bay 1**, **Bay 2**, or both fields.

    You cannot change the default value for bay 0.
11. Click **Save**.

### Configure an Interface for Control Connections

This section describes how to configure a new VPN 0 interface for an existing control connection to operate with the bays that you configured in "Create a Dynamic Interface Mode Feature Template." It also describes how to configure an IPv4 route for the interface.

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 **...** of the template for which you want to configure the interface, and then choose **Edit**.
4. Click **Transport & Management VPN** and perform these actions to create interfaces for the bays:
   a. Click **VPN Interface** in the **Additional VPN 0 Template**.
   b. Choose the new **VPN Interface Ethernet** menu that displays, and then click **Create Template**.
   c. In **Template Name**, enter a name for the template.

      This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
   d. In **Description**, enter a description of the template.

      This field can contain any characters and spaces.
   e. Add control connections to the bays that you configured as described in "Create a Dynamic Interface Mode Feature Template."
5. Choose **Basic Configuration** and perform these actions:
   a. In **Interface Name**, enter a name for the interface.

      Enter a name in the format that this example shows: "FortyGigabitEthernet0/1/0."

b. Configure other options on this tab as needed.

6. From **Tunnel**, set **Tunnel Interface** to **On**.
7. Click **Save**.
8. Choose **IPv4 Route** and perform these actions to configure an IPv4 route for the VPN0 template:
   a. Click **New IPv4 Route**.
   b. In **Prefix**, enter a prefix for the IPv4 route.
   c. In **Gateway**, choose **Next Hop**.
   d. Configure items as needed in **Next Hop**, and then click **Add**.
   e. Click **Save**.
9. Click **Update**.

### Associate the Dynamic Interface Mode Feature Template with a Device Template

After you create the dynamic interface mode feature template, associate it with a device template and attach the device template to a device. For instructions, see Create a Device Template from Feature Templates.

# Configure VPN Ethernet Interface

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

**Step 2** Click **Device Templates**, and click **Create Template**.

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

**Step 3** From the **Create Template** drop-down list, choose **From Feature Template**.

**Step 4** From the **Device Model** drop-down list, choose the type of device for which you are creating the template.

**Step 5** To create a template for VPN 0 or VPN 512:

a. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

b. Under **Additional VPN 0 Templates**, click **Cisco VPN Interface Ethernet**.

c. From the **VPN Interface** drop-down list, click **Create Template**. The **Cisco VPN Interface Ethernet** template form displays.

This form contains fields for naming the template, and fields for defining the VPN Interface Ethernet parameters.

**Step 6** In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

**Step 7** In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

# Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, choose **Basic Configuration** and configure the following parameters:

**Note** Parameters marked with an asterisk are required to configure an interface.

| Parameter Name | IPv4 or IPv6 | Options | Description |
|---|---|---|---|
| **Shutdown*** | Click **No** to enable the interface. | | |
| **Interface name*** | Enter a name for the interface.<br>For Cisco IOS XE Catalyst SD-WAN devices, you must:<br>• Spell out the interface names completely (for example, GigabitEthernet0/0/0).<br>• Configure all the router's interfaces, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured. | | |
| **Description** | Enter a description for the interface. | | |
| **IPv4 / IPv6** | Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface. | | |
| **Dynamic** | Click **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server. | | |
| | **Both** | **DHCP Distance** | Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1. |
| | **IPv6** | **DHCP Rapid Commit** | Optionally, configure the DHCP IPv6 local server to support DHCP Rapid Commit, to enable faster client configuration and confirmation in busy environments.<br>Click **On** to enable DHCP rapid commit.<br>Click **Off** to continue using the regular commit process. |
| **Static** | Click **Static** to enter an IP address that doesn't change. | | |
| | **IPv4** | **IPv4 Address** | Enter a static IPv4 address. |
| | **IPv6** | **IPv6 Address** | Enter a static IPv6 address. |
| **Secondary IP Address** | **IPv4** | Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface. | |
| **IPv6 Address** | **IPv6** | Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface. | |

| Parameter Name | IPv4 or IPv6 | Options | Description |
|---|---|---|---|
| **DHCP Helper** | **Both** | To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BootP (broadcast) DHCP requests that it receives from the specified DHCP servers. | |
| **Block Non-Source IP** | **Yes** / **No** | Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click **No** to allow other traffic. | |

To save the feature template, click **Save**.

# Create a Tunnel Interface

On Cisco IOS XE Catalyst SD-WAN devices, you can configure up to eight tunnel interfaces. This means that each Cisco IOS XE Catalyst SD-WAN device router can have up to eight TLOCs. On Cisco Catalyst SD-WAN Controllers and Cisco SD-WAN Manager, you can configure one tunnel interface.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0. The WAN interface will enable the flow of tunnel traffic to the overlay. You can add other parameters shown in the table below only after you configure the WAN interface as a tunnel interface.

To configure a tunnel interface, select **Interface Tunnel** and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click **On** to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Port Hop | Click **On** to enable port hopping, or click **Off** to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template.<br>Default: Enabled<br>Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller default: Disabled |
| TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br>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 |

| Parameter Name | Description |
|---|---|
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Allow Service | Select **On** or **Off** for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click **Advanced Options**:

| Parameter Name | Description |
|---|---|
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>Default: default |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>Range: 1 through 60 seconds<br>Default: 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>Range: 100 through 10000 milliseconds<br>Default: 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>Range: 12 through 60 seconds<br>Default: 12 seconds |

## Associate a Carrier Name with a Tunnel Interface

To associate a carrier name or private network identifier with a tunnel interface, use the **carrier** command. *carrier-name* can be **default** and **carrier1** through **carrier8:**

```
Device(config)# interface Tunnel 0
Device(config-if)# ip unnumbered GigabitEthernet1
Device(config-if)# ipv6 unnumbered GigabitEthernet2
Device(config-if)# tunnel source GigabitEthernet1
```

```
Device(config-if)# tunnel mode sdwan
Device(config-if)# exit
Device(config)# sdwan
Device(config-sdwan)# int GigabitEthernet1
Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# carrier default
```

## Create Tunnel Groups

By default, WAN Edge routers try to build tunnels with all other TLOCs in the network, regardless of color. When the restrict option is used with the color designation under the tunnel configuration, the TLOC is restricted to only building tunnels to TLOCs of the same color. For more information on the restrict option see, Configure Interfaces in the WAN Transport VPN(VPN0).

The tunnel group feature is similar to the restrict option but gives more flexibility because once a tunnel group ID is assigned under a tunnel, only TLOCs with the same tunnel group IDs can form tunnels with each other irrespective of color.

If a TLOC is associated with a tunnel group ID, it continues to form tunnels with other TLOCs in the network that are not associated with any tunnel group IDs.

**Note** The restrict option can still be used in conjunction with this feature. If used, then an interface with a tunnel group ID and restrict option defined on an interface will only form a tunnel with other interfaces with the same tunnel group ID and color.

## Configure Tunnel Groups on Cisco IOS XE Catalyst SD-WAN devices Using CLI

To configure tunnel groups on Cisco IOS XE Catalyst SD-WAN devices:

```
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet2

Device(config-interface-GigabitEthernet2)# tunnel-interface
Device(config-tunnel-interface)#group Group ID
```

## Limit Keepalive Traffic on a Tunnel Interface

By default, Cisco IOS XE Catalyst SD-WAN devices send a Hello packet once per second to determine whether the tunnel interface between two devices is still operational and to keep the tunnel alive. The combination of a hello interval and a hello tolerance determines how long to wait before declaring a DTLS or TLS tunnel to be down. The default hello interval is 1 second, and the default tolerance is 12 seconds. With these default values, if no Hello packet is received within 11 seconds, the tunnel is declared down at 12 seconds.

If the hello interval or the hello tolerance, or both, are different at the two ends of a DTLS or TLS tunnel, the tunnel chooses the interval and tolerance as follows:

- For a tunnel connection between two controller devices, the tunnel uses the lower hello interval and the higher tolerance interval for the connection between the two devices. (Controller devices are Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controller.) This choice is made in case one of the controllers has a slower WAN connection. The hello interval and tolerance times are chosen separately for each pair of controller devices.

- For a tunnel connection between a Cisco IOS XE Catalyst SD-WAN device and any controller device, the tunnel uses the hello interval and tolerance times configured on the router. This choice is made to minimize the amount traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a Cisco IOS XE Catalyst SD-WAN device and a controller device.

To minimize the amount of keepalive traffic on a tunnel interface, increase the Hello packet interval and tolerance on the tunnel interface:

```
Device(config-tunnel-interface)#  hello-interval milliseconds
Device(config-tunnel-interface)#  hello-tolerance seconds
```

The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). The hello tolerance interval must be at most one-half the OMP hold time. The default OMP hold time is 60 seconds, and you configure it with the **omp timers holdtime** command.

# Configure an Interface as a NAT Device

For information on how to configure NAT, see the *Cisco Catalyst SD-WAN NAT Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

# Apply Access Lists and QoS Parameters

Quality of service (QoS) helps determine how a service will perform. By configuring QoS, enhance the performance of an application on the WAN. To configure a shaping rate for an interface and to apply a QoS map, a rewrite rule, access lists, and policers to a interface, click **ACL/QoS**, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS Map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click **On**, and specify the name of the policer to apply to packets received on the interface. |
| Egress Policer | Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

# Add ARP Table Entries

The Address Resolution Protocol (ARP) helps associate a link layer address (such as the MAC address of a device) to its assigned internet layer address. Configure a static ARP address when dynamic mapping is not functional. To configure static ARP table entries on the interface, select ARP. Then click **Add New ARP** and configure the following parameters:

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click **Add**.

To save the feature template, click **Save**.

# Configuring VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click **Add New VRRP** and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Group ID | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>Range: 1 through 255 |
| Priority | Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two routers have the same priority, the one with the higher IP address is elected as primary VRRP router.<br>Range: 1 through 254<br>Default: 100 |
| Timer (milliseconds) | Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP routers.<br>Range: 100 through 40950 milliseconds<br>Default: 100 msecs<br>**Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface. |

| Parameter Name | Description |
|---|---|
| Track OMP<br>Track Prefix List | By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which router is the primary virtual router. if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:<br>**Track OMP**—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.<br>**Track Prefix List**—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the routers determine the primary VRRP router. |
| IP Address | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP. |

## Configure a Prefix List for VRRP

You can configure prefix list tracking for VRRP using device and feature templates. To configure a prefix list, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy**.
2. Click **Localized Policy**.
3. From the **Custom Options** drop-down list, click **Lists**.
4. Click **Prefix** from the left pane, and click **New Prefix List**.
5. In **Prefix List Name**, enter a name for the prefix list.
6. Choose **IPv4** as the **Internet Protocol**.
7. In **Add Prefix**, enter the prefix entries separated by commas.
8. Click **Add**.
9. Click **Next** and configure **Forwarding Classes/QoS**.
10. Click **Next** and configure **Access Control Lists**.
11. Click **Next** and in **Route Policy** pane, select a relevant route policy and click **…** , and click **Edit** to add the newly added prefix list.
12. From the **Match** pane, click **AS Path List** and in the **Address**, choose the newly added prefix list.
13. Click **Save Match and Actions**.
14. Click **Next** and enter the **Policy Name** and **Policy Description** in the **Policy Overview** screen.

15. Click **Save Policy**.

## Configure a Prefix List for VRRP in the Device Template

To configure the Prefix List to the VRRP and the localized policy in the device template, do the following:

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. Select a relevant device template and click **…** and click **Edit** to edit the template details.
4. From **Policy**, select the policy with the newly added prefix list.
5. Click **Update**.
6. Click **Feature Templates**.
7. Select a relevant device template and click **…** and click **Edit** to edit the template details.
8. Click **VRRP**.
9. Select a relevant group ID and click the pen icon to associate the new prefix-list to the VRRP details.
10. Click the **Track Prefix List** drop-down list and enter the newly added prefix-list name.
11. Click **Save Changes**.
12. Click **Update** to save the changes.
13. Click **Device Templates** and select the policy with the newly added prefix list.
14. Click **…** and click **Attach Devices**.
15. From **Available Devices**, double-click the relevant device to move it to **Selected Devices**, and then click **Attach**.

# Configure Advanced Properties

To configure other interface properties, select the **Advanced** tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Duplex | Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode.<br>Default: full |
| MAC Address | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |

| Parameter Name | Description |
|---|---|
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>Range: 576 through 1804<br>Default: 1500 bytes |
| PMTU Discovery | Click **On** to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur. |
| Flow Control | Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface.<br>Values: autonet, both, egress, ingress, none<br>Default: autoneg |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 552 to 1460 bytes<br>Default: None |
| Speed | Specify the speed of the interface for use when the remote end of the connection does not support autonegotiation.<br>Values: 10, 100, 1000, or 10000 Mbps |
| Clear-Dont-Fragment | Click **On** to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.<br>**Note** Clear-Dont-Fragment clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected. |
| Autonegotiation | **Note** For releases before Cisco vManage Release 20.6.1, the default value of the field is **On**. To turn autonegotiation off, click **Off**.<br>From Cisco vManage Release 20.6.1, the default behavior of the field is as follows:<br>• For the Gigabit Ethernet interface type, the **Autonegotiation** field is blank by default. However, the autonegotiation is set to **On** when the field is left blank.<br>• For other interface types such as Ten Gigabit Ethernet and Hundred Gigabit Ethernet, the **Autonegotiation** field is blank by default. To turn autonegotiation on or off, click **On** or **Off** respectively. |

| Parameter Name | Description |
|---|---|
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.<br>Note that TLOC extension over L3 is only supported for Cisco IOS XE routers. If configuring TLOC extension over L3 for a Cisco IOS XE router, enter the IP address of the L3 interface. |
| GRE Tunnel Source IP | Enter the IP address of the extended WAN interface. |
| Xconnect (on IOS XE routers) | Enter the name of a physical interface on the same router that connects to the WAN transport. |

To save the feature template, click **Save**.

# VPN Interface Bridge

Use the VPN Interface Bridge template for all Cisco IOS XE Catalyst SD-WAN device Cloud and Cisco IOS XE Catalyst SD-WAN devices.

Integrated routing and bridging (IRB) allows Cisco IOS XE Catalyst SD-WAN devices in different bridge domains to communicate with each other. To enable IRB, create logical IRB interfaces to connect a bridge domain to a VPN. The VPN provides the Layer 3 routing services necessary so that traffic can be exchanged between different VLANs. Each bridge domain can have a single IRB interface and can connect to a single VPN, and a single VPN can connect to multiple bridge domains on a Cisco IOS XE Catalyst SD-WAN device.

To configure a bridge interface using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Bridge feature template to configure parameters for logical IRB interfaces, as described in this article.
2. Create a Bridge feature template for each bridging domain, to configure the bridging domain parameters. See the Bridge help topic.

### 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. 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. Click **Service VPN** or scroll to the **Service VPN** section.

6. Click the **Service VPN** drop-down list.
7. From **Additional VPN Templates**, click **VPN Interface Bridge**.
8. From the **VPN Interface Bridge** drop-down list, click **Create Template**.

   The VPN Interface Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Bridge parameters.
9. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
10. In **Template Description**, 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 to the left of the parameter field and select one of the following:

***Table 126:***

| 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 Viptela device to a device template .<br><br>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 Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 15.3. In Release 18.2, add support for disabling ICMP redirect messages.

# Create a Bridging Interface

To configure an interface to use for bridging servers, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure bridging.

*Table 127:*

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the interface. |
| Interface name* | Enter the name of the interface, in the format **irb** *number*. The IRB interface number can be from 1 through 63, and must be the same as the VPN identifier configured in the Bridge feature template for the bridging domain that the IRB is connected to. |
| Description | Enter a description for the interface. |
| IPv4 Address* | Enter the IPv4 address of the router. |
| DHCP Helper | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| Block Non-Source IP | Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. |
| Secondary IP Address (on Cisco IOS XE Catalyst SD-WAN devices) | Click **Add** to configure up to four secondary IPv4 addresses for a service-side interface. |

To save the template, click **Save**.

# Apply Access Lists

### Apply Access Lists

To apply access lists to IRB interfaces, select the ACL tab and configure the following parameters. The ACL filter determines what is allowed in or out of a bridging domain:

*Table 128:*

| Parameter Name | Description |
|---|---|
| Ingress ACL – IPv4 | Click **On**, and specify the name of an IPv4 access list to packets being received on the interface. |
| Egress ACL– IPv4 | Click **On**, and specify the name of an IPv4 access list to packets being transmitted on the interface. |

To save the feature template, click **Save**.

# Configure VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, choose **VRRP**. Then click **Add New VRRP** and configure the following parameters:

***Table 129:***

| Parameter Name | Description |
|---|---|
| Group ID | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. *Range:* 1 through 255 |
| Priority | Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If twoCisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as primary VRRP router. *Range:* 1 through 254*Default:* 100 |
| Timer (milliseconds) | Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP router.<br>Range: 100 through 40950 milliseconds<br>Default: 100 msecs<br>**Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface. |
| Track OMP Track Prefix List | By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:<br>Track OMP—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.<br>Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN devices determine the primary VRRP router. |
| IP Address | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP. |

To save the VRRP configuration, click **Add**.

To save the feature template, click **Save**.

# Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, choose **ARP**. Then click **Add New ARP** and configure the following parameters:

***Table 130:***

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click **Add**.

To save the feature template, click **Save**.

# Configure Advanced Properties

To configure other interface properties, click **Advanced** and configure the following parameters:

***Table 131:***

| Parameter Name | Description |
|---|---|
| MAC Address | MAC addresses can be static or dynamic. A static MAC address is manually configured as opposed to a dynamic MAC address that is one learned via an ARP request. You can configure a static MAC on a router's interface or indicate a static MAC that identifies a router's interface.<br>Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| IP MTU | Similar to MTU, IP MTU only affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented.<br>Specify the maximum MTU size of packets on the interface.*Range:* 576 through 1804*Default:* 1500 bytes |

| Parameter Name | Description |
|---|---|
| TCP MSS | TCP MSS will affect any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS will be examined against the MSS exchanged in the three-way handshake. The MSS in the header will be lowered if the configured setting is lower than what is in the header. If the header value is already lower, it will flow through unmodified. The end hosts will use the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set it at 40 bytes lower than the minimum path MTU.<br>Specify the maximum segment size (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 |
| Clear-Dont-Fragment | Configure Clear-Dont-Fragment if there are packets arriving on an interface with the DF bit set. If these packets are larger than the MTU will allow, they are dropped. If you clear the df-bit, the packets will be fragmented and sent.<br>Click **On** to clear the Dont Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.<br>**Note** Clear-Dont-Fragment clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected. |
| ARP Timeout | ARP Timeout controls how long we maintain the ARP cache on a router.<br>Specify how long it takes for a dynamically learned ARP entry to time out.<br>*Range:* 0 through 2678400 seconds (744 hours)*Default:* 1200 seconds (20 minutes) |
| ICMP Redirect | ICMP Redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally.<br>The ICMP Redirect informs the sending host to forward subsequent packets to that same destination through a different gateway.<br>To disable ICMP redirect messages on the interface, click **Disable**. By default, an interface allows ICMP redirect messages. |

To save the feature template, click **Save**.

# VPN Interface DSL IPoE

Use the IPoE template for Cisco IOS XE Catalyst SD-WAN devices.

You configure IPoE on routers with DSL interfaces, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager templates:

1. Create a VPN Interface DSL IPoE feature template to configure IP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

### Navigate to the Template Screen and Name 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, choose **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional VPN 0 Templates**, click **VPN Interface DSL IPoE**.
7. From the **VPN Interface DSL IPoE** drop-down list, choose **Create Template**. The **VPN Interface DSL IPoE** template form is displayed.

   This form contains fields for naming the template, fields for defining the IPoE Interface parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, 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 and choose one of the following:

*Table 132:*

| 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 Viptela device to a device template .<br><br>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 Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Configure IPoE Functionality

To configure basic IPoE functionality, click **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

*Table 133:*

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the VDSL controller interface. |
| Controller VDSL Slot* | Enter the slot number of the controller VDSL interface, in the format *slot*/*subslot*/*port* (for example, 0/2/0). |

| Parameter Name | Description |
|---|---|
| Mode* | Select the operating mode of the VDSL controller from the drop-down:<br>• Auto—Default mode.<br>• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br>• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br>• ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br>• ANSI—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br>• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.. |
| VDSL Modem Configuration | Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager NMS. If the command is not valid, it is not executed. |
| SRA | Click **Yes** to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |

To save the feature template, click **Save**.

### Configure the Ethernet Interface

Configuring an Ethernet interface with PPPoE allows multiple users on a LAN to be connected to a remote site. To configure an Ethernet interface on the VDSL controller, click **Ethernet** and configure the following parameters. You must configure all parameters.

***Table 134:***

| Parameter Name | Description |
|---|---|
| Ethernet Interface Name | Enter a name for the Ethernet interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0. |
| VLAN ID | Enter the VLAN identifier of the Ethernet interface. |
| Description | Enter a description for the interface. |
| Dynamic/Static | Assign a dynamic or static IPv4 address to the Ethernet interface. |
| IPv4 Address | Enter the static IPv4 address of the Ethernet interface. |

| Parameter Name | Description |
|---|---|
| DHCP Helper | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |

To save the feature template, click **Save**.

### Create a Tunnel Interface

On IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

***Table 135:***

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click **On** to create a tunnel interface. |
| Color | Select a color for the TLOC. |

| Parameter Name | Description |
|---|---|
| Control Connection | By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC.<br>**Note** We recommend a minimum of 650-700 Kbps bandwidth with default 10 msec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic.<br>For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth.<br>A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below:<br>• 650 – 700 Kbps per device for control connections.<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (request)<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (response)<br>If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs:<br>A 1500 Bytes BFD request packet is sent per tunnel every 30 secs:<br>1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request)<br>A 147 Bytes BFD packet is sent in response:<br>147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response)<br>Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of:<br>700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps |
| Maximum Control Connections | Specify the maximum number of Cisco Catalyst SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8. *Default:* 2 |
| Cisco Catalyst SD-WAN Validator As STUN Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Controller Group List | Set the Cisco Catalyst SD-WAN Controllers that the tunnel interface is not allowed to connect to. *Range:* 0 through 100 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. *Range:* 0 through 8. *Default:* 5 |

| Parameter Name | Description |
|---|---|
| Port Hop | Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. *Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br>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 |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Allow Service | Choose **On** or **Off** for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

***Table 136:***

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |

| Parameter Name | Description |
|---|---|
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>*Range:* 0 through 4294967295 *Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>*Range:* 1 through 255 *Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default *Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br>**Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. *Range:* 1 through 60 seconds *Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. *Range:* 100 through 10000 milliseconds *Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>*Range:* 12 through 60 seconds *Default:* 12 seconds |

### Configure the Interface as a NAT Device

To configure an interface to act as a NAT device for applications such as port forwarding, click **NAT**, click **On**, and configure the following parameters:

***Table 137:***

| Parameter Name | Description |
|---|---|
| NAT | Click **On** to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). *Default*: Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out. *Range*: 1 through 65536 minutes *Default*: 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out. *Range*: 1 through 65536 minutes *Default*: 60 minutes (1 hour) |
| Block ICMP | Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. *Default*: Off |
| Respond to Ping | Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

***Table 138:***

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest. *Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. *Range:* 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. *Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click **Add**.

To save the feature template, click **Save**.

### Apply Access Lists

Configure ACLs to selectively indicate what traffic will enjoy the benefits of QoS. To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

***Table 139:***

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click **On**, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

### Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

***Table 140:***

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream | When the bandwidth of traffic transmitted on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager NMSs only), BW Uptream issues notifications.<br>For transmitted traffic, set the bandwidth above which to generate notifications. *Range:* 1 through $(2^{32} / 2) – 1$ kbps |

| Parameter Name | Description |
|---|---|
| Bandwidth Downstream | When the bandwidth of traffic received on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager NMSs only), BW Downtream issues notifications.<br><br>For received traffic, set the bandwidth above which to generate notifications. *Range:* 1 through $(2^{32} / 2) – 1$ kbps |
| IP MTU | IP MTU affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented.<br><br>Specify the maximum MTU size of packets on the interface. *Range:* 576 through 1804 *Default:* 1500 bytes |
| TCP MSS | In a single TCP/IPv4 datagram, the TCP Maximum Segment Size (MSS) defines the maximum data that a host will accept. This TCP/IPv4 datagram might be fragmented at the IPv4 layer. The MSS value is sent as a TCP header option only in TCP SYN segments.<br><br>Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. 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 |
| TLOC Extension | Use a TLOC Extension to bind an interface and connect another Cisco IOS XE Catalyst SD-WAN device at the same physical site to the local router's WAN transport interface (on Cisco IOS XE Catalyst SD-WAN devices only).<br><br>Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Tracker | Tracking the interface status is useful when you enable NAT on 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 on 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.<br><br>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 again functioning, the route to the internet is reinstalled.<br><br>Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |

| Parameter Name | Description |
|---|---|
| IP Directed-Broadcast | An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.<br><br>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.<br><br>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet. |

To save the feature template, click **Save**.

### Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.4.1.

# VPN Interface DSL PPPoA

To provide support for service provider digital subscriber line (DSL) functionality, configure PPP-over-ATM interfaces on routers with DSL NIM modules.

Use the VPN Interface DSL PPPoA template for Cisco IOS XE Catalyst SD-WAN devices.

You configure PPP-over-ATM interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using Cisco SD-WAN Manager templates:

1. Create a VPN Interface DSL PPPoA feature template to configure ATM interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

### 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. 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. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional VPN 0 Templates**, click **VPN Interface DSL PPPoA**.
7. From the **VPN Interface DSL PPPoA** drop-down list, click **Create Template**. The VPN Interface DSL PPPoA template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface PPP parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, 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 to the left of the parameter field and select one of the following:

***Table 141:***

| 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 Viptela device to a device template .<br><br>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 Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Configure VDSL Controller Functionality

To configure basic VDSL controller functionality in a VPN, select **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

***Table 142:***

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the VDSL controller interface. |

| Parameter Name | Description |
|---|---|
| Controller VDSL Slot* | Enter the slot number of the controller VDSL interface, in the format *slot*/*subslot*/*port* (for example, 0/2/0). |
| Mode* | Select the operating mode of the VDSL controller from the drop-down:<br>• **Auto**—Default mode.<br>• **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br>• **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br>• **ADSL2+**— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br>• **ANSI**—Operate in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br>• **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps. |
| VDSL Modem Configuration | Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager NMS. If the command is not valid, it is not executed. |
| SRA | Enabled by default. Click **No** to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |

To save the feature template, click **Save**.

### Configure the ATM Interface

To configure an ATM interface on the VDSL controller, select **ATM** and configure the following parameters. You must configure all parameters.

***Table 143:***

| Parameter Name | Description |
|---|---|
| ATM Interface Name | Enter a name for the ATM interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0. |
| Description | Enter a description for the interface. |
| VPI and VCI | Create an ATM permanent virtual circuit (PVC), in the format *vpi*/*vci*, Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI). |

| Parameter Name | Description |
|---|---|
| Encapsulation | Select the ATM adaptation layer (AAL) and encapsulation type to use on the ATM PVC from the drop-down list:<br>• AAL5 MUX—Dedicate the PVC to a single protocol.<br>• AAL5 NLPID—Use NLPID multiplexing.<br>• AAL5 SNAP—Multiplex two or more protocols on the same PVC. |
| Dialer Pool Member | Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255. |
| VBR-NRT | Configure variable bit rate non-real-time parameters:<br>• Peak Cell Rate—Enter a value from 48 through 25000 Kbps.<br>• Sustainable Cell Rate—Enter the sustainable cell rate, in Kbps.<br>• Maximum Burst Size—This size can be 1 cell. |
| VBR-RT | Configure variable bit rate real-time parameters:<br>• Peak Cell Rate—Enter a value from 48 through 25000 Kbps.<br>• Average Cell Rate—Enter the average cell rate, in Kpbs.<br>• Maximum Burst Size—This size can be 1 cell. |

To save the feature template, click **Save**.

### Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select **PPP** and configure the following parameters:

***Table 144:***

| Parameter Name | Description |
|---|---|
| Authentication Protocol | Select the authentication protocol used by the MLP:<br>• **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP**—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br>• **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click **Save**.

### Create a Tunnel Interface

On Cisco IOS XE Catalyst SD-WAN devices, you can configure up to eight tunnel interfaces. This means that each Cisco IOS XE Catalyst SD-WAN device can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select **Tunnel Interface** and configure the following parameters:

***Table 145:***

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click **On** to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | If the Cisco IOS XE Catalyst SD-WAN device has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.<br>**Note** For control connection traffic without dropping any data, a minimum of 650-700 kbps bandwidth is recommended with default parameters configured for hello-interval (10) and hello-tolerance (12). |
| Maximum Control Connections | Specify the maximum number of Cisco Catalyst SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8 *Default:* 2 |
| Cisco Catalyst SD-WAN Validator As STUN Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT. |
| Exclude Controller Group List | Set the Cisco Catalyst SD-WAN Controllers that the tunnel interface is not allowed to connect to. *Range:* 0 through 100 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. *Range:* 0 through 8 *Default:* 5 |
| Port Hop | Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value.*Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |

| Parameter Name | Description |
|---|---|
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br>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 |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Allow Service | Select **On** or **Off** for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

***Table 146:***

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>*Range:* 0 through 4294967295. *Default:* 0 |

| Parameter Name | Description |
|---|---|
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>*Range:* 1 through 255. *Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. *Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br>**Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. *Range:* 1 through 60 seconds. *Default:* 5 seconds. |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. *Range:* 100 through 10000 milliseconds. *Default:* 1000 milliseconds (1 second). |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>*Range:* 12 through 60 seconds. *Default:* 12 seconds. |

### Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select **ACL** and configure the following parameters:

*Table 147:*

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click **On**, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

### Configure Other Interface Properties

To configure other interface properties, select **Advanced** and configure the following properties:

*Table 148:*

| Parameter Name | Description |
|---|---|
| PMTU Discovery | Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. |
| TCP MSS | Specify the maximum segment size (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. |
| Clear Dont Fragment | Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS | Select a queue number to use for incoming traffic. *Range:0 through 7* |
| Autonegotiate | Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |

| Parameter Name | Description |
|---|---|
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second Cisco IOS XE Catalyst SD-WAN device at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |

To save the feature template, click **Save**.

### Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.3.

# VPN Interface DSL PPPoE

Use the VPN Interface DSL PPPoE template for Cisco IOS XE Catalyst SD-WAN devices.

You configure PPP-over-Ethernet interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using Cisco SD-WAN Manager templates:

1. Create a VPN Interface DSL PPPoE feature template to configure PPP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

### 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. 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. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional VPN 0 Templates**, click **VPN Interface DSL PPPoE**.
7. From the **VPN Interface DSL PPPoE** drop-down list, click **Create Template**. The VPN Interface DSL PPPoE template form is displayed. This form contains fields for naming the template, and fields for defining PPPoE Interface parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In **Template Description**, 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 to the left of the parameter field and select one of the following:

***Table 149:***

| 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 Viptela device to a device template .<br><br>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 Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Configure VDSL Controller Functionality

To configure basic VDSL controller functionality in a VPN, select **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

**Note** If your deployment includes devices with DSL, you must include DSL interface templates in Cisco SD-WAN Manager, even if these templates are not used.

***Table 150:***

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the VDSL controller interface. |
| Controller VDSL Slot* | Enter the slot number of the controller VDSL interface, in the format *slot*/*subslot*/*port* (for example, 0/2/0). |

| Parameter Name | Description |
|---|---|
| Mode* | Select the operating mode of the VDSL controller from the drop-down:<br>• **Auto**—Default mode.<br>• **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br>• **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br>• **ADSL2+**— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br>• **ANSI**—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br>• **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.. |
| VDSL Modem Configuration | Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager NMS. If the command is not valid, it is not executed. |
| SRA | Click **Yes** to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |

To save the feature template, click **Save**.

### Configure the Ethernet Interface on VDSL Controller

To configure an Ethernet interface on the VDSL controller, select **Ethernet** and configure the following parameters. You must configure all parameters.

*Table 151: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support for Dialer Interface in DSL | Cisco IOS XE Release 17.3.2<br>Cisco vManage Release 20.3.1 | This feature enables tracking of a Point-to-Point Protocol (PPP) session over a dialer interface on Cisco IOS XE Catalyst SD-WAN devices.<br>Dialer interface is used in Digital Subscriber Line (DSL) in the deployments of Point-to-Point Protocol over Ethernet (PPPoE), Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA). Dialer interface always stay up irrespective of the PPP session status. This helps to avoid the need for additional configuration such as IP SLA and tracking for routing failover to work while using dialer interfaces.<br>The following command is added to configure dialer down-with-vInterface which brings the dialer interface down when the PPP session goes down. |

*Table 152:*

| Parameter Name | Description |
|---|---|
| Ethernet Interface Name | Enter a name for the Ethernet interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0. |
| VLAN ID | Enter the VLAN identifier of the Ethernet interface. |
| Description | Enter a description for the interface. |
| Dialer Pool Member | Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255. |
| PPP Max Payload | Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. *Range:* 64 through 1792 bytes |
| Dialer IP | Configure the IP prefix of the dialer interface. This prefix is that of the node in the destination that the interface calls.<br>• Negotiated—Use the address that is obtained during IPCP negotiation. |

To save the feature template, click **Save**.

### Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select **PPP** and configure the following parameters:

*Table 153:*

| Parameter Name | Description |
|---|---|
| Authentication Protocol | Select the authentication protocol used by the MLP:<br>• **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP**—Enter the username and password that are provided by your ISP. *username* can be up to 255 characters.<br>• **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click **Save**.

### Create a Tunnel Interface

On IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

*Table 154:*

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click **On** to create a tunnel interface. |
| Color | Select a color for the TLOC. |

| Parameter Name | Description |
|---|---|
| Control Connection | By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC.<br>**Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic.<br>For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth.<br>A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below:<br>• 650 – 700 Kbps per device for control connections.<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (request)<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (response)<br>If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs:<br>A 1500 Bytes BFD request packet is sent per tunnel every 30 secs:<br>1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request)<br>A 147 Bytes BFD packet is sent in response:<br>147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response)<br>Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of:<br>700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps<br>• STATE—specifies the vdaemon control state.<br>Last Connection—If no control connection on that WAN interface, the uptime of the device is lifted.<br>SPI Time Remaining—countdown to the next change in SPI for IPSec. The countdown starts at half of the rekey time. |
| Maximum Control Connections | Specify the maximum number of Cisco Catalyst SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8 *Default:* 2 |
| Cisco Catalyst SD-WAN Validator As STUN Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Controller Group List | Set the Cisco Catalyst SD-WAN Controllers that the tunnel interface is not allowed to connect to. *Range:* 0 through 100 |

| Parameter Name | Description |
|---|---|
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. *Range:* 0 through 8 *Default:* 5 |
| Port Hop | Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. *Default:* Enabled. |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br><br>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 |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br><br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br><br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Allow Service | Select **On** or **On** for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

***Table 155:***

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |

| Parameter Name | Description |
|---|---|
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>*Range:* 0 through 4294967295 *Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>*Range:* 1 through 255 *Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default *Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br>**Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets that are sent on a DTLS or TLS WAN transport connection. *Range:* 1 through 60 seconds. *Default:* 5 seconds. |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. *Range:* 100 through 10000 milliseconds. *Default:* 1000 milliseconds (1 second). |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>*Range:* 12 through 60 seconds. *Default:* 12 seconds. |

### Configure the Interface as a NAT Device

To configure an interface to act as a NAT device for applications such as port forwarding, select **NAT**, click **On** and configure the following parameters:

***Table 156:***

| Parameter Name | Description |
|---|---|
| NAT | Click **On** to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). *Default*: Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out. *Range*: 1 through 65536 minutes *Default*: 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out. *Range*: 1 through 65536 minutes *Default*: 60 minutes (1 hour) |
| Block ICMP | Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. *Default*: Off |
| Respond to Ping | Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

***Table 157:***

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest. *Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. *Range:* 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. *Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click **Add**.

To save the feature template, click **Save**.

### Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select **ACL** and configure the following parameters:

***Table 158:***

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click **On**, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

### Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

***Table 159:***

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications. *Range:* 1 through $(2^{32} / 2) – 1$ kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications. *Range:* 1 through $(2^{32} / 2) – 1$ kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface. *Range:* 576 through 1804. *Default:* 1500 bytes. |

| Parameter Name | Description |
|---|---|
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. 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. |
| Clear Dont Fragment | Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |

To save the feature template, click **Save**.

### Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.3.

# VPN Interface Ethernet PPPoE

Use the PPPoE template for Cisco IOS XE Catalyst SD-WAN devices.

You configure PPPoE over GigabitEthernet interfaces on Cisco IOS XE routers, to provide PPPoE client support.

To configure interfaces on Cisco routers using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Ethernet PPPoE feature template to configure Ethernet PPPoE interface parameters, as described in this section.
2. Create a VPN feature template to configure VPN parameters. See VPN help topic.

### Navigate to the Template Screen and Name 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, choose **From Feature Template**.

4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional VPN 0 Templates**, click **VPN Interface Ethernet PPPoE**.
7. From the **VPN Interface Ethernet PPPoE** drop-down list, click **Create Template**. The VPN Interface Ethernet PPPoE template form is displayed.

   This form contains fields for naming the template, and fields for defining the Ethernet PPPoE parameters.

8. In **Template Name**, enter a name for the template.

   The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, 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 and select one of the following:

***Table 160:***

| 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 Catalyst SD-WAN device to a device template .<br><br>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 Catalyst SD-WAN device to a device template. For more information, see Create a Template Variables Spreadsheet .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Configure PPPoE Functionality

To configure basic PPPoE functionality, click **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

*Table 161:*

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the GigabitEthernet interface. |
| Ethernet Interface Name | Enter the name of a GigabitEthernet interface.<br>For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**). |
| VLAN ID | VLAN tag of the sub-interface. |
| Description | Enter a description of the Ethernet-PPPoE-enabled interface. |
| Dialer Pool Member | Enter the number of the dialer pool to which the interface belongs.<br>*Range*: 100 to 255. |
| PPP Maximum Payload | Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. *Range*: 64 through 1792 bytes |

To save the feature template, click **Save**.

### Configure the PPP Authentication Protocol

To configure the PPP Authentication Protocol, click **PPP** and configure the following parameters. Required parameters are indicated with an asterisk.

*Table 162:*

| Parameter Name | Description |
|---|---|
| PPP Authentication Protocol | Select the authentication protocol used by the MLP:<br>• **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP**—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br>• **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click **Save**.

### Create a Tunnel Interface

On IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select **Tunnel Interface** and configure the following parameters:

***Table 163:***

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click **On** to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC.<br>**Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic.<br>For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth.<br>A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below:<br>• 650 – 700 Kbps per device for control connections.<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (request)<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (response)<br>If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs:<br>A 1500 Bytes BFD request packet is sent per tunnel every 30 secs:<br>1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request)<br>A 147 Bytes BFD packet is sent in response:<br>147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response)<br>Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of:<br>700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps |
| Maximum Control Connections | Specify the maximum number of Cisco Catalyst SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8 *Default:* 2 |
| Cisco Catalyst SD-WAN Validator As STUN Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |

| Parameter Name | Description |
|---|---|
| Exclude Controller Group List | Set the Cisco Catalyst SD-WAN Controllers that the tunnel interface is not allowed to connect to. *Range:* 0 through 100 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. *Range:* 0 through 8 *Default:* 5 |
| Port Hop | Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. *Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select **On** or **Off** for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

***Table 164:***

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>*Range:* 0 through 4294967295. *Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>*Range:* 1 through 255. *Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. *Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |

| Parameter Name | Description |
|---|---|
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br>**Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.<br>**Note** Configuring administrative distance values on primary interface routes is not supported. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. *Range:* 1 through 60 seconds. *Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. *Range:* 100 through 10000 milliseconds. *Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>*Range:* 12 through 60 seconds. *Default:* 12 seconds |

### Configure the Interface as a NAT Device

To configure an interface to act as a NAT device for applications such as port forwarding, select **NAT**, click **On** and configure the following parameters:

***Table 165:***

| Parameter Name | Description |
|---|---|
| NAT | Click **On** to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). *Default*: Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out. *Range*: 1 through 65536 minutes. *Default*: 1 minutes |

| Parameter Name | Description |
|---|---|
| TCP Timeout | Specify when NAT translations over TCP sessions time out. *Range*: 1 through 65536 minutes. *Default*: 60 minutes (1 hour) |
| Block ICMP | Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. *Default*: Off |
| Respond to Ping | Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

***Table 166:***

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest. *Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. *Range:* 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. *Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click **Add**.

To save the feature template, click **Save**.

### Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, click **ACL** and configure the following parameters:

***Table 167:***

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |

| Parameter Name | Description |
|---|---|
| Rewrite Rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click **On**, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

### Configure Other Interface Properties

To configure other interface properties, click **Advanced** and configure the following properties:

***Table 168:***

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications. *Range:* 1 through $(2^{32} / 2) – 1$ kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications. *Range:* 1 through $(2^{32} / 2) – 1$ kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface. *Range:* 576 through 1804. *Default:* 1500 bytes |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. 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 |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |

| Parameter Name | Description |
|---|---|
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| IP Directed-Broadcast | Enables translation of a directed broadcast to physical broadcasts. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. |

To save the feature template, click **Save**.

### Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.4.1.

# Cisco VPN Interface GRE

When a service, such as a firewall, is available on a device that supports only GRE tunnels, you can configure a GRE tunnel on the device to connect to the remote device by configuring a logical GRE interface. You then advertise that the service is available via a GRE tunnel, and you can create data policies to direct the appropriate traffic to the tunnel. GRE interfaces come up as soon as they are configured, and they stay up as long as the physical tunnel interface is up.

To configure GRE interfaces using Cisco SD-WAN Manager templates:

1. Create a Cisco VPN Interface GRE feature template to configure a GRE interface.
2. Create a Cisco VPN feature template to advertise a service that is reachable via a GRE tunnel, to configure GRE-specific static routes, and to configure other VPN parameters.
3. Create a data policy on the Cisco Catalyst SD-WAN Controller that applies to the service VPN, including a **set-service** *service-name* **local** command.

### Navigate to the Template Screen and Name 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. To create a template for VPN 0 or VPN 512:
   a. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
   b. Under **Additional VPN 0 Templates**, click **VPN Interface GRE**.

c. From the **VPN Interface GRE** drop-down list, click **Create Template**. The VPN Interface GRE template form is displayed.

   This form contains fields for naming the template, and fields for defining the VPN Interface GRE parameters.

6. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In **Template Description**, 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 to the left of the parameter field and select the paramater scope.

### Configuring a Basic GRE Interface

To configure a basic GRE interface, click **Basic Configuration** and then configure the following parameters. Parameters marked with an asterisk are required to configure a GRE interface.

***Table 169:***

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **Off** to enable the interface. |
| Interface Name* | Enter the name of the GRE interface, in the format **gre** *number*. *number* can be from 1 through 255. |
| Description | Enter a description of the GRE interface. |
| Source* | Enter the source of the GRE interface:<br>• GRE Source IP Address—Enter the source IP address of the GRE tunnel interface. This address is on the local router. This address is on the local router. GRE keepalives can not be configured when source configured as IP address.<br>• Tunnel Source Interface—Enter the physical interface that is the source of the GRE tunnel. GRE keepalives can not be configured when source configured as loopback interface.<br>• If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name. |
| Destination* | Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. If this tunnel connects to a Secure Internet Gateway (SIG), specify the URL for the SIG. |
| GRE Destination IP Address* | Enter the destination IP address of the GRE tunnel interface. This address is on a remote device |

| Parameter Name | Description |
|---|---|
| IPv4 Address | Enter an IPv4 address for the GRE tunnel. |
| IP MTU | Specify the maximum MTU size of packets on the interface. *Range:* 576 through 1804 *Default:* 1500 bytes |
| Clear-Dont-Fragment | Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco vEdge 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 |

To save the feature template, click **Save**.

### Configure Interface Access Lists

To configure access lists on a GRE interface, click **ACL** and configure the following parameters:

***Table 170:***

| Parameter Name | Description |
|---|---|
| Rewrite Rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |

### Configure Tracker Interface

To configure a tracker interface to track the status of a GRE interface, select **Advanced** and configure the following parameter:

***Table 171:***

| Parameter Name | Description |
|---|---|
| Tracker | Enter the name of a tracker to track the status of GRE interfaces that connect to the Internet. |

# GRE-in-UDP

*Table 172: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| GRE-in-UDP | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>Cisco Catalyst SD-WAN Control Components Release 20.11.1 | You can configure GRE encapsulation for UDP transport. |

## Information About GRE-in-UDP

Cisco Catalyst SD-WAN supports generic routing encapsulation (GRE) with UDP for IPv4 and IPv6 traffic.

With a GRE-in-UDP tunnel, a router encapsulates GRE packets, containing information such as the source and destination ports, within a UDP header. The router sends the UDP packet through the tunnel. The destination device de-encapsulates the UDP packet.

## Supported Devices for GRE-in-UDP

Cisco IOS XE Catalyst SD-WAN devices.

## Prerequisites for GRE-in-UDP

Configure GRE encapsulation.

## Restrictions for GRE-in-UDP

Any restricitions that apply to GRE encapsulaton apply to GRE-in-UDP.

## Configure GRE-in-UDP Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

You can configure GRE-in-UDP tunnel only through a CLI template.

1. For the desired interface, enter interface configuration mode.

```
sdwan
interface interface
```

2. Enter tunnel interface mode.

   ```
   tunnel-interface
   ```

3. Configure GRE encapsulation.

   ```
   encapsulation gre
   ```

4. Configure GRE-in-UDP as the encapsulation mode.

   ```
   gre-in-udp
   ```

**Example**

Here is a complete example of configuring GRE-in-UDP.

```
interface GigabitEthernet1
  tunnel-interface
   encapsulation gre
   color lte
   gre-in-udp
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no 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
```

# VPN Interface IPsec

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65530, except for 512.

Cisco Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. In Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

## Create VPN IPsec Interface Template

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

**Step 2** Click **Feature Templates**.

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

**Step 3** Click **Add Template**.

**Step 4** Choose a Cisco IOS XE Catalyst SD-WAN device from the list.

**Step 5** From the VPN section, click **VPN Interface IPsec**. The Cisco VPN Interface IPsec template displays.

**Step 6** In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

**Step 7** In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

# Basic Configuration

To configure a basic IPsec tunnel interface select **Basic Configuration** and configure the following parameters:

| Parameter Name | Options/Format | Description |
|---|---|---|
| Shutdown* | **Yes** / **No** | Click **No** to enable the interface; click **Yes** to disable. |
| Interface Name* | **ipsec** *number* (1…255) | Enter the name of the IPsec interface. *Number* can be from 1 through 255. |
| Description | Enter a description of the IPsec interface. | |
| IPv4 Address* | *ipv4-prefix/length* | Enter the IPv4 address of the IPsec interface. The address must have a **/30** subnet. |
| Source * | Set the source of the IPsec tunnel that is being used for IKE key exchange: | |
| | **IP Address** | Click and enter the IPv4 address that is the source tunnel interface. This address must be configured in **VPN 0**. |
| | **Interface** | Click and enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in **VPN 0**.<br>• If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name.<br>**Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route. |

| Parameter Name | Options/Format | Description |
|---|---|---|
| Destination* | Set the destination of the IPsec tunnel that is being used for IKE key exchange. | |
| | **IPsec Destination IP Address** | Enter an IPv4 address that points to the destination. |
| | **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1960 bytes<br>*Default:* None |
| | **IP MTU** | Specify the maximum transmission unit (MTU) size of packets on the interface.<br>*Range:* 576 through 2000<br>*Default:* 1500 bytes |

### CLI Equivalent

```
crypto
   interface tunnel ifnum
      no shutdown
      vrf forwarding vrf_id
      ip address ip_address[mask]
      tunnel source wanif_ip
      tunnel mode {ipsec ipv4 | gre ip}
      tunnel destination gateway_ip
      tunnel protection ipsec profile ipsec_profile_name
```

# Configure Dead-Peer Detection

To configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable, click DPD and configure the following parameters:

| Parameter Name | Description |
|---|---|
| DPD Interval | Specify the interval for IKE to send Hello packets on the connection.<br>Range: 10 through 3600 seconds<br>Default: Disabled |
| DPD Retries | Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer.<br>Range: 2 through 60<br>Default: 3 |

To save the feature template, click **Save**.

### CLI Equivalent

```
crypto
   ikev2
      profile ikev2_profile_name
         dpd 10-3600 2-60 {on-demand | periodic}
```

# Configure IKE

*Table 173: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| SHA256 Support for IPSec Tunnels | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | This feature adds support for `HMAC_SHA256` algorithms for enhanced security. |

To configure IKE, click **IKE** and configure the following parameters:

**Note** When you create an IPsec tunnel on a Cisco IOS XE Catalyst SD-WAN device, IKE Version 1 is enabled by default on the tunnel interface.

### IKE Version 1 and IKE Version 2

To configure the IPsec tunnel that carries IKEv1 and IKEv2 traffic, click **IPSEC** and configure the following parameters:

| Parameter Name | Options | Description |
|---|---|---|
| **IKE Version** | **1** IKEv1<br>**2** IKEv2 | Enter **1** to choose IKEv1.<br>Enter **2** to choose IKEv2.<br>*Default*: IKEv1 |

| Parameter Name | Options | Description |
|---|---|---|
| **IKE Mode** | **Aggressive mode**<br>**Main mode** | For IKEv1 only, specify one of the following modes:<br>• Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear.<br>• Establishes an IKE SA session before starting IPsec negotiations.<br>**Note** For IKEv2, there is no mode.<br>**Note** IKE aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen.<br>*Default*: Main mode |
| **IPsec Rekey Interval** | 3600 - 1209600 seconds | Specify the interval for refreshing IKE keys.<br>*Range*: 1 hour through 14 days<br>*Default*: 14400 seconds (4 hours) |
| **IKE Cipher Suite** | • AES 256 CBC SHA 256<br>• AES 256 CBC SHA 384<br>• AES 256 CBC SHA 512<br>• AES 256 CBC SHA 1<br>• AES 256 GCM<br>• Nul SHA 256<br>• Nul SHA 384<br>• Nul SHA 512<br>• Nul SHA 1 | Specify the type of authentication and encryption to use during IKE key exchange.<br>*Default*: AES 256 CBC SHA 1 |

| Parameter Name | Options | Description |
|---|---|---|
| **IKE Diffie-Hellman Group** | **2**<br>**14**<br>**15**<br>**16** | Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.<br>• 1024-bit modulus<br>• 2048-bit modulus<br>• 3072-bit modulus<br>• 4096-bit modulus<br>*Default*: 4096-bit modulus |
| **IKE Authentication** | Configure IKE authentication. | |
| | **Preshared Key** | Enter the password to use with the preshared key. |
| | **IKE ID for Local End Point** | If the remote IKE peer requires a local end point identifier, specify it.<br>*Range*: 1 through 64 characters<br>*Default*: Tunnel's source IP address |
| | **IKE ID for Remote End Point** | If the remote IKE peer requires a remote end point identifier, specify it.<br>*Range*: 1 through 64 characters<br>*Default*: Tunnel's destination IP address |

To save the feature template, click **Save**.

### Change the IKE Version from IKEv1 to IKEv2

To change the IKE version, do 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.x and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Click **Basic Configuration**.
5. Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.
6. Remove the ISAKMP profile from the IPsec profile.

7. Attach the IKEv2 profile with the IPsec profile.

**Note** Perform this step if you already have an IKEv2 profile. Otherwise, create an IKEv2 profile first.

8. Use the **shutdown** parameter with the **no** option (**no shutdown**) to start up the tunnel.

**Note** You must issue the **shutdown** operations in two separate operations.

**Note** There is no single CLI for changing the IKE version. You need to follow the sequence of steps listed in the Change the IKE Version from IKEv1 to IKEv2 section.

### CLI Equivalents for IKEv1

#### ISAKMP CLI Configuration for IKEv1

```
crypto
   isakmp
      keepalive 60-86400 2-60 {on-demand | periodic}
      policy policy_num
         encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
         hash {sha384 | sha256 | sha}
         authentication pre-share
         group {2 | 14 | 16 | 19 | 20 | 21}
         lifetime 60-86400
      profile ikev1_profile_name
         match identity address ip_address [mask]
         keyring keyring_name
```

#### IPsec CLI Configuration for IKEv1

```
profile ipsec_profile_name
         set transform-set transform_set_name
         set isakmp-profile ikev1_profile_name
         set security-association
            lifetime {kilobytes disable | seconds 120-2592000}
            replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
         set pfs group {14 | 16 | 19 | 20 | 21}
   keyring keyring_name
      pre-shared-key address ip_address [mask] key key_string
   ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac |
esp-sha256-hmac] mode tunnel
```

### Summary Steps

1. enable
2. configure terminal
3. crypto isakmp policy *priority*
4. encryption {des | 3des | aes | aes 192 | aes 256 }

5. hash {sha | sha256 | sha384 | md5 }
6. authentication {rsa-sig | rsa-encr | pre-share }
7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 }
8. lifetime *seconds*
9. exit
10. exit

### CLI Equivalent for IKE2

```
crypto
   ikev2
      proposal proposal_name
         encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
         integrity {sha256 | sha384 | sha512}
         group {2 | 14 | 15 | 16}
      keyring idev2_keyring_name
         peer peer_name
         address tunnel_dest_ip [mask]
         pre-shared-key key_string
      profile ikev2_profile_name
         match identity remote address ip_address
         authentication {remote | local} pre-share
         keyring local ikev2_keyring_name
         lifetime 120-86400
```

# Configure IPsec Tunnel Parameters

To configure the IPsec tunnel that carries Internet Key Exchange (IKE) traffic, click IPsec and configure the following parameters:

| Parameter Name | Options | Description |
|---|---|---|
| **IPsec Rekey Interval** | 3600 - 1209600 seconds | Specify the interval for refreshing IKE keys.<br>Range: 1 hour through 14 days<br>Default: 3600 seconds |
| **IKE Replay Window** | 64, 128, 256, 512, 1024, 2048, 4096, 8192 | Specify the replay window size for the IPsec tunnel.<br>Default: 512 |
| **IPsec Cipher Suite** | aes256-cbc-sha1<br>aes256-gcm<br>null-sha1 | Specify the authentication and encryption to use on the IPsec tunnel<br>Default: aes256-gcm |

| Parameter Name | Options | Description |
|---|---|---|
| **Perfect Forward Secrecy** | **2** 1024-bit modulus<br>**14** 2048-bit modulus<br>**15** 3072-bit modulus<br>**16** 4096-bit modulus<br>**none** | Specify the PFS settings to use on the IPsec tunnel.<br>Choose one of the following Diffie-Hellman prime modulus groups:<br>1024-bit – group-2<br>2048-bit – group-14<br>3072-bit – group-15<br>4096-bit – group-16<br>none –disable PFS.<br>*Default*: group-16 |

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, as part of the security hardening, the weaker ciphers are deprecated. As part of this change, the option to configure Diffie-Hellman (DH) groups 1, 2, and 5 is no longer supported. DH groups are used in IKE to establish session keys and are also available in IPsec as support for perfect forward secrecy.

To save the feature template, click **Save**.

### CLI Equivalent

```
crypto
   ipsec
      profile ipsec_profile_name
         set ikev2-profile ikev2_profile_name
         set security-association
            lifetime {seconds 120-2592000 | kilobytes disable}
            replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}
         set pfs group {2 | 14 | 15 | 16 | none}
         set transform-set transform_set_name
```

# VPN Interface Multilink

Use the VPN Interface Multilink template for Cisco IOS XE Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

**Note** Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. When you complete the configuration, the system automatically maps the VPN configurations to VRF configurations.

Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

To configure multilink on Cisco IOS XE Catalyst SD-WAN Device using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Multilink feature template to configure multilink interface properties.
2. Optionally, create a VPN feature template to modify the default configuration of VPN 0.

### 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. 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. If you are configuring the multilink interface in the transport VPN (VPN 0):
   a. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
   b. Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.
6. If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0):
   a. Click **Service VPN** or scroll to the **Service VPN** section.
   b. In the Service **VPN** drop-down list, enter the number of the service VPN.
   c. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.
7. From the **VPN Interface Multilink Controller** drop-down list, click **Create Template**. The VPN Multilink template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, 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 to the left of the parameter field and select one of the following:

*Table 174:*

| 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 Viptela device to a device template .<br><br>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 Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>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.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Configure a Multilink Interface

To configure a multilink interface, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

**Note** If you are creating a VPN Interface Multilink template, you do not need to create a T1/E1 Controller template or a VPN Interface T1/E1 template.

*Table 175:*

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the multilink interface. |
| Interface Name* | Enter the number of the MLP interface. It can be a number from 1 through 65,535. |
| Description | Enter a description for the multilink interface. |
| Multilink Group Number* | Enter the number of the multilink group. It can be a number from 1 through 65,535 but it must be the same as the number you enter in the Multilink Interface Name parameter. |

| Parameter Name | Description |
|---|---|
| IPv4 Address* | To configure a static address, click **Static** and enter an IPv4 address.<br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. |
| IPv6 Address* | To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.<br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications. *Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications. *Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. *Range:* 576 through 1804 *Default:* 1500 bytes |

To save the feature template, click **Save**.

### Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select **PPP** and configure the following parameters:

***Table 176:***

| Parameter Name | Description |
|---|---|
| Authentication Protocol | Select the authentication protocol used by the MLP:<br>• **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• **PAP**—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br>• **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click **Save**.

### Create a Tunnel Interface

You can configure up to eight tunnel interfaces. This means that each device can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the **Tunnel Interface** tab and configure the following parameters:

***Table 177:***

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click **On** to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC.<br>**Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic.<br>For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth.<br>A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below:<br>• 650 – 700 Kbps per device for control connections.<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (request)<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (response)<br>If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs:<br>A 1500 Bytes BFD request packet is sent per tunnel every 30 secs:<br>1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request)<br>A 147 Bytes BFD packet is sent in response:<br>147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response)<br>Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of:<br>700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps |
| Maximum Control Connections | Specify the maximum number of Cisco Catalyst SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8 *Default:* 2 |

| Parameter Name | Description |
|---|---|
| vBond As STUN Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the device is located behind a NAT. |
| Exclude Controller Group List | Set the Cisco Catalyst SD-WAN Controller that the tunnel interface is not allowed to connect to. *Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. *Range:* 0 through 8 *Default:* 5 |
| Port Hop | Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. *Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br><br>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 |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br><br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br><br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Allow Service | Select **On** or **Off** for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

*Table 178:*

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>*Range:* 0 through 4294967295. *Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>*Range:* 1 through 255. *Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. *Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort.<br>**Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. *Range:* 1 through 60 seconds. *Default:* 5 seconds |

| Parameter Name | Description |
|---|---|
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. *Range:* 100 through 10000 milliseconds. *Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br>*Range:* 12 through 60 seconds. *Default:* 12 seconds |

### Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select **ACL** and configure the following parameters:

***Table 179:***

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click **On**, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

### Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

*Table 180:*

| Parameter Name | Description |
|---|---|
| PMTU Discovery | Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco 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 |
| Clear Dont Fragment | Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS | Select a queue number to use for incoming traffic. *Range: 0 through 7* |
| Auto negotiate | Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second Cisco Catalyst SD-WAN device at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |

To save the feature template, click **Save**.

### Release Information

Introduced in Cisco SD-WAN Manager in Release 18.3.

# Configure VPN Interface SVI using Cisco SD-WAN Manager

Use the VPN Interface SVI template to configure SVI for Cisco IOS XE Catalyst SD-WAN devices. You configure a switch virtual interface (SVI) to configure a VLAN interface.

To configure DSL interfaces on Cisco routers using Cisco SD-WAN Manager templates, create a VPN Interface SVI feature template to configure VLAN interface parameters.

### Create VPN Interface SVI Template

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

4. From the **Device Model** drop-down, choose the type of device for which you are creating the template.
5. If you are configuring the SVI in the transport VPN (VPN 0):
   a. Click **Transport & Management VPN**, or scroll to the Transport & Management VPN section.
   b. Under Additional VPN 0 Templates, click **VPN Interface SVI**.
6. If you are configuring the SVI in a service VPN (VPNs other than VPN 0):
   a. Click **Service VPN**, or scroll to the Service VPN section.
   b. In the **Service VPN** drop-down list, enter the number of the service VPN.
   c. Under **Additional VPN Templates**, click **VPN Interface SVI**.
7. From the **VPN Interface SVI** drop-down, click **Create Template**. The VPN Interface SVI template form is displayed.

   The form contains fields for naming the template, and fields for defining VLAN Interface parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you open a feature template initially, 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 next to the parameter field.

**Note** To get the SVI interface up and functional, ensure that the appropriate VLAN is explicitly configured on the Switch Port Access or Trunk interface.

### Configure Basic Interface Functionality

***Table 181: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Support for Configuring Secondary IP Address | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | You can configure up to four secondary IPv4 or IPv6 addresses, and up to four DHCP helpers. Secondary IP addresses can be useful for forcing unequal load sharing between different interfaces, for increasing the number of IP addresses in a LAN when no more IPs are available from the subnet, and for resolving issues with discontinuous subnets and classful routing protocol. |

To configure basic VLAN interface functionality in a VPN, choose **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

***Table 182:***

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the VLAN interface. |
| VLAN Interface Name* | Enter the VLAN identifier of the interface. *Range:* 1 through 1094. |
| Description | Enter a description for the interface. |
| IP MTU | Specify the maximum MTU size of packets on the interface. *Range:* 576 through 1500. *Default:* 2000 bytes |
| IPv4* or IPv6 | Click to configure one or more IPv4 of IPv6 addresses for the interface. (Beginning with Cisco IOS XE SD-WAN Release 17.2.) |
| IPv4 Address*<br>IPv6 Address | Enter the IPv4 address for the interface. |
| Secondary IP Address | Click **Add** to enter up to four secondary IP addresses. (Beginning with Cisco IOS XE SD-WAN Release 17.2.) |
| DHCP Helper* | Enter up to eight IP addresses for DHCP servers in the network to have the interface be a DHCP helper. Separate each address with a comma. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.<br>Click **Add** to configure up to four DHCP helpers. (Beginning with Cisco IOS XE SD-WAN Release 17.2, for IPv6.) |

To save the feature template, click **Save**.

### Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, choose **ACL** and configure the following parameters:

***Table 183:***

| Parameter Name | Description |
|---|---|
| Ingress ACL – IPv4 | Click **On** and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click **On** and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress Policer | Click **On** and specify the name of the policer to apply to packets being received on the interface. |

| Parameter Name | Description |
|---|---|
| Egress Policer | Click **On** and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

### Configure VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, choose **VRRP**. Then click **Add New VRRP** and configure the following parameters:

***Table 184:***

| Parameter Name | Description |
|---|---|
| Group ID | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. *Range:* 1 through 255 |
| Priority | Enter the priority level of the router. There router with the highest priority is elected as the primary router. If two Cisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as the primary one. *Range:* 1 through 254 *Default:* 100 |
| Timer | Specify how often the primary VRRP router sends VRRP advertisement messages. If the subordinate routers miss three consecutive VRRP advertisements, they elect a new primary router. *Range:* 1 through 3600 seconds *Default:* 1 second |
| Track OMP Track Prefix List | By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:<br><br>Track OMP—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.<br><br>Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router. |
| IP Address | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP. |

### Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, choose **ARP**. Then click **Add New ARP** and configure the following parameters:

***Table 185:***

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click **Add**.

To save the feature template, click **Save**.

### Configure Other Interface Properties

To configure other interface properties, choose **Advanced** and configure the following properties:

***Table 186:***

| Parameter Name | Description |
|---|---|
| TCP MSS | Specify the maximum segment size (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 |
| ARP Timeout | Specify how long it takes for a dynamically learned ARP entry to time out. *Range:* 0 through 2678400 seconds (744 hours) *Default:* 1200 (20 minutes) |

To save the feature template, click **Save**.

# VPN Interface T1/E1

Use the VPN Interface T1/E1 template for Cisco Catalyst SD-WANs running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters, as described in this article.
2. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters.
3. Create a VPN feature template to configure VPN parameters.

### 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. 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. To create a template for VPN 0 or VPN 512:

**Note** **Note**: Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. When you complete the configuration, the system automatically maps the VPN configurations to VRF configurations.

   a. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
   b. Under **Additional VPN 0 Templates**, click **VPN Interface T1/E1 Serial**.
   c. From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The **VPN Interface T1/E1** template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.

6. To create a template for VPNs 1 through 511, and 513 through 65530:
   a. Click **Service VPN** or scroll to the **Service VPN** section.
   b. Click the **Service VPN** drop-down list.
   c. Under **Additional VPN** templates, click **VPN Interface**.
   d. From the **VPN Interface** drop-down list, click **Create Template**. The **VPN Interface Ethernet** template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.
7. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In **Template Description**, 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 to the left of the parameter field.

### Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

*Table 187:*

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the interface. |
| Interface name* | Enter a name for the interface. The name should be in the format **serial** *slot* **/** *subslot* **/** *port* **:** *channel-group*.<br>You must also configure a number for the channel group in the T1/E1 Controller feature configuration template. |
| Description | Enter a description for the interface. |
| IPv4 Address* | Enter an IPv4 address. |
| IPv6 Address* | Enter an IPv6 address. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications. *Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications. *Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface. *Range:* 576 through 1804 *Default:* 1500 bytes |

### Create a Tunnel Interface

On Cisco IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select **Tunnel Interface** and configure the following parameters:

*Table 188:*

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click **On** to create a tunnel interface. |
| Color | Select a color for the TLOC. |

| Parameter Name | Description |
|---|---|
| Control Connection | By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC.<br>**Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic.<br>For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth.<br>A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below:<br>• 650 – 700 Kbps per device for control connections.<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (request)<br>• 175 Bytes (or 1.4 Kbps) per BFD session on the device (response)<br>If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs:<br>A 1500 Bytes BFD request packet is sent per tunnel every 30 secs:<br>1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request)<br>A 147 Bytes BFD packet is sent in response:<br>147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response)<br>Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of:<br>700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps |
| Maximum Control Connections | Specify the maximum number of Cisco Catalyst SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8 *Default:* 2 |
| Cisco Catalyst SD-WAN Validator As STUN Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Controller Group List | Set the Cisco Catalyst SD-WAN Controllers that the tunnel interface is not allowed to connect to. *Range:* 0 through 100 |
| Cisco SD-WAN Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. *Range:* 0 through 8 *Default:* 5 |

| Parameter Name | Description |
|---|---|
| Port Hop | Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. *Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br>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 |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has **Dont Fragment** configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the **Dont Fragment** bit in the IPv4 packet header for packets being transmitted out of the interface. When the **Dont Fragment** bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br>**Note** **Clear-Dont-Fragment** clears the **Dont Fragment** bit and the **Dont Fragment** bit is set. For packets not requiring fragmentation, the **Dont Fragment** bit is not affected. |
| Allow Service | Select **On** or **Off** for each service to allow or disallow the service on the interface. |

To save the feature template, click **Save**.

### Release Information

Introduced in Cisco vManage Release 18.2.

# T1/E1 Controller

Use the T1/E1 Controller template for Cisco IOS XE Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters, as described in this article.

2. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters.
3. Create a VPN feature template to configure VPN parameters.

### 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. 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. To create a template for VPN 0 or VPN 512:
   a. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
   b. Under **Additional VPN 0 Templates**, click **VPN Interface**.
   c. From the **VPN Interface** drop-down list, click **Create Template**. The **VPN Interface T1/E1** template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
   a. Click **Service VPN** or scroll to the **Service VPN** section.
   b. Click the **Service VPN** drop-down list.
   c. Under **Additional VPN** templates, click **VPN Interface**.
   d. From the **VPN Interface** drop-down list, click **Create Template**. The VPN Interface Ethernet template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.
7. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In **Template Description**, 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 and select one of the following:

- Device Specific (indicated by a host icon)
- Global (indicated by a globe icon)

### Configure a T1 Controller

To configure a T1 controller, click **T1** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

***Table 189:***

| Parameter Name | Description |
|---|---|
| Slot* | Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0. |
| Framing* | Enter the T1 frame type:<br>• **esf**—Send T1 frames as extended superframes. This is the default.<br>• **sf**—Send T1 frames as superframes. Superframing is sometimes called D4 framing. |
| Line Code | Select the line encoding to use to send T1 frames:<br>• ami—Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes.<br>• b8zs—Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes |
| Clock Source | Select the clock source:<br>• internal—Use the controller framer as the primary clock.<br>• line—Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. |
| Line Mode | If you choose the Line clock source, select whether the line is a primary or a secondary line. |
| Description | Enter a description for the controller. |
| Channel Group | Enter the number of the channel group. If you do so, you must enter a time slot in the Time Slot field. *Range:* 0 through 30 |
| Time Slot | Enter the time slot or time slots that are part of the channel group. *Range:* 1 through 24 |
| Cable Length | Select the cable length to configure the attenuation<br>• long—Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet.<br>• short—Set the transmission attenuation for cables that are 660 feet or shorter.<br>There is no default length. |

| Parameter Name | Description |
|---|---|
| Length | If you specify a value in the **Cable Length Field**, enter the length of the cable.<br>For short cables, the length values can be:<br>• 110—Length from 0 through 110 feet<br>• 220—Length from 111 through 220 feet<br>• 330—Length from 221 through 330 feet<br>• 440—Length from 331 through 440 feet<br>• 550—Length from 441 through 550 feet<br>• 660—Length from 551 through 660 feet<br>For long cables, the length values can be:<br>• 0 dB<br>• –7.5 dB<br>• –15 dB<br>• –22.5 dB |

To save the feature template, click **Save**.

### Configure an E1 Controller

To configure an E1 controller, click **E1** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

***Table 190:***

| Parameter Name | Description |
|---|---|
| Slot* | Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0. |
| Framing* | Enter the E1 frame type:<br>• **crc4**—Use cyclic redundancy check 4 (CRC4). This is the default.<br>• **no-crc4**—Do no use CRC4. |
| Line Code* | Select the line encoding to use to send E1 frames:<br>• ami—Use alternate mark inversion (AMI) as the linecode.<br>• hdb3—Use high-density bipolar 3 as the linecode. This is the default. |

| Parameter Name | Description |
|---|---|
| Clock Source | Select the clock source:<br>• internal—Use the controller framer as the primary clock.<br>• line—Use phase-locked loop (PLL) on the interface. This is the default. |
| Line Mode | If you choose the Line clock source, select whether the line is a primary or secondary line. If you configure both a primary and a secondary line, if the primary line fails, the PLL automatically switches to the secondary line. When the PLL on the primary line becomes active again, the PLL automatically switches back to the primary line. |
| Description | Enter a description for the controller. |
| Channel Group | To configure the serial WAN on the E1 interface, enter a channel group number. *Range:* 0 through 30 |
| Time Slot | For a channel group, configure the timeslot. *Range:* 1 through 31 |

To save the feature template, click **Save**.

#### Release Information

Introduced in Cisco vManage Release 18.1.1.

# Cellular Interfaces

To enable LTE connectivity, configure cellular interfaces on a router that has a cellular module. The cellular module provides wireless connectivity over a service provider's cellular network. One use case is to provide wireless connectivity for branch offices.

A cellular network is commonly used as a backup WAN link, to provide network connectivity if all the wired WAN tunnel interfaces on the router become unavailable. You can also use a cellular network as the primary WAN link for a branch office, depending on usage patterns within the branch office and the data rates supported by the core of the service provider's cellular network.

When you configure a cellular interface on a device, you can connect the device to the Internet or another WAN by plugging in the power cable of the device. The device then automatically begins the process of joining the overlay network, by contacting and authenticating with Cisco Catalyst SD-WAN Validators, Cisco Catalyst SD-WAN Controllers, and Cisco SD-WAN Manager systems.

## Configure Cellular Interfaces Using Cisco SD-WAN Manager

To configure cellular interfaces using Cisco SD-WAN Manager templates:

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

**Note** If your deployment includes devices with cellular interface, you must include cellular controller templates in Cisco SD-WAN Manager, even if these templates are not used.

If the device has the LTE or cellular controller module configured and the cellular controller feature template does not exist, then the device tries to remove the cellular controller template. For releases earlier than Cisco IOS XE Release 17.4.2, the following error message is displayed.

```
bad-cli - No controller Cellular 0/2/0, parser-context - No controller Cellular 0/2/0,
parser-response % Cannot remove controllers this way
```

For devices running on Cisco IOS XE Release 17.4.2 and later, the device will return an access-denied error message.

### Create VPN Interface Cellular

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, select the type of device for which you are creating the template.
5. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional Cisco VPN 0 Templates**, click **VPN Interface Cellular**.
7. From the **VPN Interface Cellular** drop-down list, click **Create Template**. The VPN Interface Cellular template form is displayed.

   This form contains fields for naming the template, and fields for defining the VPN Interface Cellular parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, 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.

### Configure Basic Cellular Interface Functionality

To configure basic cellular interface functionality, click **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface. You must also configure a tunnel interface for the cellular interface.

*Table 191:*

| Parameter Name | Description |
|---|---|
| Shutdown* | Click **No** to enable the interface. |
| Interface Name* | Enter the name of the interface. It must be **cellular0**. |
| Description | Enter a description of the cellular interface. |
| DHCP Helper | Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications. Range: 1 through ($2^{32}$ / 2) – 1 kbps |
| IP MTU* | Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value. |

To save the feature template, click **Save**.

### Create a Tunnel Interface

To configure an interface in VPN 0 to be a WAN transport connection, you must configure a tunnel interface on the cellular interface. The tunnel, which provides security from attacks, is used to send the phone number. At a minimum, select **On** and select a color for the interface, as described in the previous section. You can generally accept the system defaults for the reminder of the tunnel interface settings.

To configure a tunnel interface, click **Tunnel**, and configure the following parameters. Parameters marked with an asterisk (*) are required to configure a cellular interface.

| Parameter Name | Description |
|---|---|
| Tunnel Interface* | From the drop-down, select **Global**. Click **On** to create a tunnel interface. |
| Per-tunnel QoS | From the drop-down, select **Global**. Click **On** to create per-tunnel QoS.<br>You can apply a Quality of Service (QoS) policy on individual tunnels, and is only supported for hub-to-spoke network topologies. |
| Per-tunnel QoS Aggregrator | From the drop-down, select **Global**. Click **On** to create per-tunnel QoS.<br>**Note** 'bandwidth downstream' is required for per-Tunnel QoS feature to take effect as spoke role. |
| Color* | From the drop-down, select **Global**. Select a color for the TLOC. The color typically used for cellular interface tunnels is **lte**. |
| Groups | From the drop-down, select **Global**. Enter the list of groups in the field. |

| Parameter Name | Description |
|---|---|
| Border | From the drop-down, select **Global**. Click **On** to set TLOC as border TLOC. |
| Maximum Control Connections | Set the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8<br>Default: 2 |
| vBond As STUN Server | Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Control Group List | Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allows to establish control connections with.<br>Range: 0 through 100 |
| vManage Connection Preference | Set the preference for using the tunnel to exchange control traffic with the Cisco SD-WAN Manager.<br>Range: 0 through 9<br>Default: 5<br>If the edge device has two or more cellular interfaces, you can minimize the amount of traffic between the Cisco SD-WAN Manager and the cellular interfaces by setting one of the interfaces to be the preferred one to use when sending updates to the Cisco SD-WAN Manager and receiving configurations from the Cisco SD-WAN Manager.<br>To have a tunnel interface never connect to the Cisco SD-WAN Manager, set the number to 0. At least one tunnel interface on the edge device must have a nonzero Cisco SD-WAN Manager connection preference. |
| Port Hop | From the drop-down, select **Global**. Click **Off** to allow port hopping on tunnel interface.<br>Default: **On**, which disallows port hopping on tunnel interface. |
| Low-Bandwidth Link | Click **On** to set the tunnel interface as a low-bandwidth link.<br>Default: **Off** |

| Parameter Name | Description |
|---|---|
| Tunnel TCP MSS | 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 TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow 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.<br>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 |
| Clear-Dont-Fragment | Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.<br>Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.<br>**Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected. |
| Network Broadcast | From the drop-down, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Turn this **On** only if the **Directed Broadcast** is enabled on the LAN interface feature template.<br>Default: **Off** |
| Allow Service | Click **On** or **Off** for each service to allow or disallow the service on the cellular interface. |

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

***Table 192:***

| Parameter Name | Description |
|---|---|
| GRE | From the drop-down, select **Global**. Click **On** to use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| GRE Preference | From the drop-down, select **Global**. Enter a value to set GRE preference for TLOC.<br>Range: 0 to 4294967295 |

| Parameter Name | Description |
|---|---|
| GRE Weight | From the drop-down, select **Global**. Enter a value to set GRE weight for TLOC.<br>Default: 1 |
| IPsec | From the drop-down, select **Global**. Click **On**to use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | From the drop-down, select **Global**. Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>Range: 0 through 4294967295. Default: 0 |
| IPsec Weight | From the drop-down, select **Global**. Enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>Range: 1 through 255. Default: 1 |
| Carrier | From the drop-down, select **Global**. From the **Carrier** drop-down, select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the format **ge** *slot*/*port*. |
| Last-Resort Circuit | From the drop-down, select **Global**. Click **On** to use the tunnel interface as the circuit of last resort. By default, it is disabled.<br>**Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.<br>When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.<br>Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds. |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second). |

| Parameter Name | Description |
|---|---|
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>Range: 12 through 60 seconds. Default: 12 seconds.<br><br>The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable. |

To save the feature template, click **Save**.

### Configure the Cellular Interface as a NAT Device

To configure a cellular interface to act as a NAT device for applications such as port forwarding, click **NAT**, and configure the following parameters:

***Table 193:***

| Parameter Name | Description |
|---|---|
| NAT | Click **On** to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes. Default: 1 minute |
| TCP Timeout | Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes. Default: 60 minutes (1 hour) |
| Block ICMP | Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. Default: Off |
| Respond to Ping | Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

*Table 194:*

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click **Add**.

To save the feature template, click **Save**.

### Apply Access Lists

To configure a shaping rate to a cellular interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, click **ACL/QoS** and configure the following parameters:

*Table 195: Access Lists Parameters*

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite rule | Click **On**, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click **On**, and specify the name of an IPv4 access list to packets being received on the interface. |
| Egress ACL– IPv4 | Click **On**, and specify the name of an IPv4 access list to packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click **On**, and specify the name of an IPv6 access list to packets being received on the interface. |
| Egress ACL– IPv6 | Click **On**, and specify the name of an IPv6 access list to packets being transmitted on the interface. |

| Parameter Name | Description |
|---|---|
| Ingress policer | Click **On**, and specify the name of the policer to apply to packets being received on the interface. |
| Egress policer | Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click **Save**.

### Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, click **ARP**. Then click **Add New ARP** and configure the following parameters:

***Table 196:***

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click **Add**.

To save the feature template, click **Save**.

### Configure Other Interface Properties

To configure other interface properties, click **Advanced** and configure the following parameters.

***Table 197: Cellular Interfaces Advanced Parameters***

| Parameter Name | Description |
|---|---|
| PMTU Discovery | Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. 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. |
| Clear-Dont-Fragment | Click **On** to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS | Select a queue number to use for incoming traffic. Range: 0 through 7 |
| Autonegotiate | Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |

| Parameter Name | Description |
|---|---|
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| IP Directed-Broadcast | From the drop-down, select **Global**. Click **On** for IP directed-broadcast.<br>Default: **Off** |

To save the feature template, click **Save**.

# Configure Cellular Interfaces Using CLI

The following example enables a cellular interface:

```
interface Cellular0/2/0
   description Cellular interface
   no shutdown
   ip address negotiated
   ip mtu 1428
   mtu 1500
  exit

  controller Cellular 0/2/0
   lte sim max-retry 1
   lte failovertimer 7
   profile id 1 apn Broadband authentication none pdn-type ipv4
```

# Data Profile

***Table 198: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Ability to Configure APNs under Running Configurations for Single and Dual SIMs | Cisco IOS XE Catalyst SD-WAN Release 17.8.1a<br>Cisco vManage Release 20.8.1 | This feature allows you to create a data profile for a cellular device. |

A data profile for a cellular device defines the following parameters, which the device uses for communication with the service provider. You can configure the following parameters by using the **profile id** command in cellular configuration mode. For more information about the following parameters, see profile id.

- Identification number of the data profile
- Name of the access point network of the service provider
- Authentication type used for APN access: No authentication, CHAP authentication only, PAP authentication only, or either CHAP or PAP authentication

- Username and password that are provided by the service provider for APN access authentication, if authentication is used
- Type of packet data matching that is used for APN access: IPv4 type bearer, IPv6 type bearer, or IPv4v6 type bearer
- SIM slot that contains the SIM to configure

# Best Practices for Configuring Cellular Interfaces

Cellular technology on edge devices can be used in a number of ways:

- Circuit of last resort: An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.

  When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.

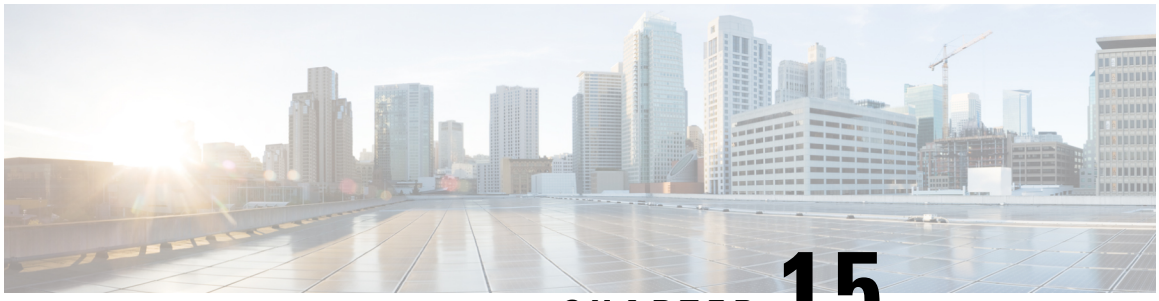
  Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.

  Use the **last-resort-circuit** command to configure a cellular interface to be a circuit of last resort.

- Active circuit: You can choose to use a cellular interface as an active circuit, perhaps because it is the only last-mile circuit or to always keep the cellular interface active so that you can measure the performance of the circuit. In this scenario the amount of bandwidth utilized to maintain control and data connections over the cellular interface can become a concern. Here are some best practices to minimize bandwidth usage over a cellular interface:
  - When a device with cellular interface is deployed as a spoke, and data tunnels are established in a hub-and-spoke manner, you can configure the cellular interface as a low-bandwidth interface. To do this, include the **low-bandwidth-link** command when you configure the cellular interface's tunnel interface. When the cellular interface is operating as a low-bandwidth interface, the device spoke site is able to synchronize all outgoing control packets. The spoke site can also proactively ensure that no control traffic, except for routing updates, is generated from one of the remote hub nodes. Routing updates continue to be sent, because they are considered to be critical updates.
  - Increase control packet timers—To minimize control traffic on a cellular interface, you can decrease how often protocol update messages are sent on the interface. OMP sends Update packets every second, by default. You can increase this interval to a maximum of 65535 seconds (about 18 hours) by including the **omp timers advertisement-interval** configuration command. BFD sends Hello packets every second, by default. You can increase this interval to a maximum of 5 minutes (300000 milliseconds) by including the **bfd color hello-interval** configuration command. (Note that you specify the OMP Update packet interval in seconds and the BFD Hello packet interval in milliseconds.)
  - Prioritize Cisco SD-WAN Manager control traffic over a non-cellular interface: When a edge device has both cellular and non-celluar transport interfaces, by default, the edge device chooses one of the interfaces to use to exchange control traffic with the Cisco SD-WAN Manager. You can configure the edge device to never use the cellular interface to exchange traffic with the Cisco SD-WAN

Manager, or you can configure a lower preference for using the cellular interface for this traffic. You configure the preference by including the **vmanage-connection-preference** command when configuring the tunnel interface. By default, all tunnel interface have a Cisco SD-WAN Manager connection preference value of 5. The value can range from 0 through 8, where a higher value is more preferred. A tunnel with a preference value of 0 can never exchange control traffic with the Cisco SD-WAN Manager.

**Note** At least one tunnel interface on the edge device must have a non-0 Cisco SD-WAN Manager connection preference value. Otherwise, the device has no control connections.



CHAPTER 15

# Hot Standby Router Protocol (HSRP)

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 199: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support for HSRP and HSRP Authentication on Cisco IOS XE Catalyst SD-WAN Devices | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a<br>Cisco vManage Release 20.7.1<br>Cisco SD-WAN Release 20.7.1 | This feature allows you to configure HSRPv2 and HSRP authentication on Cisco IOS XE Catalyst SD-WAN platforms via CLI template. HSRP is a long-standing Cisco proprietary First Hop Redundancy Protocol (FHRP) to support version 2 of the protocol and authentication. |


- Information About HSRP, on page 725
- Supported Devices for HSRP, on page 728
- Configure HSRP Using CLI, on page 729
- Verify HSRP Configurations Using CLI, on page 731


# Information About HSRP

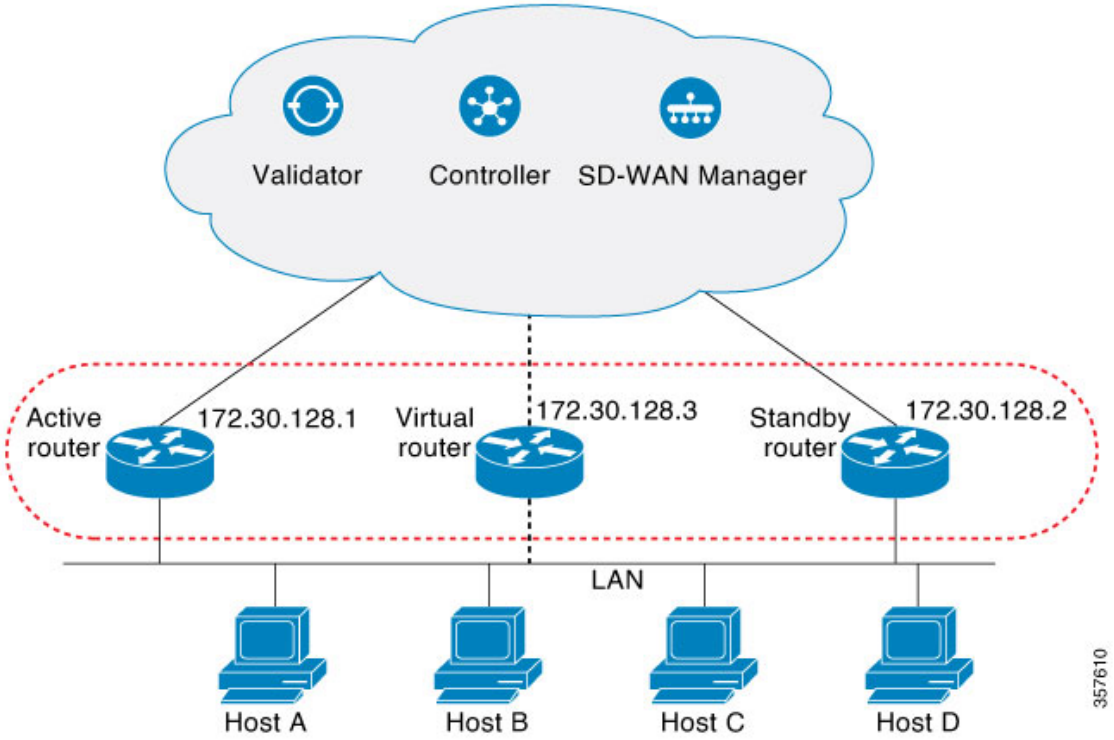
The Hot Standby Router Protocol (HSRP) is a First Hop Redundancy Protocol (FHRP) designed to allow transparent failover of the first-hop IP device. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on networks configured with a default gateway IP address. For identifying

an active and standby device in a group of routers, HSRP is used. In a group of device interfaces, the active device is the device of choice for routing packets; the standby device is the device that takes over if the active device fails or if preset conditions are met.

You can configure multiple hot standby groups on an interface, thereby making full use of redundant devices and load sharing.

The following figure shows a network configured for HSRP. By sharing a virtual MAC address and IP address, two or more devices can act as a single virtual router. The virtual device represents the common default gateway for devices that are configured to provide backup to each other. You don't need to configure the hosts on the LAN with the IP address of the active device. Instead, you can configure them with the IP address (virtual IP address) of the virtual device as their default gateway. If the active device fails to send a hello message within a configurable time period, the standby device takes over and responds to the virtual addresses and becomes the active device, taking over the duties of the active device.

***Figure 5: HSRP Topology***




### HSRP Version 2 Support

Following are the HSRP version 2 (HSRPv2) features:

- HSRPv2 advertises and learns millisecond timer values. This change ensures stability of the HSRP groups in all cases.
- HSRPv2 expands the group number range from 0 to 4095.
- HSRPv2 provides improved management and troubleshooting. The HSRPv2 packet format includes a 6-byte identifier field that is used to uniquely identify the sender of the message. Typically, this field is populated with the interface MAC address.

- HSRPv2 uses the IP multicast address 224.0.0.102 to send hello packets. This multicast address allows Cisco Group Management Protocol (CGMP) leave processing to be enabled at the same time as HSRP.
- HSRPv2 has a different packet format that uses a type-length-value (TLV) format.

### HSRP MD5 Authentication

HSRP supports simple plain text string and message digest 5 (MD5) schemes of protocol packets authentication. HSRP MD5 authentication is an advanced type of authentication that generates an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This functionality provides added security and protects against the threat from HSRP-spoofing software.

MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each HSRP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated, and if the hash within the incoming packet doesn't match the generated hash, the packet is ignored.

The key for the MD5 hash can be either given directly in the configuration using a key string or supplied indirectly through a key chain.

HSRP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packets.
- MD5 digests differ on the device and in the incoming packets.
- Text authentication strings differ on the device and in the incoming packets.

### HSRP Object Tracking

Object tracking separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by any other process and HSRP. The priority of a device can change dynamically when it has been configured for object tracking, and the object that is being tracked goes down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced.

### HSRP Static NAT Redundancy Overview

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a release, HSRP Static NAT redundancy is supported on Cisco IOS XE Catalyst SD-WAN. Static mapping support for HSRP enables the active router configured with a NAT address to respond to an incoming ARP. This feature provides redundancy in NAT for traffic that fails over from HSRP active router to standby router without waiting for the ARP entry to timeout from previously active router.

The static NAT configuration is mirrored on the active and standby routers, and the active router processes the traffic.

A virtual IP address is assigned to the router. The edge device sends traffic to the virtual IP address, which is serviced by the active router. The standby routers monitor the active router. When the failover occurs, the new HSRP active edge router automatically resumes the ownership of static NAT mapping without waiting for ARP timeout. It sends gratuitous ARP for the static NAT mapping entry to update devices with their own mac addresses in the same LAN segment.

**Note** Only static NAT is supported in HSRP NAT redundancy configuration.

Perform the following tasks on active and standby routers to configure NAT static mapping for HSRP:

- Ensure that the source and destination NAT works.
- Enable HSRP on the NAT interface.
- Configure HSRP redundancy group name.
- Configure static NAT mapping manually on both active and standby edges, referring to HSRP redundancy group name configured.

To enable static NAT redunndancy for high availability in an HSRP environment, refer to Static NAT mapping support with HSRP.

### HSRP Benefits

- Redundancy: HSRP employs a redundancy scheme that is time proven and deployed extensively in large networks.
- Fast Failover: HSRP provides transparent fast failover of the first-hop device.
- Preemption: Preemption allows a standby device to delay becoming active for a configurable amount of time.
- Authentication: HSRP MD5 algorithm authentication protects against HSRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

# Supported Devices for HSRP

Cisco Catalyst 8500 Series Edge Platforms

Cisco Catalyst 8300 Series Edge Platforms

Cisco Catalyst 8200 Series Edge Platforms

Cisco Catalyst 8200 uCPE Series Edge Platforms

Cisco ASR 1000 Series Aggregation Services Routers

Cisco ISR 1000 and ISR 4000 Series Integrated Services Routers (ISRs)

Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers (ISRs)

Cisco IR1101 Integrated Services Router Rugged

Cisco Catalyst 8000v Series Cloud Services Router

For details on supported models for each of these device families, refer to Cisco Catalyst SD-WAN Device Compatibility page.

# Configure HSRP Using CLI

You can configure HSRP using the Cisco SD-WAN Manager CLI Add-on feature templates and CLI device templates. For more information on configuring using CLI templates, see CLI Templates.

**Note** The following commands can be used in any order.

The following list provides information about HSRP configuration on Cisco IOS XE Catalyst SD-WAN devices.

- Enable HSRP.

  Create (or enable) the HSRP group in IPv4 using its number and virtual IP address:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number ip [ip-address [secondary]]
  ```

  Activate HSRP in IPv6:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number ipv6 {link-local-address | autoconfig }
  ```

- Change to Version 2.

  Change the HSRP version. Note that the **nostandby** or **nostandby version 2** commands are rejected when the interface has IPv6 groups.

  **Note** **nostandby** or **nostandby version 2** command is rejected when the interface has IPv6 groups.

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby version {1|2}
  ```

- Configure HSRP priority and preemption.

  Set the priority value used in choosing the active router, and configure HSRP preemption and preemption delay:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number ip [ip-address [secondary]]
  Device(config-if)# standby group-number priority [priority]
  Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload
  seconds] [ sync seconds]}]
  ```

- Configure HSRP Authentication.

  Configure HSRP MD5 authentication using a key chain.

  Key chains allow a different key string to be used at different times according to the key chain configuration. HSRP queries the appropriate key chain to obtain the current live key and key ID for the specified key chain.

  ```
  Device(config)# interface interface-type
  Device(config-if)# ip address ip-address mask [secondary ]
  Device(config-if)# standby group-number priority [priority]
  ```

```
Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload
seconds] [ sync seconds]}]
Device(config-if)# standby group-number authentication md5 key-chain key-chain-name
Device(config-if)# standby group-number ip [ip-address [secondary]]
```

Configure HSRP text authentication.

The authentication string can be up to eight characters in length; the default string is Cisco.

```
Device(config)# interface interface-type
Device(config-if)# ip address ip-address mask [secondary ]
Device(config-if)# standby group-number priority [priority]
Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload
seconds] [ sync seconds]}]
Device(config-if)# standby group-number authentication text string
Device(config-if)# standby group-number ip [ip-address [secondary]]
```

- Configure HSRP timers.

  Configure the time between the hello packets and the time before other routers declare the active router to be inactive:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number ip [ip-address [secondary]]
  Device(config-if)# standby group-number timers hellotime holdtime
  ```

- Configure HSRP object tracking.

  Configure HSRP to track an object and change the HSRP priority based on the state of the object:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number track object-number [decrement priority-decrement]
   [shutdown]
  ```

- Improve CPU and network performance with HSRP multiple group optimization.

  Configure an HSRP group as a client group:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number follow group-name
  ```

  Configure the HSRP client group refresh interval:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number mac-refresh seconds
  ```

- Configure an HSRP virtual MAC address.

  Specify a virtual MAC address for HSRP:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number mac-address mac-address
  ```

- Link IP redundancy clients to HSRP groups.

  Configure the name of a standby group:

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, static NAT mapping configurations with HSRP is supported. The redundancy naming conventions doesn't include spaces. We recommend that you do not use redundancy name with spaces while configuring **standby group-number name***[redundancy-name]* command.

```
Device(config)# interface interface-type
Device(config-if)# standby group-number name [redundancy-name]
```

The following is a complete HSRP configuration example on Cisco IOS XE Catalyst SD-WAN devices through CLI:

```
config-transaction
!
    interface GigabitEthernet0/0/1.94
    encapsulation dot1Q 94
    vrf forwarding 509
    ip address 10.96.194.2 255.255.255.0
    ip directed-broadcast
    ip mtu 1500
    ip nbar protocol-discovery
    standby version 2
    standby 1 preempt
    standby 94 ip 10.96.194.1
    standby 94 timers 1 4
    standby 94 priority 110
    standby 94 preempt delay minimum 180
    standby 94 authentication md5 key-string 7 094F471A1A0A
    standby 94 track 8 shutdown
    standby 194 ipv6 2001:10:96:194::1/64
    standby 194 timers 1 4
    standby 194 priority 110
    standby 194 preempt delay minimum 180
    standby 194 authentication md5 key-string 7 094F471A1A0A
    standby 194 track 80 shutdown
    ip policy route-map clear-df
    ipv6 address 2001:10:96:194::2/64
    ipv6 mtu 1500
    arp timeout 1200
    end
```

# Verify HSRP Configurations Using CLI

The following is a sample output from the **show standby** command displaying the standby router information:

```
Device# show standby
GigabitEthernet0/0/1.94 - Group 94 (version 2)
  State is Standby
    1 state change, last state change 01:06:09
    Track object 8 state Up
  Virtual IP address is 10.96.194.1
  Active virtual MAC address is 0000.0c9f.f05e (MAC Not In Use)
    Local virtual MAC address is 0000.0c9f.f05e (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.688 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is 10.96.194.2, priority 110 (expires in 4.272 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-94" (default)
  FLAGS: 0/1
GigabitEthernet0/0/1.94 - Group 194 (version 2)
  State is Standby
    1 state change, last state change 01:06:07
```

```
    Track object 80 state Up
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:C2 (impl auto EUI64)
    Virtual IPv6 address 2001:10:96:194::1/64
  Active virtual MAC address is 0005.73a0.00c2 (MAC Not In Use)
    Local virtual MAC address is 0005.73a0.00c2 (v2 IPv6 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.480 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is FE80::CE16:7EFF:FE8C:6DD1, priority 110 (expires in 4.032 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-194" (default)
  FLAGS: 0/1
```

The following is a sample output from the **show standby** command displaying HSRP Version 2 information if HSRP Version 2 is configured:

```
Device# show standby
Ethernet0/1 - Group 1 (version 2)
  State is Speak
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is unknown
   Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
   Next hello sent in 1.804 secs
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 20 (configured 20)
  Group name is "hsrp-Et0/1-1" (default)
Ethernet0/2 - Group 1
  State is Speak
  Virtual IP address is 10.22.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (default 100)
    Track interface Serial2/0 state Down decrement 10
  Group name is "hsrp-Et0/2-1" (default)
```

The following is a sample output from the **show standby** command displaying HSRP authentication information if HSRP MD5 authentication is configured:

```
Device# show standby
Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string, timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Et0/1-1" (default)
```

The following is a sample output from the **show standby brief** command displaying HSRP information for a specific interface:

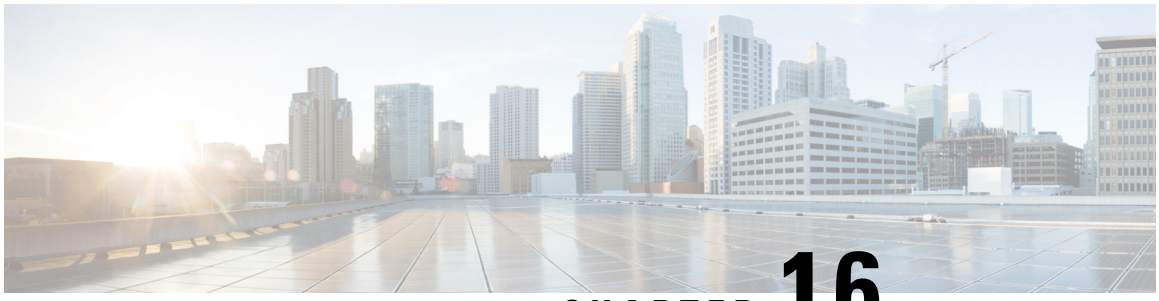
```
Device# show standby brief
Interface   Grp  Pri P State   Active                    Standby   Virtual IP
Gi0/0/1.94  94   105 P Standby 10.96.194.2                 local    10.96.194.1
Gi0/0/1.94  194  105 P Standby FE80::CE16:7EFF:FE8C:6DD1   local    FE80::5:73FF:FEA0:C2
```

The following is a sample output from the **show standby neighbors** command displaying the HSRP neighbors on Ethernet interface 0/0. Neighbor 10.0.0.250 is active for group 2 and standby for groups 1 and 8, and is registered with BFD:

```
Device# show standby neighbors Ethernet0/0
HSRP neighbors on Ethernet0/0
  10.0.0.250
    Active groups: 2
    Standby groups: 1, 8
    BFD enabled
  10.0.0.251
    Active groups: 5, 8
    Standby groups: 2
    BFD enabled
  10.0.0.253
    No Active groups
    No Standby groups
    BFD enabled
```

The following is a sample output from the **show standby neighbors** command displaying information for all HSRP neighbors:

```
Device# show standby neighbors
HSRP neighbors on FastEthernet2/0
  10.0.0.2
    No active groups
    Standby groups: 1
    BFD enabled
HSRP neighbors on FastEthernet2/0
  10.0.0.1
    Active groups: 1
    No standby groups
    BFD enabled
```



CHAPTER 16

# Configure a Cellular Gateway


- Configure a Cellular Gateway, on page 735
- Information About Configuring a Cellular Gateway, on page 736
- Supported Cellular Gateway Devices, on page 736
- Configure a Cellular Gateway Using a Feature Template in Cisco SD-WAN Manager, on page 736
- Configure a Cellular Gateway Using a Configuration Group in Cisco SD-WAN Manager, on page 740


# 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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 200: Feature History*

| Feature Name | Release Information | Feature Description |
|---|---|---|
| Cellular Gateway Configuration | Cisco vManage Release 20.4.1<br>Cisco IOS XE Catalyst SD-WAN Release 17.4.1a (on devices) | This feature provides templates for configuring a supported cellular gateway as an IP pass-through device. This release supports the Cisco Cellular Gateway CG418-E and CG522-E. |
| Cellular Gateway Configuration Using a Configuration Group | Cisco Catalyst SD-WAN Manager Release 20.13.1<br>Cisco IOS CG Release 17.13.1 | Added support for configuring cellular gateways using configuration groups. A new Create Cellular Gateway Group workflow creates a configuration group specifically for cellular gateways. |

# Information About Configuring a Cellular Gateway

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.

### Secure Communication with Devices through a vmanage-admin Account

Cisco SD-WAN Manager communicates with devices, such as Cisco Catalyst Cellular Gateways, using a secure channel—either a datagram transport layer security (DTLS) tunnel or transport layer security (TLS) tunnel. Within this secure channel, it communicates with the devices or controllers using the NETCONF protocol, within an SSH session. It uses an internal-use-only passwordless "vmanage-admin" user account on the device or controller. The vmanage-admin account is created during the initial device setup. Cisco SD-WAN Manager uses this secure channel for monitoring, configuring, and managing devices.

As noted, the vmanage-admin user accounts do not have any password associated with them, so Cisco SD-WAN Manager uses a passwordless procedure to log in to the account. To accomplish this, Cisco SD-WAN Manager generates an asymmetric encryption public-private key pair. During deployment of a device, Cisco SD-WAN Manager copies the public key that it has generated to the device. It sends the public key using a proprietary protocol, within a secure channel—a DTLS or TLS tunnel.

The activity that Cisco SD-WAN Manager performs using the vmanage-admin account appears in syslog messages and in the output of certain show commands. The syslog messages are logged with the same level of detail as activities performed through any other user account. The level of syslog detail depends on the syslog configuration of the device.

Cisco SD-WAN Manager requires the vmanage-admin account on devices in order to monitor, configure, and manage the devices. Removing, disabling, or altering this account on a device would prevent Cisco SD-WAN Manager from performing these activities, and is not supported.

# Supported Cellular Gateway Devices

Cisco Catalyst Cellular Gateway models:

- CG418-E
- CG522-E

# Configure a Cellular Gateway Using a Feature Template in Cisco SD-WAN Manager

### Before You Begin

This procedure configures a cellular gateway using a feature template. For information about using a configuration group, see Configure a Cellular Gateway Using a Configuration Group in Cisco SD-WAN Manager, on page 740.

### Configure a Cellular Gateway Using a Feature Template

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

   See Configure Devices in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

   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 201: 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. |
| 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. |

| Parameter Name | Description |
|---|---|
| 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 202: 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.<br>• Profile ID: Enter a unique ID for the profile<br>• Access Point Name: Enter the name of the access point for this profile<br>• Packet Data Network Type: Choose the type of network for data services for this profile (**IPv4**, **IPv6**, or **IPv4v6**)<br>• 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<br>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.<br>You can add up to 16 profiles. |
| Profile ID | Enter a unique identifier for the profile.<br>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.

   For information, see Attach and Detach a Device Template in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

# Configure a Cellular Gateway Using a Configuration Group in Cisco SD-WAN Manager

### Before You Begin

Create a configuration group for Cisco Catalyst Cellular Gateways using **Workflows** > **Create Cellular Gateway Group**. On the **Configuration Groups** page, the resulting configuration group is labelled cellulargateway in the **Device Solution** column.

For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.

### Configure a Cellular Gateway Using a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for a Cisco Catalyst Cellular Gateway and choose **Edit**.
3. Open the **Global Profile** section and add (click **Add Global Profile Feature**) or edit (click **…** and **Edit**) any of the following features.
   - **AAA** feature:

   ***Table 203: Local***

| Parameter Name | Description |
|---|---|
| **Name** | The account name is preset to **admin** and cannot be changed. |
| **Password** | Enter a password for login. |

*Table 204: TACACS*

| Parameter Name | Description |
|---|---|
| **TACACS Configuration** | Enable TACACS configuration.<br>Click **Add TACACS** to add one or more TACACS servers. |
| **Authentication** | TACACS authentication option:<br>• **tacacs_ascii**: Send authentication information in ASCII format.<br>• **tacacs_pap**: Send authentication information using the password authentication protocol (PAP). |
| **Timeout** | Timeout for TACACS authentication.<br>Range: 1 through 1000 seconds |
| **TACACS** | |
| **IP Address** | IP address of the TACACS server. |
| **Auth Port** | TCP port number to connect to the TACACS server.<br>Default: 49 |
| **Secret Key** | Encryption key for encrypting and decrypting traffic between the cellular gateway and the TACACS server. Configure the same key on the TACACS server. |
| **Source Interface** | Preconfigured as Cellular1/0, and cannot be changed.<br>This is the only interface that the cellular gateway can use for communication with the TACACS server. |
| **Priority** | Priority level of the TACACS server. Zero is a default priority value and indicates the highest priority. If a cellular gateway is unable to establish a connection with the highest priority server, it attempts to connect to the server of the next highest priority.<br>Range: 0 through 7 |

- **Cellular** feature:

*Table 205: Cellular Settings*

| Parameter Name | Description |
|---|---|
| **Primary Slot** | Choose a SIM slot to designate it as primary.<br>Range: 0, 1<br>Default: 0 |
| **SIM SLOT 0 Cellular Profile** | |

| Parameter Name | Description |
|---|---|
| **Profile Id** | Profile ID.<br>You can click **Add** to add multiple profiles. |
| **Access Point Name** | Access point name, from your service provider. |
| **Authentication Method** | Authentication method (**none**, **pap**, **chap**, **pap_or_chap**) indicated by your service provider. |
| **Username** | Username for authentication, as indicated by your service provider. |
| **Password** | Password for authentication, as indicated by your service provider. |
| **Packet Data Network Type** | Packet data network type (**IPv4**, **IPv6**, **IPv4v6**), as indicated by your service provider. |
| **Attach Profile** | Choose the attach profile from the defined profiles. |
| **Data Profile** | Choose the data profile from the defined profiles. You can use the same profile for the attach profile and data profile. |
| **SIM SLOT 1 Cellular Profile** | |
| See the fields described for SIM slot 0. | |

- **Logging** feature:

***Table 206: Disk***

| Parameter Name | Description |
|---|---|
| **Disk File Rotate** | Maximum number of log files to store locally.<br>The device collects diagnostic monitor log files, which have a maximum size of 20 MB each, until the number of files reaches the rotate value. Then the device deletes the oldest file to make room for a new file.<br>Range: 1 through 10 |
| **Disk File Size** | Maximum file size for each log file that the device stores locally. After reaching the maximum size, the device creates a new log file, with a numerically sequenced filename.<br>Range: 1 through 20 megabytes |

***Table 207: Servers***

| Parameter Name | Description |
|---|---|
| **Server Name Type** | Choose **ipv4** or **ipv6**, according to the server address type, or choose **dns** if you enter a server domain name in the **Server Name Value** field. |

| Parameter Name | Description |
|---|---|
| **Server Name Value** | IP address or domain name of the server. |
| **Source IP** | By default, this is the system IP address. You can choose the **Device Specific** option to specify per device. |
| **Priority** | Filter the type of log messages saved using one of the following priority options, listed from lowest to highest priority.<br>Each priority option configures the device to save log messages of that priority and all higher priorities.<br>For example, information is the lowest priority of message, so choosing **information** includes information log messages and all other log messages too. Choosing **error** excludes information, notice, and warn log messages, but includes error messages and all other log messages of higher priority (critical, alert, and emergency).<br>From lowest to highest priority, the options are the following:<br>• information<br>• notice<br>• warn<br>• error<br>• critical<br>• alert<br>• emergency |

- **Network Protocol** feature:

***Table 208: Basic Configuration***

| Parameter Name | Description |
|---|---|
| **Passthrough** | The cellular gateway operates in one of two modes: IP passthrough and NAT.<br>In IP passthrough mode, the cellular gateway passes the public IP address assigned by the internet service provider (ISP) to a downstream device attached to the cellular gateway.<br>Disabling the **Passthrough** option enables NAT, which gives the devices that are connected to the cellular gateway access to a DHCP server and to the local gateway.<br>**Note** Enabling passthrough mode disables and hides the other fields in the **Basic Configuration** section. |
| **DHCP Pool** | |

| Parameter Name | Description |
|---|---|
| **DHCP Pool** | Enable a DHCP pool for NAT. |
| **DHCP Network Pool** | IP address pool, in classless interdomain routing (CIDR) format. |
| **Lease Days** | Days for DHCP lease time<br>Range: 0 to 365 |
| **Lease Hours** | Hours for DHCP lease time.<br>Range: 0 to 23 |
| **Lease Minutes** | Minutes for DHCP lease time.<br>Range: 0 to 59 |
| **PAT Configuration** | |
| **PAT Configuration** | Enable port address translation (PAT). |
| **Add PAT Config** | Click this to add one or more PAT configurations. |
| **Description** | Description of the PAT configuration. |
| **Protocol** | Choose **TCP** or **UDP**. |
| **LocalAddress** | IPv4 format address. |
| **LocalPort** | Port number.<br>Range: 0 to 65535 |
| **InterfaceName** | Preconfigured as Cellular1/0, which is the WAN interface for the cellular gateway. |
| **GlobalPort** | Global port number.<br>Range: 1 to 65535 |

***Table 209: NTP Servers***

| Parameter Name | Description |
|---|---|
| **NTP** | To configure a network time protocol (NTP) server, enter an IPv4 address or a DNS name.<br>Maximum number of NTP servers: 4 |

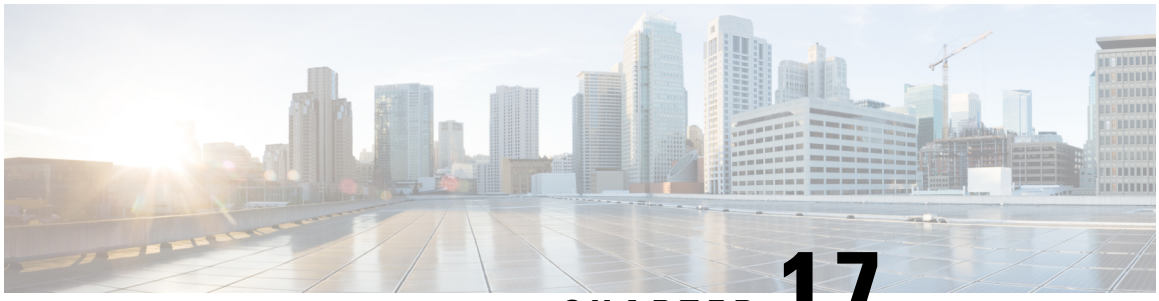
4. (Optional) To add CLI configuration commands, do the following:
   a. Open the **CLI Add-on Profile**.
   b. Click **Add Feature**.
   c. In the **Type** drop-down list, choose **Config**.

**d.** Enter a name for the feature.

**e.** Enter a CLI configuration.

**f.** Click **Save**.

**Note** CLI configuration commands in the CLI Add-on Profile override any configuration done using the Global Profile.



CHAPTER 17

# Configure Geofencing

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 210: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Geofencing | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1 | This feature provides a way to restrict a device's location to an operational geographical boundary, and to identify a device's location and report any violations of the configured boundary. If the device is identified to be in violation, you can restrict network access to the device using Cisco SD-WAN Manager operational commands.<br>In the CLI or a CLI template, configure geofencing coordinates for establishing the location of the device. You can also register for SMS alerts. |
| Added Support for Configuring Geofencing Using a **Cisco System** Feature Template | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a<br>Cisco vManage Release 20.7.1 | This feature adds support for configuring the geographical boundary of a device using a **Cisco System** feature template.<br>With this feature, you can also configure automatic geolocation detection, where the device determines its own location, while configuring geofencing. A new parameter **auto-detect-geofencing-location** is added to the **geolocation (system)** command. |

| Feature Name | Release Information | Description |
|---|---|---|
| Added Support for LTE Advanced NIM Modules | Cisco IOS XE Catalyst SD-WAN Release 17.8.1a | Added support for Long-Term Evolution (LTE) Advanced Network Interface Modules (NIMs) for Cisco ISR 4000 routers. |


- Information About Geofencing, on page 748
- Supported Devices for Geofencing, on page 749
- Prerequisites for Geofencing, on page 750
- Restrictions for Geofencing, on page 750
- Configure Geofencing Using a Cisco System Template, on page 750
- Configure Geofencing Using the CLI, on page 752
- Verify Geofencing Configuration, on page 753
- Monitor Geofencing Alarms, on page 755
- Configuration Example for Geofencing, on page 756


# Information About Geofencing

Geofencing allows you to define a geographical boundary within which a device can be deployed. When devices are detected outside of the boundary, SMS alerts as well as critical-event alarms can be generated to Cisco SD-WAN Manager.

Global Positioning System (GPS) within a Long-Term Evolution Pluggable Interface Module (PIM) is used for device detection and monitoring in Cisco IOS XE Catalyst SD-WAN devices.

On the device CLI or through a Cisco SD-WAN Manager CLI template, you can configure the following settings:

- Base location (latitude and longitude) and a geofence range for device detection
- Short-message service (SMS) alert registration for sending SMS messages to a mobile number
- GPS enablement on a Long-Term Evolution PIM in the controller cellular 0/x/0 section

**Note** You can also enable GPS on a Long-Term Evolution PIM using a feature template.

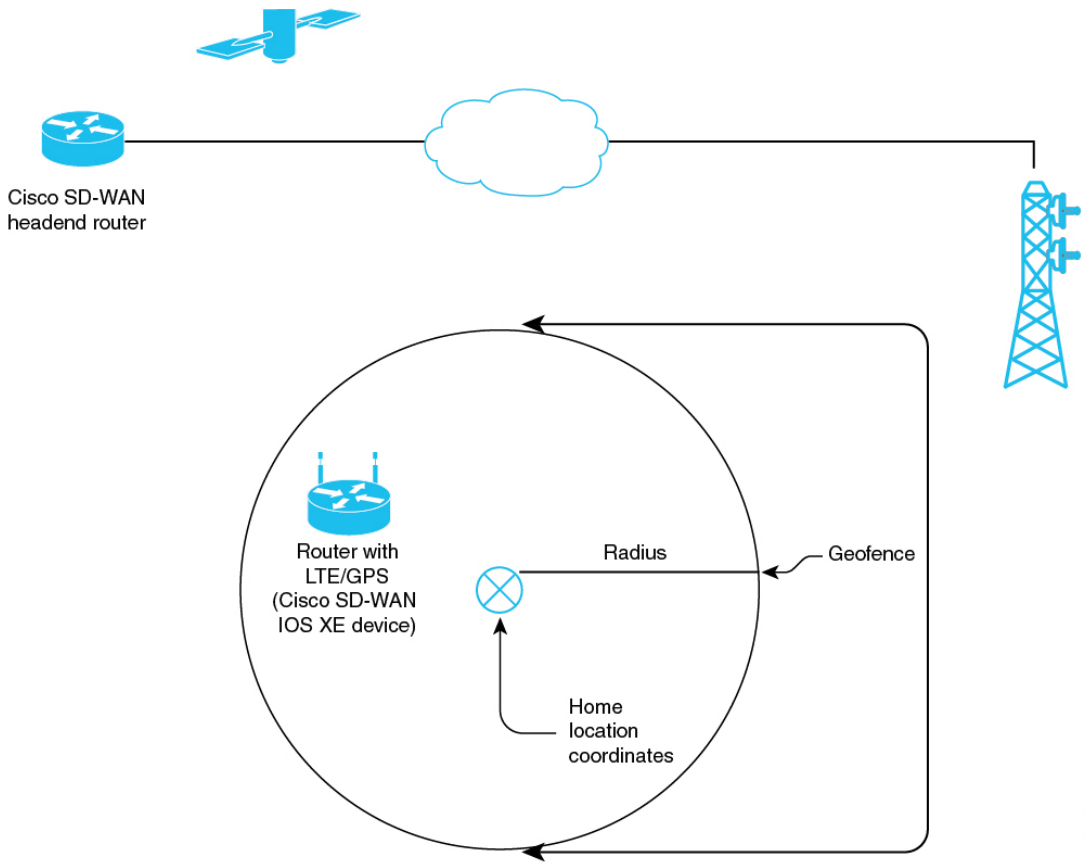
Starting from Cisco vManage Release 20.7.1, you can configure geofencing using a **Cisco System** feature template. You can also enable automatic geolocation detection of a device where the device determines its own base location.

In Cisco SD-WAN Manager, you can use operational commands for restricting network access if a device exceeds its geographical boundary.

For more information on the operational commands for restricting network access, see the Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide.

Geofencing status alerts are sent to Cisco SD-WAN Manager upon detection of device boundary violations.

*Figure 6: Overview of Geofencing*




## Benefits of Geofencing

- Protects against inappropriate access to an organization's network if a device is beyond its geographical boundary
- Notifies end users of any displaced devices
- Supports a geofence radius for specifying the target location of the device
- Supports SMS alerts for mobile phone alerts

# Supported Devices for Geofencing

Supported Devices:

- Cisco ISR 1000 with Long-Term Evolution (fixed and pluggable)
- Cisco Catalyst 8K with Long-Term Evolution Pluggable Interface Module (PIM)
- Cisco ISR 4000 with Long-Term Evolution Advanced Network Interface Modules (NIMs)

Supported Long-Term Evolution PIMs:

- P-LTE-VZ(WP7601)
- P-LTE-US(WP7603)
- P-LTE-JN(WP7605)
- P-LTE-MNA(WP7610)
- P-LTE-GB(WP7607)
- P-LTE-IN(WP7608)
- P-LTE-AU(WP7609)
- P-LTEA-EA(EM7455)
- P-LTEA-LA(EM7430)

Supported Long-Term Evolution Advanced NIMs:

- NIM-LTEA-EA(EM7455)
- NIM-LTEA-LA(EM7430)

# Prerequisites for Geofencing

- Ensure that your Cisco IOS XE Catalyst SD-WAN C1100 series router has a built-in Long-Term Evolution interface.
- Enable geofencing using the CLI or a CLI template. From Cisco vManage Release 20.7.1, you can also enable geofencing using a feature template.

  For more information, see *Cisco IOS XE SD-WAN Qualified Command Reference*.
- A SIM card is mandatory in the Long-Term Evolution PIM for receiving SMS alerts.

# Restrictions for Geofencing

- Geofencing can be used only in Cisco Catalyst SD-WAN controller mode.

# Configure Geofencing Using a Cisco System 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 Geofencing Using the CLI

### Configure Latitude, Longitude, a Geofence Range, and Enable SMS Alerts

This section provides example CLI configurations for the following:

- Configure a base location, latitude and longitude.
- Enable automatic detection of a device where the device determines its own location.
- Enable, configure, and specify a geofence range.

**Note**
- Geofencing range unit is in meters.
- Geofencing range is an optional configuration parameter, and if not configured, it takes the default value of 100 meters.

- Add mobile numbers for receiving SMS alerts.

**1.** Configure a base location:

```
Device(config)# system
Device(config-system)# gps-location latitude 37.317342 longitude -122.218170
```

**2.** Enable automatic detection of a device:

```
Router(config)# system
Router(config-system)# no gps-location latitude
Router(config-system)# no gps-location longitude
Router(config-system)# gps-location auto-detect-geofencing-location
```

**Note** Do not configure latitude and longitude coordinates when using the auto-detect-geofencing-location parameter.

You can choose to either configure a base location using latitude and longitude coordinates, or you can enable automatic detection of a device.

**3.** Enable, configure, and specify a geofence range:

```
Device(config-system)# gps-location geo-fencing-enable
Device(config-system)# gps-location geo-fencing-config
Device(conf-geo-fencing-config)# geo-fencing-range 1000
```

4. Set up an SMS alert by adding the cell phone numbers for the users of the device:

```
Device(config-geo-fencing-config)# sms

Device(config-sms)# sms-enable
Device(config-sms)# mobile-number +12344567234
Device(config-mobile-number-+12344567234)# exit
Device(config-mobile-number-+12344567234)# mobile-number +12344567235
Device(config-mobile-number-+12344567235)# exit
Device(config-mobile-number-+12344567235)# mobile-number +12344567236
Device(config-mobile-number-+12344567236)# exit
Device(config-mobile-number-+12344567236)# mobile-number +12344567237
Device(config-mobile-number-+12344567237)# exit
Device(config-sms)# commit
```

5. Commit your changes.

### Enable GPS on a Long-Term Evolution PIM in the Controller Cellular Section

This section provides sample CLI configurations for enabling GPS on the Long-Term Evolution PIM in the 0/x/0 section of the configuration.

1. Enable GPS on a Long-Term Evolution PIM in the controller cellular section:

```
Device(config)# controller Cellular 0/2/0
Device(config-Cellular-0/2/0)# lte gps enable
```

2. Enable ms-based mode with a SIM card present in a Long-Term Evolution PIM. We recommend that you use ms-based with a SIM card present.

   Mobile station-based assistance refers to the case where the Global Navigation Satellite System (GNSS-enabled) mobile device computes its own position locally.

```
Device(config-Cellular-0/2/0)# lte gps mode ms-based
```

3. Enable National Marine Electronics Association (NMEA) streaming:

```
Device(config-Cellular-0/2/0)# lte gps nmea
```

4. Commit your changes.

# Verify Geofencing Configuration

The following is a sample output from the **show sdwan geofence-status** command:

```
Device# show sdwan geofence-status
geofence-status
 Geofence Config Status =                 Geofencing-Enabled
 Target Latitude =                        37.317342
 Target Longitude =                       -122.218170
 Geofence Range(in m) =                   100
 Current Device Location Status =         Location-Valid
 Current Latitude =                       37.317567
 Current Longitude =                       -122.218170
 Current Device Status =                  Within-defined-fence
 Distance from target location(in m) =    30
```

```
 Last updated device location timestamp =  2021-05-06T22:58:34+00:00
 Auto-Detect Geofencing Enabled =          true
```

In this output, `Geofence Config Status = Geofencing-Enabled`, so geofencing is enabled.

In this output, `Auto-Detect Geofencing Enabled = true`. Therefore, automatic detection of the device is enabled. If automatic detection of the device is not enabled, `Auto-Detect Geofencing Enabled = false` is displayed in the output.

The following is a sample output from the **show cellular 0/x/0 gps** command:

```
Device# show cellular 0/2/0 gps
GPS Feature =  enabled
GPS Mode Configured =  ms-based
GPS Port Selected =  Dedicated GPS port
GPS Status =  GPS coordinates acquired
Last Location Fix Error =  Offline [0x0]
============================
GPS Error Count =  0
NMEA packet count =  17899
NMEA unknown packet count =  0


Per talker traffic count =
        US-GPS =  5982
        GLONASS =  2560
        GALILEO =  3505
        BEIDOU =  0
        GNSS =  3409
        Unknown talker =  2443
============================
Speed over ground in km/hr =  0
============================

Latitude =  31 Deg 19 Min 14.6203 Sec North
Longitude =  122 Deg 58 Min 32.8164 Sec West
*Apr 15 23:58:45.298: GPS Mode Configured =Timestamp (GMT) =  Thu Apr 15 23:57:21 2021

Fix type index =  0, Height =  18 m
Satellite Info
---------------
Satellite #2, elevation 51, azimuth 42, SNR 24 *
Satellite #5, elevation 36, azimuth 144, SNR 34 *
Satellite #6, elevation 14, azimuth 45, SNR 24 *
Satellite #12, elevation 72, azimuth 146, SNR 33 *
Satellite #25, elevation 60, azimuth 305, SNR 25 *
============================
 Total Satellites in view =  5
 Total Active Satellites =  5
 GPS Quality Indicator =  1
 Total satellites from each constellation:
         US-GPS =  3
         GLONASS =  1
         GALILEO =  1
         BEIDOU =  0
============================
```

In this output, `GPS Feature = enabled` and `GPS Mode Configured = ms-based`. Therefore, GPS for controller cellular is enabled, and `ms-based` is configured.

The following is a sample output from the **show sdwan notification stream viptela** command:

```
Device# show sdwan notification stream viptela
notification
 eventTime 2021-04-13T23:05:02.881093+00:00
```

```
 system-logout-change
  severity-level minor
  host-name pm5
  system-ip 172.16.255.15
  user-name admin
  user-id 0
 !
!
notification
 eventTime 2021-04-14T00:36:31.344117+00:00
 geo-fence-alert-status
  severity-level major
  host-name pm5
  system-ip 172.16.255.15
  alert-type device-location-inside
  alert-msg Device Locking started for Geofencing Mode and device is within range
```

# Monitor Geofencing Alarms

You can monitor geofencing alarms based on severity or based on time.

The following are the types of geofencing alarms.

***Table 211: Geofencing Alarm Types***

| Type | Severity | Description |
|---|---|---|
| **Device Location Outside** | **Critical** | This notification is sent when the device location is outside the defined geofencing range. |
| **Device Location Inside** | **Major** | This notification is sent when the device location is determined to be inside the defined geofence range when it was previously determined to be outside the defined geofence range, or the device location could not be obtained due to a GPS signal outage. |
| **Device Location Lost** | **Major** | This notification is sent when the device location cannot be determined due to a GPS outage. |
| **Device Location Update** | **Major** | This notification is sent when the device location changes by more than 20 meters either when geofencing is enabled or not. If geofencing is not enabled, this notification is sent only if the device location is available. |

You can monitor geofencing alarms using Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs**.

Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.

2. If there are geofencing alarms, the alarms display in the form of a chart, followed by a table.

   You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.

3. To view the alarm details, click **. . .** and choose **Alarm Details** to view information about the device.

# Configuration Example for Geofencing

### End-to-End Configuration for Geofencing and Controller Cellular

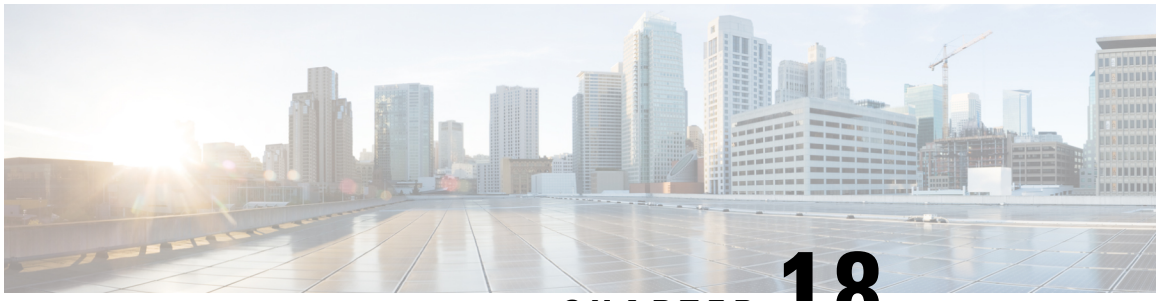
The following is an end-to-end sample output that displays the configuration process for geofencing and controller cellular when configuring automatic detection of a device:

```
system
  gps-location auto-detect-geofencing-location
  gps-location geo-fencing-enable
  gps-location geo-fencing
    geo-fencing-range 1000
    sms
      sms-enable
      mobile-number +112312345676
      !
      mobile-number +112312345677
      !
      mobile-number +112312345678
      !
      mobile-number +112312345679
      !
     !
    !
  system-ip             10.1.1.35
  site-id               273
  admin-tech-on-failure
  organization-name     LTE-Test
  vbond vbond-dummy.test.info port 12346
  !
  controller Cellular 0/2/0
  lte gps enable
  lte gps mode ms-based
  lte gps nmea
  !
```

The following is an end-to-end sample output that displays the configuration process for geofencing and controller cellular when manually configuring latitude and longitude coordinates:

```
system
   gps-location latitude 37.317342
   gps-location longitude -122.218170
   gps-location geo-fencing-enable
   gps-location geo-fencing-config
    geo-fencing-range 1000
    sms
     sms-enable
     mobile-number +112312345676
     !
     mobile-number +112312345677
```

```
!
mobile-number +112312345678
!
mobile-number +112312345679
!
!
!
```



CHAPTER 18

# VRRP Interface Tracking

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 212: 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<br><br>Cisco vManage Release 20.7.1 | This feature enables VRRP to set the edge as active or standby based on the WAN Interface or SIG tracker events and increase the TLOC preference value on a new VRRP active to ensure traffic symmetry, for Cisco IOS XE Catalyst SD-WAN Devices.<br><br>Starting this release, you can configure VRRP interface tracking through Cisco SD-WAN Manager feature template and CLI template on Cisco IOS XE Catalyst SD-WAN Devices. |


- Information About VRRP Interface Tracking, on page 760
- Restrictions and Limitations, on page 760
- VRRP Tracking Use Cases, on page 760
- Workflow to Configure VRRP Tracking, on page 761
- Configure an Object Tracker, on page 761
- Configure VRRP for a VPN Interface Template and Associate Interface Object Tracker, on page 762
- Configure VRRP Tracking Using CLI Templates, on page 763
- Configuration Example for VRRP Object Tracking Using CLI, on page 765

• Configuration Examples for SIG Object Tracking, on page 765
• Monitor VRRP Configuration, on page 765
• Verify VRRP Tracking, on page 766

# Information About VRRP Interface Tracking

The Virtual Router Redundancy Protocol (VRRP) is a LAN-side protocol that provides redundant gateway service for switches and other IP end stations. In Cisco IOS XE Catalyst SD-WAN devices, you can configure VRRP on interfaces and subinterfaces using Cisco SD-WAN Manager templates and CLI add-on templates.

For more information, see Configuring VRRP.

# Restrictions and Limitations

- VRRP is only supported with service-side VPNs. If you are using subinterfaces, configure VRRP physical interfaces in VPN 0.
- VRRP tracking is enabled on either a physical uplink interface or a logical tunnel interface (IPSEC or GRE or both).
- The VRRP Tracking feature does not support IP prefix as an object.
- You can use the same tracker under multiple VRRP groups or VPNs.
- You cannot use the same track object to track multiple interfaces.
- You can group a maximum of 16 track objects under a list track object.
- You cannot configure **tloc-change** and **increase-preference** on more than one VRRP group.

# VRRP Tracking Use Cases

The VRRP state is determined based on the tunnel link status. If the tunnel or interface is down on the primary VRRP, then the traffic is directed to the secondary VRRP. The secondary VRRP router in the LAN segment becomes primary VRRP to provide gateway for the service-side traffic.

### Zscaler Tunnel Use Case 1—Primary VRRP, Single Internet Provider

The primary and secondary Zscaler tunnels are connected through a single internet provider to the primary VRRP. The primary and secondary VRRP routers are connected through using TLOC extension. In this scenario, the VRRP state transition occurs if the primary and secondary tunnels go down on primary VRRP. The predetermined priority value decrements when the tracking object is down, which triggers the VRRP state transition. To avoid asymmetric routing, VRRP notifies this change to the Overlay through OMP.

### Zscaler Tunnel Use Case 2—VRRP Routers in TLOC Extension, Dual Internet Providers

The primary and secondary VRRP routers are configured in TLOC extension high availability mode. The primary and secondary Zscaler tunnels are directly connected with primary and secondary VRRP routers, respectively, using dual internet providers. In this scenario too, the VRRP state transition occurs if the primary and secondary tunnels go down on primary VRRP. The predetermined priority value decrements when the

tracking object is down, which triggers the VRRP state transition. VRRP notifies this change to the Overlay through OMP.

### TLOC Preference

Transport Locators (TLOCs) connect an OMP route to a physical location. A TLOC is directly reachable using an entry in the routing table of the physical network, or represented by a prefix beyond a NAT device.

In Cisco IOS XE Catalyst SD-WAN devices, the TLOC change increase preference value increases based on the configured value. You can configure the TLOC change increase preference value on both the active and the backup nodes.

# Workflow to Configure VRRP Tracking

1. Configure an object tracker. For more information, see Configure an Object Tracker, on page 761.
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 762.

# 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 213: 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 214: 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** explicitly.<br>**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.<br>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**.

# Configure VRRP Tracking Using CLI Templates

You can configure VRRP tracking using the CLI add-on feature templates and CLI device templates. For more information, see CLI Templates.

# VRRP Object Tracking Using CLI

### Interface Object Tracking using CLI

Use the following configuration to add an interface to a track list using Cisco SD-WAN Manager device CLI tempale:

```
Device(config)# track <object-id1> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track < object-id2> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
```

```
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit
Device(config)# interface GigabitEthernet2


Device(config-if)# vrf forwarding <vrf-number>

Device(config-if)# ipv4 address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)# exit
```

# SIG Container Tracking

The following example shows how to configure a track list and tracking for SIG containers using the Cisco SD-WAN Manager device CLI template.

**Note** In Cisco IOS XE Catalyst SD-WAN Release 17.7.1a SIG Object Tracking, you can only set *global* as the variable for Service Name.

### SIG Object Tracking Using CLI

```
Device(config)# track <object-id1> service global


Device(config-tracker)# exit
Device(config)# track <object-id2> service global
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit

Device(config)# interface GigabitEthernet2

Device(config-if)# vrf forwarding <vrf-number>

Device(config-if)# ip address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)#exit
```

# Configuration Example for VRRP Object Tracking Using CLI

### Interface Object Tracking Using CLI

```
config-transaction
  track 100 interface Tunnel123 line-protocol
   exit
 track 200 interface GigabitEthernet5 line-protocol
  exit
track 400 list boolean and
  object 100
  object 200
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 400 decrement 10
  tloc-change increase-preference 333
  exit
```

# Configuration Examples for SIG Object Tracking

### SIG Object Tracking Using CLI

```
config-transaction
  track 1 service global
  exit
  exit
  track 2 service global
track 3 list boolean and
  object 1
  object 2
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 3 decrement 10
  tloc-change increase-preference 333
  exit
```

# 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**.

# Verify VRRP Tracking

Device# **show vrrp**

The following is a sample output for the **show vrrp** command:

```
GigabitEthernet2 - Group 1 - Address-Family IPv4
  State is MASTER
  State duration 37 mins 52.978 secs
  Virtual IP address is 10.10.1.10
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 100
  State change reason is VRRP_TRACK_UP
  Tloc preference configured, value 333
    Track object 400 state UP decrement 10
  Master Router is 10.10.1.1 (local), priority is 100
  Master Advertisement interval is 1000 msec (expires in 607 msec)
  Master Down interval is unknown
  FLAGS: 1/1
```

Device# **show track brief**

The following is a sample output for the **show track brief** command:

```
Track Type        Instance                  Parameter        State Last Change
100   interface   Tunnel123                 line-protocol    Up    00:12:48
200   interface   GigabitEthernet5          line-protocol    Up    00:49:57
400   list                                  boolean          Up    00:12:47
```

Device# **show track list**

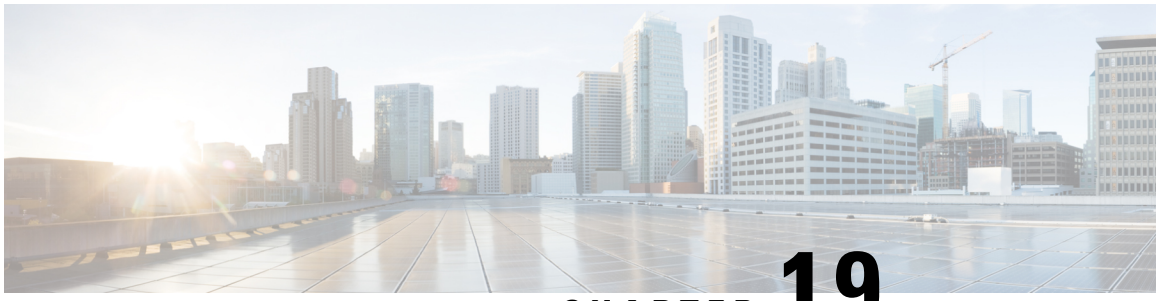
The following is a sample output for the **show track list** command:

```
Track 400
  List boolean and
  Boolean AND is Up
    6 changes, last change 00:12:58
    object 100 Up
    object 200 Up
  Tracked by:
    VRRPv3 GigabitEthernet2 IPv4 group 1
```

Device# **show track list brief**

The following is a sample output for the **show track brief** command:

```
Track Type        Instance                  Parameter        State Last Change
400   list                                  boolean          Up    00:13:02
```



CHAPTER 19

# Configure VDSL and G.SHDSL

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

This chapter provides usage information and guidelines for configuring very-high-data-rate DSL (VDSL) and G.symmetric high bit rate DSL (G.SHDSL) in SD-WAN mode.


- Configure VDSL, on page 769
- Configure G.SHDSL, on page 773


# Configure VDSL

The following table provides usage information and guidelines for configuring asymmetric DSL (ADSL2/2+) and VDSL for supported Integrated Services Router Network Interface Modules (ISR NIMs) in SD-WAN mode. VDSL2 and ADSL2/2+ provide highly reliable WAN connections for remote sites.

For related information, see VDSL Commands.

| Function | Command | Guidelines |
|---|---|---|
| Configure operating mode | Device# **configure terminal**<br>Device(config)# **controller VDSL** *slot/subslot/port*<br>Device(config)# **operating mode auto** | To switch from operating mode auto adsl1 (adsl2+/ or vdsl2) to operating mode auto ads2+ (adsl1 or vdsl2), switch to operating mode auto first.<br>Before you change the operating mode, ensure that line-mode is changed to line-mode single-wire line 0. |

| Function | Command | Guidelines |
|---|---|---|
| Enable DSL on a line | Device(config)# **line-mode single-wire line***line-number* | This command is supported only on DSL NIM-VAB-A. |
| Enable bonding | Device(config)# **line-mode bonding** | This command is supported only on DSL NIM-VAB-A. |
| Load firmware on a device | Device# **configure terminal**<br>Device(config)# **controller VDSL** *slot*/*subslot*/*port*<br>Device(config-controller)# **firmware phy filename** *filename* | The Cisco Catalyst SD-WAN CLI template does not support specifying the file location. Prepend the file name with flash: or with bootflash:, depending on its location. |
| Enable or disable SRA | Device(config-controller)# **sra** | The Cisco Catalyst SD-WAN CLI template does not support the sra *line number* command. In line-mode bonding, sra enables sra on both lines and no sra disables sra on both lines. |
| Enable or disable bitswap | Device(config-controller)# **bitswap** | The Cisco Catalyst SD-WAN CLI template does not support the bitswap *line number* command. In line-mode bonding, bitswap enables bitswap on both lines and no bitswap disables bitswap on both lines. |
| Enable modem features | Device(config-controller)# **modem***keyword* | – |
| Display a description of a controller | Device(config-controller)# **description** *string* | – |
| Enable dual ended line testing | Device(config-controller)# **diagnostics DELT** | – |
| Modify the file in which the training log is stored | Device(config-controller)# **training log filename flash:** *filename* | The Cisco Catalyst SD-WAN CLI template does not support specifying the file location. Prepend the file name with flash: or with bootflash:, depending where the file should be stored. |
| Enable sync mode | Device(config-controller)# **sync mode** *mode* | To switch from one sync mode to another, delete the existing sync mode, then configure the new one. |

| Function | Command | Guidelines |
|---|---|---|
| Enable sync interval | Device(config-controller)# **sync interval** *seconds* | – |

### Command Examples

```
Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config)# operating mode auto


Device# config-transaction
Device(config)# line-mode single-wire line 1


Device# config-transaction
Device(config)# line-mode bonding


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# firmware phy filename flash:IDC_1.7.2.6_DFE_FW_BETA_120111A.pkg


Device# config-transaction
Device(config-controller)# sra


Device# config-transaction
Device(config-controller)# bitswap


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# modem customUKAnnexM


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# description to ISP 1


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# diagnostics DELT


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# training log filename bootflash:VDSLLOG.log


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# sync mode ansi previous


Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# sync interval -4
Device(config-ptp-port)# end
```

### Configuration Example

```
Device(config)# show controllers vdSL 0/2/0
Controller VDSL 0/2/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xA39A
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:     FGL2149956Y C1117-4P 16.7.20180
Serial Number Far:
Modem Version Near:     16.7.20180709:09395
Modem Version Far:      0xa39a

Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.993.2 (VDSL2) Profile 17a

TC Mode:                PTM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running

Failed full inits:      0
Short inits:            0
Failed short inits:     0

Modem FW  Version:      4.14L.04
Modem PHY Version:      A2pv6F039t.d26d

Line 0:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                      ON
SRA:                     enabled                 enabled
SRA count:               0                       0
Bit swap:                enabled                 enabled
Bit swap count:          1                       3
Line Attenuation:        18.4 dB                  0.0 dB
Signal Attenuation:       0.0 dB                  0.0 dB
Noise Margin:             5.2 dB                 6.0 dB
Attainable Rate:        46022 kbits/s           18866 kbits/s
Actual Power:           14.5 dBm                10.4 dBm
Per Band Status:        D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):   13.9    32.7    50.1    N/A     25.6    37.7    42.3
Signal Attenuation(dB): 13.5    32.4    N/A     N/A     25.0    36.9    41.9
Noise Margin(dB):       5.3     5.1     N/A     N/A     6.0     6.0     5.9
Total FECC:             446                      0
Total ES:               3                        0
Total SES:              0                        0
Total LOSS:             0                        0
Total UAS:              50                       50
Total LPRS:             0                        0
Total LOFS:             0                        0
Total LOLS:             0                        0


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):            NA           47610           NA              18859
SRA Previous Speed:      NA               0           NA                  0
Previous Speed:          NA               0           NA                  0
```

```
Reed-Solomon EC:          NA             446           NA               0
CRC Errors:               NA              51           NA               0
Header Errors:            NA            3935           NA               0
Interleave (ms):          NA            1.00           NA            1.00
Actual INP:               NA            0.00           NA            0.00

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin
```

# Configure G.SHDSL

## Overview

G.SHDSL is an international standard that allows devices to send and receive high-speed symmetrical data streams over a single pair of copper wires. This section provides information about the Cisco G.SHDSL EFM/ATM NIM and provides guidelines for configuring G.SHDSL in SD-WAN mode.

For related information, see Configuring Cisco G.SHDSL HWICs in Cisco Access Routers and VDSL Commands.

## Cisco G.SHDSL EFM/ATM NIM

The Cisco G.SHDSL EFM/ATM NIM connects Cisco 4000 Series Integrated Services Routers with central office Digital Subscriber Line Access Multiplexers (DSLAMs) and supports up to four DSL pairs. The DSL pairs are bundled in groups and configured in the Cisco IOS CLI by using the dsl-group command. Use the mode command to choose the mode (ATM or EFM).

The NIM supports the following configuration:

- You can configure up to four DSL groups.
- You can configure auto mode on only one DSL group. For example, DSL group 0.
- In ATM Mode, you can configure the lines to use 2-wire, 4-wire (standard or enhanced), or m-pair.
- In EFM mode, you can configure a DSL group with any one of the lines in 2-wire non-bonding mode or with multiple lines in bonding mode.
- Depending on the mode (ATM or EFM), the corresponding interface (ATM or EFM) is automatically created.

## Cisco G.SHDSL Configuration Guidelines

The following table provides usage information and guidelines that apply when you configure the Cisco G.SHDSL EFM/ATM in CPE or CO mode.

| Function | Command | Guidelines |
|---|---|---|
| Configure a device with the dsl-group auto command | Device(config-controller)# **dsl-group auto** | Use customer premises equipment (CPE) mode when configuring a device with the dsl-group auto command. If you use this command in Central Office (CO) mode, the configuration does not take effect. |

| Function | Command | Guidelines |
|---|---|---|
| Add or delete a link | — | The efm-grp command is not supported. To add or delete a link to a dsl-group, delete the dsl-group, then create a new dsl-group. |
| Load firmware on a device | Device(config-controller)# **firmware phy filename** *location* | File name location options are not supported when using the firmware phy command. Prepend the file name with flash: or with bootflash:, depending on the location. |
| Create or delete an annex | Device(config-controller-dsl-group)# **no shdsl annex**<br>Device(config-controller-dsl-group)# **no shdsl rate** *rate* | To avoid Cisco IOS and Cisco Catalyst SD-WAN configuration from going out of sync when you create or delete an annex, create or delete the rate in the same transaction. |
| Enable SHDSL to use enhanced mode | (config-controller-dsl-group)# **shdsl 4-wire mode enhanced** | To enable SHDSL to use the enhanced mode in a 2-pair digital subscriber line (DSL) group, use the shdsl 4-wire mode enhanced command in configuration controller DSL group mode. |
| Ignore CRC errors | (config-controller-dsl-group)# **ignore***seconds* | To configure a device to ignore CRC errors, use the ignore command. Replace *timeout* with a value from 0 through 60, which indicates the number of seconds that the device ignores CRC errors that do not resolve before the device terminates an action. |
| Shutdown a DSL group | (config-controller-dsl-group)# **shutdown** | To shut down a DSL group, use the shutdown command. |

### Examples

```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# dsl-group auto
```

```
Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# firmware phy filename bootflash:IDC_1.1.1.0_DFE_1.1-1.8.1__001.pkg
```

```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# dsl-group 0 pairs 0
```

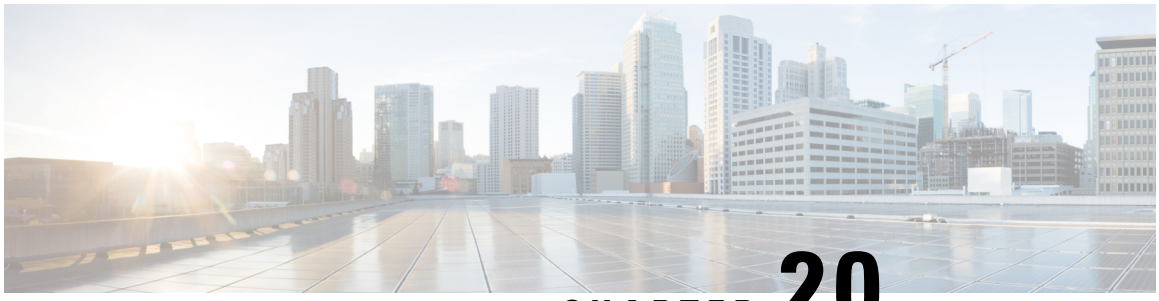
```
Device(config-controller-dsl-group)# no shdsl annex
Device(config-controller-dsl-group)# no shdsl rate 5696


Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
(config-controller-dsl-group)# shdsl 4-wire mode enhanced


Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
config-controller-dsl-group)# ignore 30


Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
config-controller-dsl-group)# shutdown
```

## Configuration Example

```
Device# sh controllers shDSL 0/1/0
Controller SHDSL 0/1/0 is UP
  Hardware is NIM-SHDSL-EA, on slot 0,bay 0
  Capabilities: EFM: 2-wire, EFM-Bond, Annex A, B, F & G
                ATM: 2-wire, Mpair, Annex A, B, F & G
  CPE termination
  cdb=0x7F7EB723D8A8
  Vendor: Intel, Chipset: SOCRATES-4e
  PHY Source: System
  IDC Firmware version: 0.0.0.0
  DFE Firmware version:
  Group 0 info:
        Type: EFM Auto status: Down
         Ethernet Interface: Ethernet0/1/0, hwidb: 0x7F7EB723B648
         ATM Interface: ATM0/1/0, hwidb: 0x7F7EB724CE08
        Configured/active num links: 4/0, bit map: 0xF/0x0
        Line termination: CPE, Annex: auto
        PMMS disabled,Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Dying Gasp: Present
        SHDSL wire-pair (0) is in DSL DOWN state
                LOSWS Defect alarm: none
                SNR Margin alarm: none
                Loop Attenuation alarm: none
                Termination: CPE, Line mode: EFM Auto, Annex: auto
                Line coding: AUTO-TCPAM
                Configured/actual rate: AUTO/0 kbps
                Modem status: DOWN_NOT_READY,Condition: NO_COND_
        DSL Stats:
                Power Back Off: 0dB
                LoopAttn: 0dB, SnrMargin: 0dB
                Current 15 minute statistics (Time elapased 1 seconds)
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 15 minute statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Current 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 24 hr statistics
```

```
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
EFM Stats:
        EFM-TC Tx: data frames: 0
        EFM-TC Rx: data frames: 0
SHDSL wire-pair (1) is in DSL DOWN state
        LOSWS Defect alarm: none
        SNR Margin alarm: none
        Loop Attenuation alarm: none
        Termination: CPE, Line mode: EFM Auto, Annex: auto
        Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Modem status: DOWN_NOT_READY,Condition: NO_COND_
DSL Stats:
        Power Back Off: 0dB
        LoopAttn: 0dB, SnrMargin: 0dB
        Current 15 minute statistics (Time elapased 1 seconds)
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 15 minute statistics
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Current 24 hr statistics
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 24 hr statistics
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
EFM Stats:
        EFM-TC Tx: data frames: 0
        EFM-TC Rx: data frames: 0
SHDSL wire-pair (2) is in DSL DOWN state
        LOSWS Defect alarm: none
        SNR Margin alarm: none
        Loop Attenuation alarm: none
        Termination: CPE, Line mode: EFM Auto, Annex: auto
        Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Modem status: DOWN_NOT_READY,Condition: NO_COND_
DSL Stats:
        Power Back Off: 0dB
        LoopAttn: 0dB, SnrMargin: 0dB
        Current 15 minute statistics (Time elapased 1 seconds)
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 15 minute statistics
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Current 24 hr statistics
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 24 hr statistics
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
EFM Stats:
        EFM-TC Tx: data frames: 0
        EFM-TC Rx: data frames: 0
SHDSL wire-pair (3) is in DSL DOWN state
        LOSWS Defect alarm: none
        SNR Margin alarm: none
        Loop Attenuation alarm: none
        Termination: CPE, Line mode: EFM Auto, Annex: auto
        Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Modem status: DOWN_NOT_READY,Condition: NO_COND_
DSL Stats:
        Power Back Off: 0dB
        LoopAttn: 0dB, SnrMargin: 0dB
        Current 15 minute statistics (Time elapased 1 seconds)
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 15 minute statistics
                ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Current 24 hr statistics
```

```
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        EFM Stats:
                EFM-TC Tx: data frames: 0
                EFM-TC Rx: data frames: 0
Group 1 is not configured
Group 2 is not configured
Group 3 is not configured
```



CHAPTER 20

# Dynamic On-Demand Tunnels

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 215: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Dynamic On-Demand Tunnels | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | This feature enables you to configure an Inactive state for tunnels between edge devices, reducing performance demands on devices and reducing network traffic. |
| Dynamic On-Demand Tunnels with Transport Gateways | Cisco Catalyst SD-WAN Control Components Release 20.12.1<br>Cisco IOS XE Catalyst SD-WAN Release 17.12.1a | A transport gateway can serve as the hub between two spoke devices, providing the backup route that is necessary for spoke-to-spoke on-demand tunnels to operate.<br>Using a transport gateway as the hub simplifies the process of enabling on-demand tunnels. This method does not require any change to control policy on Cisco SD-WAN Controllers. |


- Information About On-Demand Tunnels, on page 780
- Prerequisites for On-Demand Tunnels, on page 782

• Restrictions for On-Demand Tunnels, on page 785
• Configure On-Demand Tunnels, on page 786
• Monitor the Status of On-Demand Tunnels, on page 789

# Information About On-Demand Tunnels

Cisco Catalyst SD-WAN supports dynamic 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. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance.

### Backup Route and Reactivating the Tunnel

To enable two spoke device peers to use on-demand tunnels, they must have an alternate route, a backup route, through a hub. Using the backup route, either spoke device can resume traffic flow between the two spokes, which reactivates the tunnel to handle the traffic directly from peer to peer.

### Advantages

On-demand tunnels offer the following advantages:

- Improved performance, especially for less-powerful platforms operating in a full-mesh network.
- Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes.
- Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network.
- Direct tunnels between spokes, while also optimizing CPU and memory usage.

### Mechanism

When you configure a site to use dynamic tunnels, the on-demand functionality is enabled. In this mode of operation, Cisco Catalyst SD-WAN edge routers do not bring up direct tunnels to other sites that are also enabled with on-demand functionality.

Cisco Catalyst SD-WAN selects one or more edge routers (typically centrally located routers) to act as backup forwarding node(s), providing a secondary path for traffic between two nodes. The backup node(s) are not enabled for on-demand. All on-demand sites form static tunnels with the backup node(s). The backup node(s) provide a static backup route for traffic between two nodes that have on-demand enabled.

The first packet of traffic between two nodes is routed though the static backup path, and triggers the on-demand tunnel to become active between the sites. The backup path continues to forward traffic until the direct path becomes active.

All on-demand sites learn the TLOCs and prefixes of all other on-demand remote sites. The prefixes also have a backup path set up through Cisco Catalyst SD-WAN Controller control policy. So in the control plane, the on-demand tunnel network has the same state as a full-mesh tunnel network, including a backup path. The control plane downloads to the data plane, routes, with the backup path and remote TLOCs that represent a potential direct path between any two sites, but it does not set up a direct path tunnel to remote TLOCs.

Traffic from either end of the on-demand tunnel triggers setting up the tunnel. This enables on-demand tunnels to accommodate network address translation (NAT) traversal.

The on-demand tunnel feature introduces two states for the on-demand branch site:

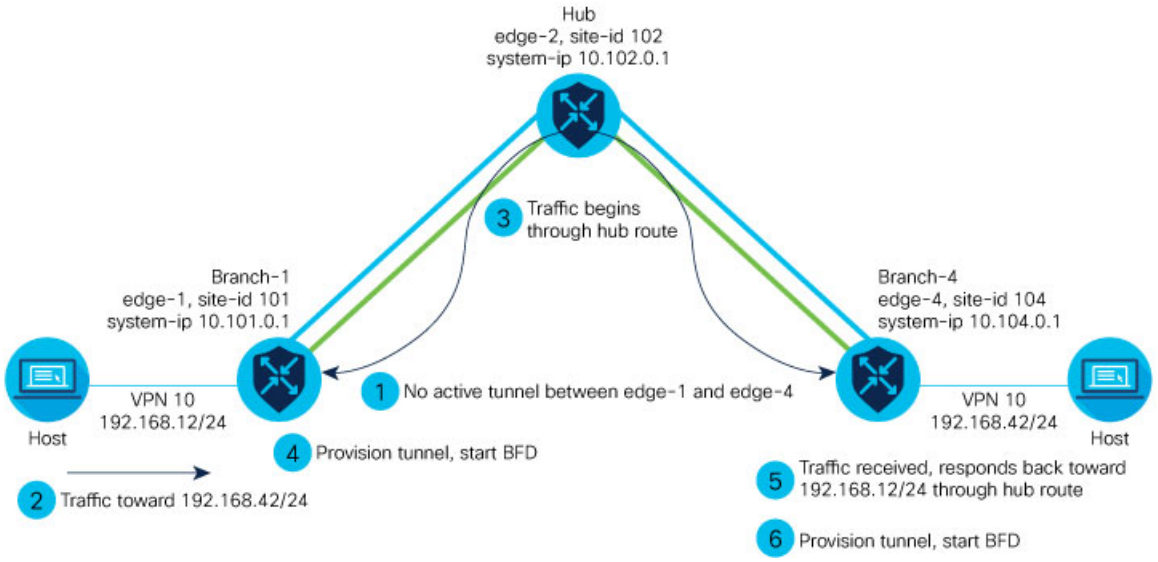
- **Inactive**: The on-demand tunnel is not set up with the remote site. There is no active traffic to or from the remote site. Remote site TLOCs are inactive - no bidirectional forwarding detection (BFD) is set up, the prefix is installed with the inactive paths, and the backup path is set as the path to forward any traffic. The inactive path detects flows and triggers a direct site-to-site tunnel to be set up.
- **Active**: The on-demand direct site-to-site tunnel is set up to the remote site. There is active traffic to or from the remote site. This state is identical to the case of a typical tunnel, where the remote TLOCs have BFD set up, and the prefix is installed with the direct path tunnel. In this state, tunnel activity is tracked. If there is no traffic for the “idle time” duration (default 10 minutes), the direct site-to-site tunnel is removed and the state changes to Inactive.

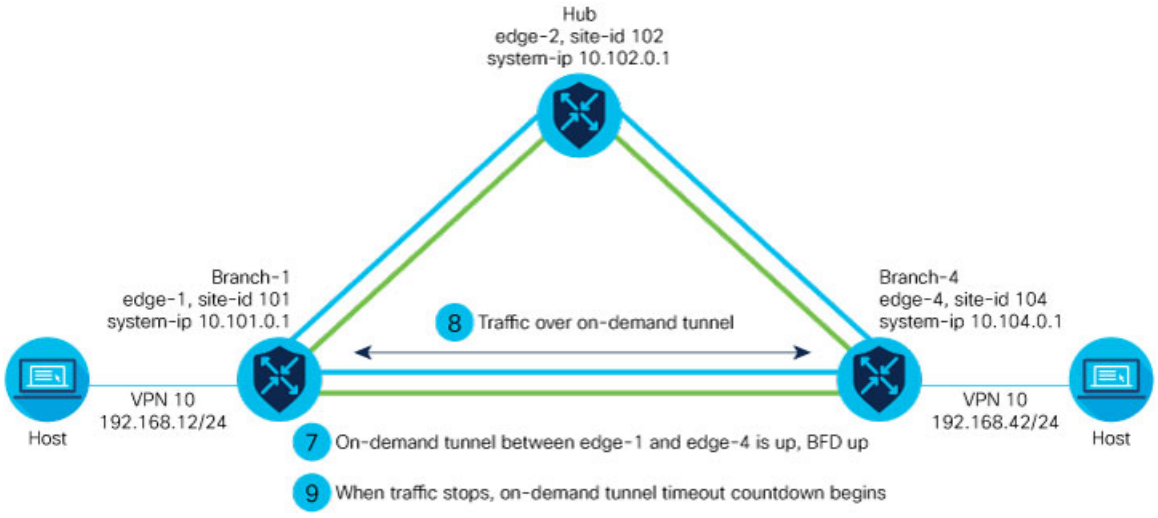
### Steps in Illustrations

The figures below show the following steps that occur between two edge routers with an on-demand tunnel configured.

1. There is no active tunnel between the two edge routers. edge-1 and edge-4 are in Inactive state.
2. The host behind edge-1 initiates traffic toward the host behind edge-4.
3. edge-1 forwards the traffic through the backup path using the hub or backup node to edge-4.
4. edge-1 provisions the on-demand tunnel and begins bidirectional forwarding detection (BFD). edge-4 is now in Active state on edge-1.
5. When edge-4 receives the return traffic for the host behind edge-1, it forwards the traffic through the backup path using the hub or backup node to edge-1.
6. edge-4 provisions the on-demand tunnel and begins BFD. edge-1 is now in Active state on edge-4.
7. At this point, the on-demand tunnel between edge-1 and edge-4 is up, and BFD is up.
8. Traffic between the two edge devices takes the direct route through the on-demand tunnel.
9. Both edge-1 and edge-4 track the traffic activity on the on-demand tunnel in both directions.

   If there is no traffic for the idle timeout duration, the on-demand tunnel is deleted, and the edge-1 and edge-4 devices go back to the Inactive state.




### On-Demand Tunnels with a Transport Gateway

A transport gateway can serve as the hub between two spoke devices, providing the backup route that is necessary for spoke-to-spoke on-demand tunnels to operate. Using a transport gateway as the hub simplifies the process of enabling on-demand tunnels. This method does not require configuring control policy on Cisco SD-WAN Controllers.

For information about configuration, see Configure On-Demand Tunnels Using a Transport Gateway, on page 787.

# Prerequisites for On-Demand Tunnels

There are several prerequisites for using on-demand tunnels:

- Configure a Centralized Control Policy for On-Demand Tunnels, on page 786

- Prerequisites: OMP Settings, on page 783
- Prerequisites: Hub Device Traffic Engineering Service, on page 783
- Prerequisites: Spoke Device ECMP Limit, on page 784


# Prerequisites: OMP Settings

The Cisco Catalyst SD-WAN Controller send-path-limit must be more than the default 4.

**Explanation**: When on-demand tunnels are enabled, spokes use backup paths through the hub, so a higher path limit is necessary. The direct paths as well as the backup paths need to be advertised. To accommodate this, increase the Cisco Catalyst SD-WAN Controller send-path-limit to advertise all available paths. We recommend to use the maximum possible value.

**Note** If there are too many Hub TLOCs configured in the on-demand tunnel control policy, the recommended value for **send-path-limit** is not enough always. In such cases, the on-demand tunnel feature will not work at all.

Starting from Cisco vManage Release 20.8.1 and Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, the maximum **send-path-limit** is 32. In Cisco vManage Release 20.7.x and earlier releases, the maximum **send-path-limit** is 16.

For information about configuring Cisco SD-WAN Controller **send-path-limit**, see the routing configuration guides on the Cisco Catalyst SD-WAN Configuration Guides page.

### Configure the OMP Send Path Limit Using Cisco SD-WAN Manager

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 and click **Cisco OMP**.
5. In **Basic Configuration**, set the **Number of Paths Advertised per Prefix** to 16 (recommended).

### Configure the OMP Send Path Limit Using a CLI Template

```
omp
 no shutdown
 send-path-limit 16
 graceful-restart
```

# Prerequisites: Hub Device Traffic Engineering Service

On the hub device, the Traffic Engineering service (service TE) must be enabled.

**Explanation**: This ensures that the Cisco Catalyst SD-WAN Overlay Management Protocol (OMP) on the spoke devices accepts the backup path through the hub, which is being added as an intermediate path between the two spoke devices. Without this, the backup path through the hub would be considered invalid and unresolved by the spoke devices.

### Enable the Traffic Engineering Service Using Cisco SD-WAN Manager

1. In Cisco SD-WAN Manager, open **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 platform.
5. From **VPN**, select **VPN**.
6. Ensure that in **Basic Configuration**, the **VPN** field is set to 0.
7. From **Service**, click **New Service** and select **TE**.
8. Click **Add**, and then click **Update**. The TE service appears in the table of services.
9. Apply the VPN-0 template to the hub.

### Enable the Traffic Engineering Service Using a CLI Template (Cisco IOS XE Catalyst SD-WAN Devices)

```
sdwan
 service TE vrf global
exit
```

### Enable the Traffic Engineering Service Using a CLI Template (Cisco vEdge Devices)

```
vpn 0
 service TE
 exit
```

# Prerequisites: Spoke Device ECMP Limit

On spoke devices, the ecmp-limit must be more than the default 4. Recommended: 16

**Explanation**: When on-demand tunnels are enabled, spoke devices create both direct and backup paths. To accommodate the need for more paths, increase the ecmp-limit.

### Configure the ECMP Limit Using Cisco SD-WAN Manager

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 and click **Cisco OMP**.
5. In **Basic Configuration**, set the **ECMP Limit** field to 16 (recommended).

#### Configure the ECMP Limit Using a CLI Template

```
omp
 no shutdown
 ecmp-limit       16
```

**Note** You can view the current ecmp-limit using the **show running-config omp** command.

# Restrictions for On-Demand Tunnels

- On-demand tunnel Performance Routing (PfR) statistics collection starts fresh every time an on-demand tunnel is setup. PfR statistics are not cached for deleted on-demand tunnels after idle timeout.
- Out of order (OOO) packets may occur when traffic moves from the backup path to the direct on-demand tunnel. Packets are forwarded by the Cisco Catalyst SD-WAN router as they are received.
- Unidirectional flows do not trigger on-demand tunnel setup. They continue to use the backup path.
- Multicast traffic does not trigger on-demand tunnel setup. It continues to use the backup path.
- Do not configure a data policy that applies a **set tloc-list** action to an on-demand site TLOC. If configured, traffic will be dropped.
- On-demand tunnels are not supported when the Pair Wise Key (PWK) IPSEc feature is enabled.
- All TLOCs in the system are reset (disabled and then enabled) when you execute **on-demand enable** or **no on-demand enable**.
- When an edge device provisions on-demand tunnels, it provisions to all the TLOCs on the remote site.
- For a multi-home site to be in on-demand mode, you must configure on-demand enable on all of the systems at the site.
- All edge devices using on-demand tunnels are kept active if there is a service or user traffic on any on-demand tunnel in either direction.
- On-demand tunnels can be enabled between two sites only if both sites are enabled with on-demand mode.
- The first packet to any host behind a remote site triggers on-demand tunnel setup to that remote site. Return traffic from that host triggers tunnel setup in the opposite direction.

- All prefixes from on-demand remote sites must also have a backup path configured. If not, sites will not be able set up on-demand tunnels. The backup path is a static tunnel and must be always UP.
- The setup or removal of on-demand tunnels does not affect overlay route (OMP) updates by Cisco Catalyst SD-WAN Controller, or service/LAN-side route updates (examples: OSPF or BGP).
- If either the local site or the remote site is not in on-demand mode, static tunnels are set up between the sites.

# Configure On-Demand Tunnels

The following procedures describe how to configure on-demand tunnels using different methods, including using control policy, or a simpler method using a transport gateway as a hub.

# Configure On-Demand Tunnels Using Control Policy

To configure on-demand tunnels using the control policy method, do the following:

1. Configure a control policy, as described in Configure a Centralized Control Policy for On-Demand Tunnels, on page 786.
2. On spoke devices, enable on-demand tunnels, as described in Enable On-Demand Tunnels on a Spoke Device Using Cisco SD-WAN Manager, on page 788 and Enable On-Demand Tunnels Using a CLI Template, on page 789.

## Configure a Centralized Control Policy for On-Demand Tunnels

### Before You Begin

This procedure configures a centralized control policy on a Cisco Catalyst SD-WAN Controller to enable on-demand tunnels.

- The Cisco Catalyst SD-WAN Controller centralized control policy must include the **tloc-action backup** action.

  **Explanation**: This ensures that the backup path through the hub for communication between all of the spoke devices.

- The Cisco Catalyst SD-WAN Controller centralized control policy must accept all spoke prefix routes.
- The Cisco Catalyst SD-WAN Controller centralized control policy must accept TLOCs of all spokes.

  For information about configuring a Cisco SD-WAN Controller **centralized control policy**, see the policies configuration guides on the Cisco Catalyst SD-WAN Configuration Guides page.

- When configuring on-demand tunnels using a transport gateway, do not use the control policy procedure described here. For information, see Configure On-Demand Tunnels Using a Transport Gateway, on page 787.

### Configure Centralized Control Policy for On-Demand Tunnels Using Cisco SD-WAN Manager

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

2. Select **Centralized Policy**.
3. Click **Add Topology** and select **Custom Control (Route & TLOC)**.
4. From **Match Conditions**, in **Site** , select one or more site lists, and click **Accept**.
5. From **Actions**, in **TLOC Action**, select the **Backup** action.
6. From **TLOC List**, select an existing TLOC list or create a new one.

### Configure Centralized Control Policy for On-Demand Tunnels Using a CLI Template

```
viptela-policy:policy
 control-policy Dynamic-Tunnel-Control-Policy
    sequence 100
     match route
      site-list Branches
     !
     action accept
      set
       tloc-action backup
       tloc-list Hub-TLOCs
      !
     !
     sequence 200
      match tloc
     !
     action accept
    !
  default-action accept
 !
 lists
  site-list Branches
   site-id 200
   site-id 300
  !
  tloc-list Hub-TLOCs
   tloc 10.0.0.1 color mpls encap ipsec
   tloc 10.0.0.1 color public-internet encap ipsec
!
!
apply-policy
 site-list Branches
  control-policy Dynamic-Tunnel-Control-Policy out
 !
!
```

# Configure On-Demand Tunnels Using a Transport Gateway

### Before You Begin

- On Cisco SD-WAN Controllers, configure the send path limit, as described in Prerequisites: OMP Settings, on page 783.
- On spoke devices, configure the ECMP limit, as described in Prerequisites: Spoke Device ECMP Limit, on page 784.

- When using a transport gateway as a hub to support on-demand tunnels, there is no need to create or modify a control policy. Do not use the procedure described in Configure a Centralized Control Policy for On-Demand Tunnels, on page 786.

### Configure On-Demand Tunnels Using Transport Gateways

1. On a router serving as the hub, providing a backup route between spokes, enable transport gateway functionality, as described in , in the Transport Gateway section of the *Cisco Catalyst SD-WAN Routing Configuration Guide*.
2. On spoke devices, enable on-demand tunnels and configure the idle timeout, as described in Enable On-Demand Tunnels on a Spoke Device Using Cisco SD-WAN Manager, on page 788.

# Enable On-Demand Tunnels on a Spoke Device Using Cisco SD-WAN Manager

### Before You Begin

- 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. In the case of multi-homed sites, enable on-demand on all systems at the site.

### Enable On-Demand Tunnels on a Spoke 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 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.

# Enable On-Demand Tunnels Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global configuration mode.

### Before You Begin

- See Prerequisites for On-Demand Tunnels, on page 782.
- Do not enable on-demand on the hub device

### Enable On-Demand Tunnels

On the spoke devices, enable on-demand tunnels at the system level. In the case of multi-homed sites, enable on-demand on all systems in the site.

The default idle timeout value is 10 minutes. Range: 1 to 65535 minutes

### Example

```
system
     on-demand enable
     on-demand idle-timeout 10
```

# Monitor the Status of On-Demand Tunnels

The following sections describe procedures for monitoring the status of on-demand tunnels.

# View the Current Status of On-Demand Tunnels Using Cisco SD-WAN Manager

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. Select a device.
3. Select **Real Time**.
4. For **Device Options**, select one of the following:
   - **On Demand Local**: Displays the status of on-demand tunnels on the specified device.
   - **On Demand Remote**: Displays the status of on-demand tunnels on the specified device, and on all connected devices.

The output is equivalent to executing the **show** [**sdwan**] **system on-demand** [**remote-system**] [**system-ip** *ip-address*] CLI command. It displays the status of on-demand tunnels.

# View a Chart of the On-Demand Tunnel Status Over Time in Cisco SD-WAN Manager

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. Select a device.
3. From **WAN**, choose **Tunnel**.
4. From the **Chart Options** drop-down list, select **On-Demand Tunnel Status**. The chart shows the status of tunnels as ACTIVE or INACTIVE. INACTIVE indicates that an on-demand tunnel is in Inactive mode.

# View the Route to a Destination Device

Viewing the route between routers A and B can show whether the route is using an on-demand tunnel. On router A, use the **traceroute** command and enter router B as the destination. The command output shows whether the current route includes a hop at a hub device or whether the route is directly to the destination.

In the following examples, the router IP addresses are as follows:

- Router A: 10.1.1.1
- Router B: 10.1.1.2
- Hub device: 10.100.1.100

### No Active On-Demand Tunnel

In the following example, there is no active on-demand tunnel between routers A and B, so the route includes the hub device. Note that it takes two hops to reach router B.

```
RouterA#traceroute vrf 1 10.1.1.2 numeric
Type escape sequence to abort.
Tracing the route to 10.1.1.2
VRF info: (vrf in name/id, vrf out name/id)
1 10.100.1.100 10 msec 8 msec 0 msec
2 10.1.1.2 2 msec * 1 msec
```

### Active On-Demand Tunnel

In the following example, there is an active on-demand tunnel between routers A and B, so the route from router A and to router B is direct.

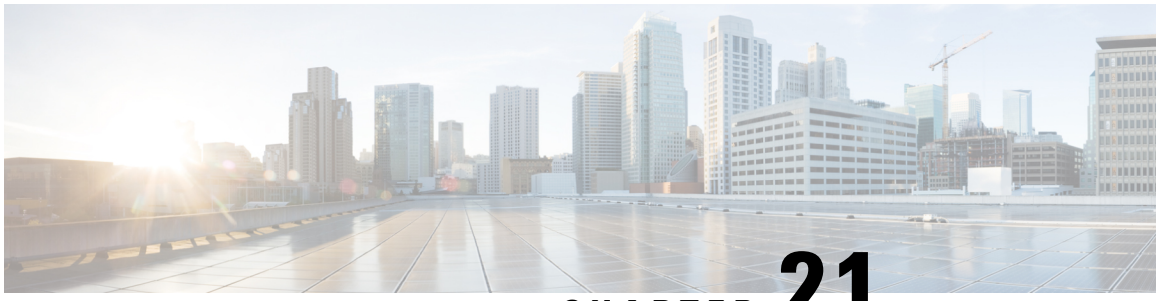
```
RouterA#traceroute vrf 1 10.1.1.2 numeric
Type escape sequence to abort.
Tracing the route to 10.1.1.2
VRF info: (vrf in name/id, vrf out name/id)
1 10.1.1.2 1 msec
```

# View OMP Routes

Viewing OMP routes can show the status of on-demand tunnels between two routers. Use the **show sdwan omp routes** command and view the **STATUS** column. The following table shows the possible values for this column, depending on whether an on-demand tunnel is active or not between two routers:

*Table 216: Status of Routes, with or without an Active On-Demand Tunnel Between Two Routers*

| On-Demand Tunnel Between Routers A and B | STATUS for OMP Routes Between Routers A and B | STATUS for Backup Routes (through the Hub) |
|---|---|---|
| Not active | I, U, IA<br>(installed, unresolved, and inactive) | C, I, R<br>(chosen, installed, and resolved) |
| Active | C, I, R<br>(chosen, installed, and resolved) | R<br>(resolved) |



CHAPTER 21

# Track Static Routes for Service VPNs

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 217: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Static Route Tracker for Service VPNs | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | This feature enables you to configure IPv4 static route endpoint tracking for service VPNs.<br>For static routes, endpoint tracking determines whether the configured endpoint is reachable before adding that route to the route table of the device. |
| 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<br>Cisco vManage Release 20.7.1 | This feature enables you to configure the TCP/UDP static route endpoint trackers. Using this feature you can also configure IPv4, TCP/UDP dual endpoint static-route tracker groups for service VPNs to enhance the reliability of probes. |


- Information About Static Route Tracking, on page 794
- Supported Platforms, on page 794
- Restrictions for IPv4 Static Route Tracking, on page 794

• Workflow to Configure IPv4 Static Route Tracking, on page 795
• Configure Static Routes Using CLI, on page 799
• Configuration Examples for Static Route Tracking Using the CLI, on page 800
• Verify Static Route Tracking Configuration Using CLI, on page 802

# Information About Static Route Tracking

Static-route tracking for service VPNs enables you to track the availability of the configured endpoint address to determine if the static route can be included in the routing table of a device. This is applicable when a site uses a static route in a service VPN to advertise its route over Overlay Management Protocol (OMP). The static route tracker periodically sends ICMP ping probes to the configured endpoint. If the tracker does not receive a response, the static route is not included in the routing table and is not advertised to OMP. You can configure an alternative next-hop address or a static route with a higher administrative distance to provide a backup path. This path is advertised over OMP.

**Note** From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure TCP/UDP individual endpoint trackers and configure a tracker group with dual endpoints (using two trackers), and associate the trackers and tracker group to a static route. Dual endpoints help in avoiding false negatives that might be introduced because of the unavailability of the routes.

# Supported Platforms

- Cisco ASR 1000 Series Aggregated Services Routers
- Cisco ISR 1000 Series-Integrated Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco CSR 1000 Series Cloud Service Routers

# Restrictions for IPv4 Static Route Tracking

- Only one endpoint tracker is supported per static route per next-hop address.
- IPv6 static routes are not supported.
- To configure a static route with tracker:
  1. Delete any existing static route, if it is already configured without a tracker. Plan for any connectivity downtime that might occur during this step for static route advertisement.
  2. Configure a new static route with tracker using the same prefix and next-hop as the deleted static route.
- To add a new tracker after you reach maximum tracker limit per router:
  1. Delete an old tracker and attach the template to the device.

2. Add a new tracker and attach the device to the template again.

- UDP tracker endpoint enabled with IP SLA UDP packet responder is supported only on Cisco IOS XE Catalyst SD-WAN devices.
- You cannot link the same endpoint-tracker to static routes in different VPNs. Endpoint-tracker is identified by a name and can be used for multiple static routes in a single VPN.

# Workflow to Configure IPv4 Static Route Tracking

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 218: Tracker Parameters***

| Field | Description |
|---|---|
| Name | Name of the tracker. The name can be up to 128 alphanumeric characters. |

| Field | Description |
|---|---|
| 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).<br>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.<br>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.<br>**Note** Configuring the tracker type Static Route using endpoint URL or endpoint DNS name is not supported. |
| 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 219: 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**.<br>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. |

| Fields | Description |
|---|---|
| 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**.<br>**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.<br>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**.

# Configure Static Routes Using CLI

The following sections provide information about how to configure static routes using the CLI.

### Configure a Static Route Tracker

**Note** You can configure static route tracking using the Cisco SD-WAN Manager CLI Add-on feature templates and CLI device templates. For more information on configuring using CLI templates, see CLI Templates.

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

### Configure a Static Route Tracker with TCP Port as the Endpoint

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> tcp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

### Configure a Static Route Tracker with UDP Port as the Endpoint

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> udp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

### Configure Tracker Groups

**Note** You can create tracker groups to probe static routes from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1.

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name1>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> tcp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name1> endpoint-tracker

Device# config-transaction
Device(config)# endpoint-tracker <tracker-name2>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> udp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name2> endpoint-tracker

Device(config)# endpoint-tracker <static-tracker-group>
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements <tracker-name1> <tracker-name2>
Device(config-endpoint-tracker)# boolean {and | or}
Device(config-endpoint-tracker)# exit
Device(config)# track <static-tracker-group> endpoint-tracker

Device(config)# ip route vrf <vrf-name> <prefix> <mask> <nexthop-ipaddress>
<administrative-distance> track name <static-tracker-group>
```

**Note**

- Use the **ip route** command to bind a tracker or tracker group with a static route and to configure a backup route for administrative distance that is higher than the default value of 1.
- You can apply only one tracker to an endpoint.
- A tracker group can have a mix of endpoint trackers. For example, you can create a tracker group with an IP address tracker and UDP tracker.

# Configuration Examples for Static Route Tracking Using the CLI

### Configure Tracker

This example shows how to configure a single static route tracker:

```
config-transaction
```

```
!
 endpoint-tracker tracker1
!
  tracker-type static-route
  endpoint-ip 10.1.1.1
  threshold 100
  multiplier 5
  interval 20
  exit
!
track tracker1 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name tracker1
```

This example shows how to configure a tracker with TCP port as endpoint:

```
config-transaction
!
 endpoint-tracker tcp-10001
!
  tracker-type static-route
  endpoint-ip 10.0.0.1 tcp 10001
  threshold    100
  interval     10
  multiplier   1
  exit
!
track tcp-10001 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name tcp-10001
```

This example shows how to configure a tracker with UDP port as endpoint:

```
config-transaction
!
  endpoint-tracker udp-10001
!
    tracker-type static-route
    endpoint-ip 10.0.0.1 udp 10001
    threshold    100
    interval     10
    multiplier   1
    exit
!
track udp-10001 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name udp-10001
```

### Configure Tracker Groups

This example shows how to configure a tracker group with two trackers (two endpoints). You can create tracker groups to probes static routes from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
config-transaction
!
 endpoint-tracker tcp-10001
!
    tracker-type static-route
    endpoint-ip 10.1.1.1 tcp 10001
    threshold 100
    multiplier 5
    interval 20
```

```
    track tcp-10001 endpoint-tracker
!
 endpoint-tracker udp-10002
!
   tracker-type static-route
   endpoint-ip 10.2.2.2 udp 10002
   threshold 100
   multiplier 5
   interval 20
   track udp-10002 endpoint-tracker
!
endpoint-tracker static-tracker-group
!
  tracker-type tracker-group
  tracker-elements tcp-10001 udp-10002
  boolean and
  track static-tracker-group endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name static-tracker-group
```

**Note**

- You must configure an administrative distance when you are configuring through CLI templates.
- Use the **ip route** command to bind the tracker or tracker group with a static route and to configure a backup route for administrative distance when it is higher than the default value of 1.
- You can apply only one tracker to an endpoint.

# 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:

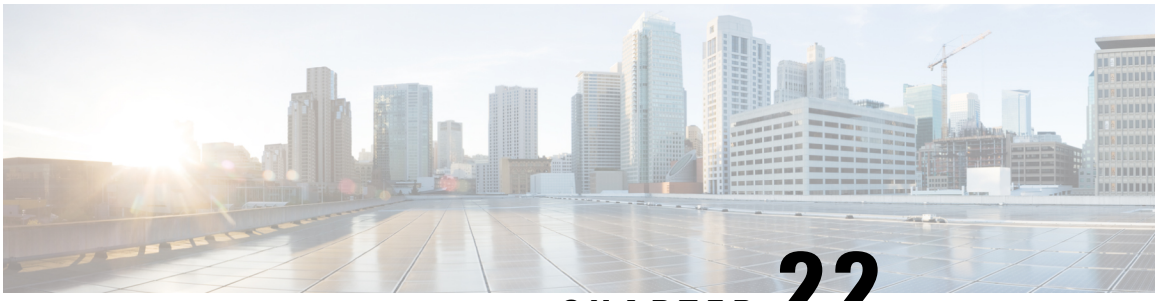
```
Device# show endpoint-tracker group
Tracker Name               Element trackers name    Status         RTT in msec  Probe ID

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:

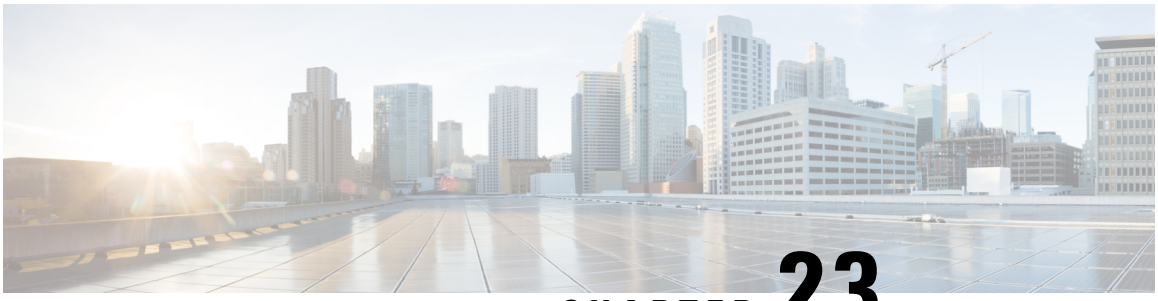
```
Device# show ip static route vrf 1
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, 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]
```



CHAPTER 22

# NAT DIA Tracker for Cisco IOS XE Catalyst SD-WAN Devices

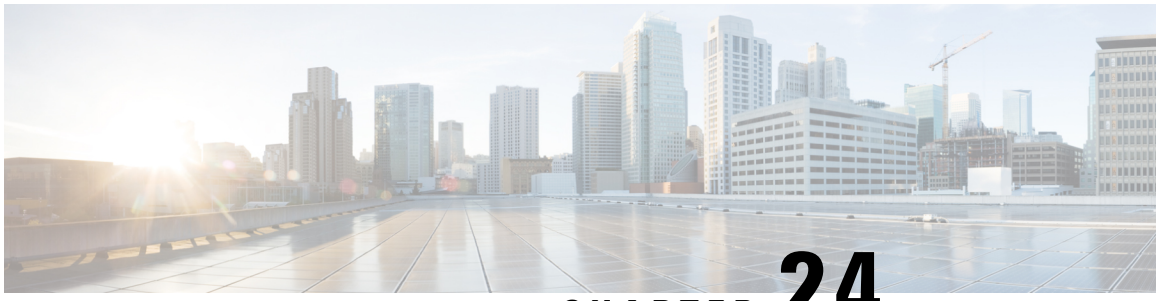
For information on the NAT DIA tracker for Cisco IOS XE Catalyst SD-WAN devices, see the NAT DIA Tracker section of the *Cisco Catalyst SD-WAN NAT Configuration Guide, Cisco IOS XE Release 17.x*.



CHAPTER 23

# Service-Side NAT on Cisco IOS XE Catalyst SD-WAN Devices

For information on service-side NAT on Cisco IOS XE Catalyst SD-WAN devices, see the Service-Side NAT section in the *Cisco Catalyst SD-WAN NAT Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.



CHAPTER 24

# DHCP Vendor Option Support

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 220: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| DHCP Vendor Option Support | Cisco IOS XE Catalyst SD-WAN Release 17.10.1a<br>Cisco vManage Release 20.10.1 | This feature allows DHCP client options, 124 and 125 to configure vendor-specific information in client-server exchanges.<br>Configure this feature using the CLI Add-on feature template in Cisco SD-WAN Manager. |


- Information about DHCP Vendor Option Support, on page 809
- DHCPv6 Client Options, on page 810
- Configure DHCP Vendor Option Using a CLI Template, on page 811
- Configure DHCPv6 Client Option Using a CLI Template, on page 812


# Information about DHCP Vendor Option Support

The configurable dynamic host configuration protocol client functionality allows a DHCP client to use a user-specified client identifier, class identifier, or suggested lease time when requesting an address from a DHCP server.

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The DHCP client provides flexibility by allowing the following options to be configured for a DHCP client:

- Option 124—This option is used by DHCP clients and servers to exchange vendor-class information.
- Option 125—This option is used by DHCP clients and servers to exchange vendor-specific information.

In the DHCP address assignment workflow, Option 124 (Vendor-Identifying Vendor Class) and Option 125 (Vendor-Identifying Information) are used to provide differential services. These options are used by Zero-Touch Provisioning (ZTP), Cisco Plug-and-Play (PnP), and Identity Services Engine (ISE) across solutions to enable several use cases. For example, the content of Option 124 is used for device classification, enable solution specific feature and so on.

By default, Cisco IOS XE DHCP client sends the following data:

| Attribute | IPv4 DHCP Option | Default Value |
|---|---|---|
| Vendor-Identifying Vendor Class Option | 124 | PID |

**Note** The **ip dhcp client vendor-class <mac-address | ascii | disable | hex>** command overrides PID with MAC Address or user defined string or disable Option 124.

The DHCP Vendor Option Support feature introduces new CLI parameters to make Option 124 and Option 125 flexible. You can modify and customize enabling vendor specific options to carry different values for different customer features. The combination of Option 124 and Option 125 enables various features.

The **ip dhcp client vendor-class** command provides flexibility to pack either Device PID or MAC Address of the DHCP client or any user configurable string in option-124. The default behavior for this command is to continue to send Device PID when you choose option 124. The default behavior can be overridden to carry MAC Address in Day 1 configuration mode by explicitly requesting option-125 from the server using the **ip dhcp client vendor-class** command.

# DHCPv6 Client Options

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The DHCP client provides flexibility by allowing the following options to be configured for a DHCP client:

- Option 16—This option is used by DHCP clients and servers to exchange vendor-class information.
- Option 17—This option is used by DHCP clients and servers to exchange vendor-specific information.

In DHCPv6, option-16 and option-17 is used by DHCP clients and servers to exchange vendor-specific information.

By default, Cisco IOS XE DHCP client sends the following data:

| Attribute | IPv6 DHCP Option | default value |
|---|---|---|
| Vendor Class Option | 16 | PID |

**Note** The **ipv6 dhcp client vendor-class <mac-address | hex | ascii | disable>** command can be used to override default value of PID with MAC Address or User defined string or disable the option.

The **ipv6 dhcp client vendor-class** command provides flexibility to pack either Device PID or MAC Address of the DHCP Client or any user configurable string in option-16. The default behavior for this command is to continue to send Device PID when you choose option 16 but it can be overridden to carry MAC Address in Day 1 configuration mode using the **ipv6 dhcp client vendor-class** command.

# Configure DHCP Vendor Option Using a CLI Template

For more information about using CLI templates, see Create a CLI Add-On Feature Template.

**Note** By default, CLI templates execute commands in global config mode.

The section provides a sample CLI configurations to configure DHCP vendor option.

1. Configure an interface type and enter the interface configuration mode.

   ```
   interface type number
   ```

2. Acquire an IP address on an interface from DHCP.

   ```
   ip address dhcp
   ```

3. Configure the DHCP vendor-class option.

   ```
   ip dhcp client vendor-class [mac-address | ascii | hex | disable]
   ```

**Note** You must first configure the **no ip dhcp-client** command before configuring the IP address.

The following example shows the configuration to override the decive PID with MAC address:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class mac-address
    !
```

The DHCP vendor-class option, overrides the Device PID with MAC Address.

The following example shows the configuration to override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class hex aabbcc
    !
```

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class ascii cisco
    !
```

The following example shows the configuration to disable option-124 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class disable
    !
```

# Configure DHCPv6 Client Option Using a CLI Template

For more information about using CLI templates, see Create a CLI Add-On Feature Template.

**Note** By default, CLI templates execute commands in global config mode.

The section provides a sample CLI configurations to configure DHCP vendor option.

1. Configure an interface type and enter the interface configuration mode.

   ```
   interface type number
   ```

2. Acquire an IPv6 address on an interface from DHCP.

   ```
   ipv6 address dhcp
   ```

3. Configure the DHCP vendor-class option.

   ```
   ipv6 dhcp client vendor-class {mac-address | ascii | hex | disable}
   ```

By default DHCPv6 client carries device PID of the device in option-16. This default behaviour can be overridden by configuring the **ipv6 dhcp client vendor-class** command.

The following example shows the configuration to override the decive PID with MAC address:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class mac-address
    !
```

The DHCPv6 vendor-class option, overrides the Device PID with MAC Address.

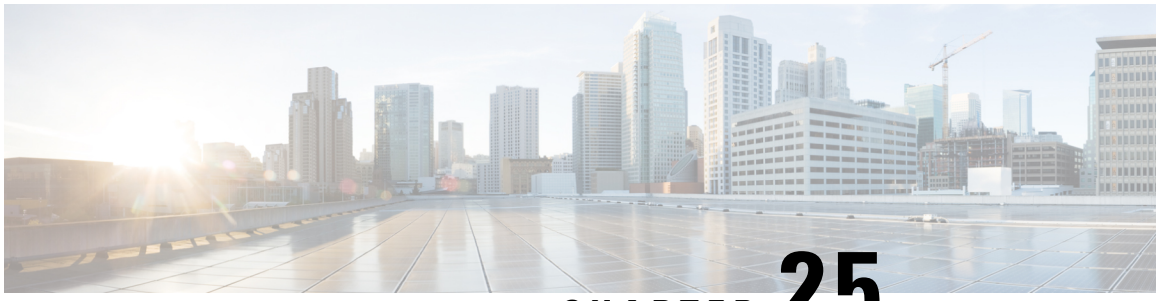
The following example shows the configuration to override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class hex aabbcc
    !


interface GigabitEthernet 0/0/0
```

```
    ipv6 address dhcp
    ipv6 dhcp client vendor-class ascii cisco
    !
```

The following example shows the configuration to disable option-16 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class disable
    !
```



CHAPTER 25

# IP DHCP Smart-Relay

*Table 221: Feature History*

| Feature Name | Release Information | Feature Description |
|---|---|---|
| IP DHCP Smart-Relay | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a<br><br>Cisco Catalyst SD-WAN Manager Release 20.13.1 | With this feature, you can set the gateway address to the secondary IP address using the DHCP relay agent, when there is no IP address and DHCP service information from the DHCP server. A DHCP relay agent is any host or IP router that forwards DHCP packets between clients and servers.<br><br>This functionality is useful when the DHCP server cannot be configured to use secondary pools. |


- Information About the IP DHCP Smart-Relay, on page 815
- Prerequisites for IP DHCP Smart-Relay, on page 816
- Configure IP DHCP Smart-Relay Agent Using a CLI Template, on page 816


# Information About the IP DHCP Smart-Relay

A Dynamic Host Configuration Protocol (DHCP) relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay-agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks transparently. Relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway IP address and, if configured, adds the relay agent information option (option 82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

The Cisco IOS XE DHCP relay agent supports the use of unnumbered interfaces. An unnumbered interface can borrow the IP address of another interface already configured on the router, which conserves network and address space. For DHCP clients connected though the unnumbered interfaces, the DHCP relay agent automatically adds a static host route once the DHCP client obtains an address, specifying the unnumbered interface as the outbound interface. The route is automatically removed once the lease time expires or when the client releases the address.

# Benefits of IP DHCP Smart-Relay

- Using automatic IP address assignment at each remote site substantially reduces the internet access cost. Static IP addresses are considerably more expensive to purchase than are automatically allocated IP addresses.
- Enables easier configuration and minimizes operational overhead and costs associated with device configuration tasks and eases deployment by nontechnical users.
- DHCP server maintains configurations for several subnets. An administrator only needs to update a single, central server when configuration parameters change.

# Prerequisites for IP DHCP Smart-Relay

- To configure the IP DHCP smart-relay feature, configure the IP helper address on desired interfaces using **ip helper-address** command. You can use the **service dhcp** command to enable the DHCP service and **no service dhcp** command, if the service is disabled depending on the requirement.
- The Cisco DHCP relay agent is enabled on an interface only when the **ip helper-address** command is configured. This command enables the DHCP broadcast to be forwarded to the configured DHCP server.

# Configure IP DHCP Smart-Relay Agent Using a CLI Template

To forward UDP broadcasts to the DHCP server, configure helper addresses on the interface. If you have configured the secondary addresses on that interface and you want the router to step through each IP network when forwarding DHCP requests, use the **ip dhcp smart-relay** command. If smart relay agent forwarding is not configured, all requests are forwarded using the primary IP address on the interface. If smart relay agent forwarding is not configured, all requests are forwarded using only the primary IP address on the interface.

If the **ip dhcp smart-relay** command is configured, the relay agent counts the number of times that the client retries sending a request to the DHCP server when there is no DHCPOFFER message from the DHCP server. After three retries, the relay agent sets the gateway address to the secondary address. If the DHCP server still does not respond after three more retries, then the next secondary address is used as the gateway address.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

1. Enter SD-WAN configuration mode.

   ```
   sdwan
   ```

2. Enable DHCP server.

   ```
   service dhcp
   ```

3. In the SD-WAN configuration mode, configure an interface type such as, Gigabit Ethernet.

   ```
   interface Gigabitethernet0/0
   ```

4. Enable the DHCP broadcast to be forwarded to the configured DHCP server.

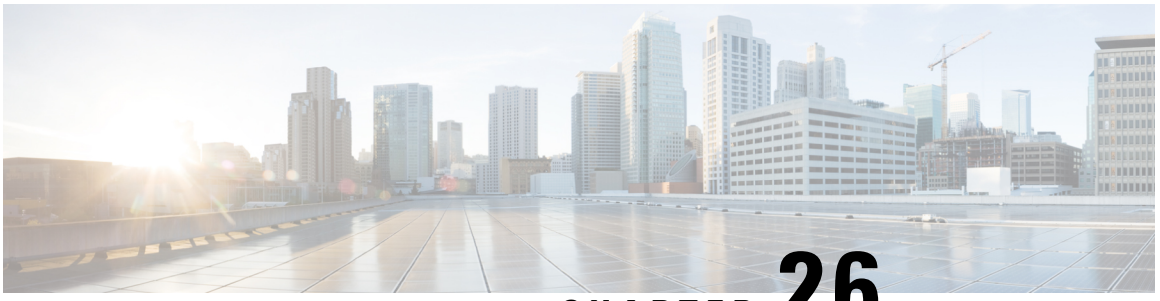
   ```
   ip helper-address
   ```

5. Configure the DHCP relay agent to switch the gateway address to a secondary address when there is no DHCPOFFER message from a DHCP server.

```
ip dhcp smart-relay
```

The following is a DHCP smart-relay CLI configuration. In the following example, the device forwards the DHCP broadcast received on Gigabitethernet interface 0/0 to the DHCP server (10.0.0.1), by inserting 192.168.255.254 in the gateway address field of the DHCP packet.

```
service dhcp
ip address 172.16.0.1 255.255.0.0
secondary ip address 192.168.255.254 255.255.0.0

interface GigabitEthernet0/0
ip helper-address 10.0.0.1
ip dhcp smart-relay
end
```



CHAPTER 26

# IPv6 Functionality

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

This chapter describes the options for enabling IPv6 functionality for Cisco Catalyst SD-WAN templates and policies. Use the information in this chapter if your deployment uses IPv6.

### Configure IPv6 Functionality for an Interface or Subinterface Template

To configure IPv6 functionality for an interface or subinterface template, perform the following steps.

Cisco Catalyst SD-WAN supports dual stack: you can configure IPv4 and IPv6 in the same deployment. You can configure up to three global IPv6 addresses per interface.

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

3. Select **Cisco VPN Interface Ethernet** from the list of templates.
4. From **Basic Configuration**, click **IPv6** and configure the parameters that the following table describes:

| Parameter Name | Description |
|---|---|
| Static | This radio button is selected by default because IPv6 addresses are static. |
| IPv6 Address | Enter the IPv6 address of the interface or subinterface. |

*CLI equivalent:*

```
interface GigabitEthernet1
  no shutdown
  ipv6 address 2001:DB8:1::1/64
  ipv6 enable
```

### Configure IPv6 Functionality for an OMP Template

To configure IPv6 functionality for an Overlay Management Protocol (OMP) template, follow these steps:

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

3. Select **Cisco OMP** from the list of templates.
4. Click **Advertise** and choose **IPv6** to configure the parameters that the following table describes:

| Parameter Name | Description |
|---|---|
| Connected | Click **Off** to disable advertising connected routes to OMP.<br>By default, connected routes are advertised to OMP. |
| Static | Click **Off** to disable advertising static routes to OMP.<br>By default static routes are advertised to OMP. |
| BGP | Click **On** to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP. |

*CLI equivalent:*

First enable Service VRF for IPv6:

```
config-transaction
vrf definition 1
  rd 1:1
  address-family ipv6
```

Next enable OMP.

OMP supports global IPv6 configuration. In addition, per VRF level configuration is allowed. Per VRF level configuration overrides global configuration.

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    advertise static
```

Global configuration is the default configuration, so IPv6 is enabled by default for OMP. To disable IPv6 OMP route redistribution for a particular VRF, configure the redistribution protocol to no as follows:

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    no advertise connected
    no advertise static
    no advertise bgp
```

### Configure IPv6 Functionality for a BGP Template

To configure IPv6 functionality for a Border Gateway Protocol (BGP) template, follow these steps:

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

3. Select **Cisco BGP** from the list of templates.
4. Click **Unicast Address Family** and choose **IPv6** to configure the parameters that the following table describes:

| Tab | Parameter Name | Description |
|---|---|---|
| | Maximum Paths | Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing.*Range:* 0 to 32 |
| | Address Family | Enter the BGP IPv6 unicast address family. |
| RE-DISTRIBUTE | | Click the **Redistribute** tab, and then click **Add New Redistribute**. |
| | Protocol | Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are Connected, NAT, OMP, OSPF, and Static. At a minimum, select the following:<br>• For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP.<br>• For transport-side BGP routing, select Connected, and then under Route Policy, specify a route policy that has BGP advertise the loopback interface address to its neighbors. |
| | Route Policy | Enter the name of the route policy to apply to redistributed routes. |
| | | Click **Add** to save the redistribution information. |

| Tab | Parameter Name | Description |
|---|---|---|
| NETWORK | | Click the **Network** tab, and then click **Add New Network**. |
| | Network Prefix | Enter a network prefix, in the format of *prefix*/*length*, to be advertised by BGP. |
| | | Click **Add** to save the network prefix. |
| AGGREGATE ADDRESS | | Click the **Aggregate Address** tab, and then click **Add New Aggregate Address**. |
| | Aggregate Prefix | Enter the prefix of the addresses to aggregate for all BGP sessions, in the format prefix/length. |
| | AS Set Path | Click **On** to generate set path information for the aggregated prefixes. |
| | Summary Only | Click **On** to filter out more specific routes from BGP updates. |
| | | Click **Add** to save the aggregate address. |

1. In the Neighbor area, click **IPv6**, create a new neighbor or edit an existing one, and then configure the parameters that the following table describes.

Parameters marked with an asterisk are required.

| Parameter Name | Description |
|---|---|
| IPv6 Address* | Specify the IPv6 address of the BGP neighbor. |
| Description | Enter a description of the BGP neighbor. |
| Remote AS* | Enter the AS number of the remote BGP peer. |
| Address Family | Select **Global** from the drop-down list, click **On** and select the address family. Enter the address family information. |
| Shutdown | To shut down a BGP neighbor when you push the template, select **Global** from the drop-down list and then click **Yes**.*Default:* Off |

*CLI equivalent:*

```
config-transaction
router bgp 1
 bgp log-neighbor-changes
  address-family ipv6 unicast vrf 1
  neighbor 2001:DB8:19::1 remote-as 2
  neighbor 2001:DB8:19::1 activate
  neighbor 2001:DB8:19::1 advertisement-interval 1
  neighbor 2001:DB8:19::1 password cisco
  redistribute omp
  redistribute static
  exit-address-family
```

### Configure IPv6 Functionality for a VRRP Template

To configure IPv6 functionality for a Virtual Router Redundancy Protocol (VRRP) template, follow these steps:

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

3. Select **Cisco VPN Interface Ethernet** from the list of templates.
4. Click **VRRP** and choose **IPv6**.
5. Click **New VRRP**.
6. Configure the parameters that the following table describes:

| Parameter Name | Description |
|---|---|
| Group ID | Enter a virtual router ID, which represents a group of routers.<br>Range:<br>1 through 255 |
| Priority | Enter the priority level of the router within a VRRP group.<br>• *Range:* 1 through 254<br>• *Default:* 100 |
| Timer | Not used. |
| Track OMP | Select **On** to track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router.*Default:* Off |
| Track Prefix List | Enter a value to track a list of IPv6 remote prefixes. This value is an alphanumeric string that is configured under Policy. |
| Link Local IPv6 Address | Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8. |
| Global IPv6 Address | Enter a virtual global unicast IPv6 address, which represents the global address of the group. The address should be an IPv6 global prefix address that has the same mask as the interface forwarding address on which the VRRP group is configured. For example, 2001::2/124.<br>You can configure up to 3 global IPv6 addresses. |

*CLI equivalent:*

```
config-transaction
interface GigabitEthernet1

 vrrp 10 address-family ipv6
   priority 20
   track omp shutdown
   address FE80::10:100:1 primary
   address 2001:10:100::1/64

Prefix-list tracking
track 1 ipv6 route 1:1::1/128
 reachability
 ipv6 vrf 1

 track 2 ipv6 route 2:2::2/128
 reachability
 ipv6 vrf 2

 track 20 list boolean or
  object 1
  object 2

vrrp 10 address-family ipv6
  track 20 shutdown
```

### Configure IPv6 Functionality for an SNMP Template

To configure IPv6 functionality for an SNMP template, follow these steps:

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

3. Click **Cisco SNMP** from the list of templates.
4. Choose **SNMP Version** > **TRAP TARGET SERVER** and create or edit an SNMP trap target.
5. Configure the parameters that the following table describes:

| Parameter Name | Description |
|---|---|
| VPN ID | Enter the number of the VPN to use to reach the trap server. Range: 0 through 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 though 65535. |
| Trap Group Name | Select the name of a trap group that was configured under the Group tab. |
| User Name | Select the name of a community that was configured under the Community tab. |
| Source Interface | Enter the interface to use to send traps to the SNMP server that is receiving the trap information. |

**Note** Make sure that you have already configured the SNMP community and trap target group.

*CLI equivalent:*

The following example permits any SNMP to access all objects with read-only permission using the community string named public. The device also will send Border Gateway Protocol(BGP) traps IPv6 host 3ffe:b00:c18:1::3/127 using SNMP v1.The community string named public will be sent with the traps.

```
Device# config-transaction
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

In the following example, the SNMP context A is associated with the views in SNMPv2c group GROUP1 and the IPv6 named access list public2:

```
Device# config-transaction
Device(config)# snmp-server context A
Device(config)# snmp mib community-map commA context A target-list comm AVpn
Device(config)# snmp mib target list commAVpn vrf CustomerA
Device(config)# snmp-server view viewA ciscoPingMIB included
Device(config)# snmp-server view viewA ipForward included
Device(config)# snmp-server group GROUP1 v2c contextA read viewA write viewA notify access
 ipv6 public2
```

The following example configures the IPv6 host as the notification server:

```
Device> enable
Device# config-transaction
Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Device(config)# snmp-server group publicv2c access ipv6 public2
Device(config)# snmp-server hosthost1.com2c vrf trap-vrf mgr
Device(config)# snmp-server user user1 bldg1 remote3ffe:b00:c18:1::3/127 v2c access ipv6
public2
Device(config)# snmp-server enable traps bgp
Device(config)# exit
```

### Configure IPv6 Functionality for a DHCP Relay Agent Template

To configure IPv6 functionality for a DHCP Relay Agent template, follow these steps:

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

3. Select **Cisco VPN Interface Ethernet** from the list of templates.
4. From **Basic Configuration**, click **IPv6**.
5. Click **Add** next to **DHCP Helper**.

6. Configure the parameters that the following table describes.

*Table 222:*

| Parameter Name | Description |
|---|---|
| DHCPv6 Helper # | IP address of the DHCP helper |
| DHCPv6 Helper VPN | VPN ID of the VPN source interface for the DHCP helper. |

*CLI equivalent:*

```
device-configuration
interface GigabitEthernet8
 vrf forwarding 2
 no ip address
 ipv6 address 2001:A14:99::F/64
 ipv6 dhcp relay destination vrf 1 2001:A14:19::12 GigabitEthernet2
```

### Configure IPv6 Functionality for an ACL Template or a QoS Template

To configure IPv6 functionality for an ACL and QoS template, follow these steps:

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

3. Select **Cisco VPN Interface Ethernet** from the list of templates.
4. From **ACL/QoS**, configure the parameters that the following table describes:

| Parameter Name | Description |
|---|---|
| Ingress ACL – IPv6 | Click **On** to enable the IPv6 ingress access list. |
| IPv6 Ingress Access List | Enter the name of the IPv6 ingress access list. |
| Egress ACL – IPv6 | Click **On** to enable the IPv6 egress access list. |
| IPv6 Egress Access List | Enter the name of the IPv6 egress access list. |

*CLI Equivalent for Configuring IPv6 Functionality for an ACL Template:*

```
Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)#    sequence 11
Device(config-sequence-11)#     match
Device(config-match)#       source-ip 2001:380:1::64/128
Device(config-match)#      destination-ip 2001:3c0:1::64/128
Device(config-match)#      source-port      4000
```

```
Device(config-match)#      destination-port 3000
Device(config-match)#      traffic-class    6
Device(config-match)#      next-header      6
Device(config-match)#      packet-length    1000
Device(config-match)#     action accept
Device(config-action)#

Device(config)# sdwan interface GigabitEthernet6 ipv6 access-list ipv6_acl in
Device(config-interface-GigabitEthernet6)#
Device(config-interface-GigabitEthernet6)#

Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64

Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv_ipv6_prefix
Device(config-access-list-ipv_ipv6_prefix)# sequence 11
Device(config-sequence-11)#     match
Device(config-match)#       source-data-prefix-list data-ipv6-prefix-list
Device(config-match)#       destination-data-prefix-list source_ipv6_list
Device(config-match)#      destination-ip 2001:3c0:1::64/128
Device(config-match)#      source-port      4000
Device(config-match)#      destination-port 3000
Device(config-match)#      traffic-class    6
Device(config-match)#      next-header      6
Device(config-match)#      packet-length    1000
Device(config-match)#     !
Device(config-match)#     action accept
```

*CLI Equivalent for Configuring IPv6 Functionality for a QoS Template:*

```
Device(config)# class-map match-any class0
Device(config-cmap)#  match qos-group 0
Device(config-cmap)# class-map match-any class1
Device(config-cmap)#  match qos-group 1
Device(config-cmap)# !
Device(config-cmap)# policy-map qos_map_for_data_policy
Device(config-pmap)#  class class0
Device(config-pmap-c)#   bandwidth percent 10
Device(config-pmap-c)#   random-detect
Device(config-pmap-c)#  class class1
Device(config-pmap-c)#   bandwidth percent 10
Device(config-pmap-c)#   random-detect
Device(config-pmap-c)#
Device(config-pmap-c)# policy
Device(config-policy)#  no app-visibility
Device(config-policy)#  class-map
Device(config-class-map)#   class class0 queue 0
Device(config-class-map)#   class class1 queue 1
Device(config-class-map)# !
Device(config-class-map)#  ipv6
Device(config-ipv6)#   access-list fwd_class_data_policy
Device(config-access-list-fwd_class_data_policy)#    sequence 5
Device(config-sequence-5)#     match
Device(config-match)#      traffic-class 0
Device(config-match)#     !
Device(config-match)#     action accept
Device(config-action)#      count fwd_class_data_policycnt_5
Device(config-action)#      class class0
Device(config-action)#     !
Device(config-action)#    !
Device(config-action)#    sequence 6
Device(config-sequence-6)#     match
Device(config-match)#      traffic-class 1
```

```
Device(config-match)#     !
Device(config-match)#     action accept
Device(config-action)#      count fwd_class_data_policycnt_6
Device(config-action)#      class class1
Device(config-action)#     !
Device(config-action)#    !
Device(config-action)#    !
Device(config-action)#    default-action drop

class-map match-any class0
match qos-group 0
class-map match-any class1
match qos-group 1
!
policy-map qos_map_for_data_policy
class class0
  bandwidth percent 10
  random-detect
class class1
  bandwidth percent 10
  random-detect

policy
no app-visibility
class-map
  class class0 queue 0
  class class1 queue 1
!
ipv6
  access-list fwd_class_data_policy
   sequence 5
    match
     traffic-class 0
    !
    action accept
     count fwd_class_data_policycnt_5
     class class0
    !
   sequence 6
    match
     traffic-class 1
    !
    action accept
     count fwd_class_data_policycnt_6
     class class1
!
default-action drop
```

### Configure IPv6 Functionality for a Logging Template

To configure IPv6 functionality for a Logging template, follow these steps:

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

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

3. Select **Cisco Logging** from the list of templates.

4. From **Server**, click **IPv6**.
5. Configure the parameters that the following table describes.

| Parameter Name | Description |
|---|---|
| IPv6 Hostname/IPv6 Address | Host name or IP address of the server to direct the logging information. |
| VPN ID | VPN ID of the VPN source interface. |
| Source Interface | Name of the source interface. |
| Priority | Choose the maximum severity of messages that are logged. |

*CLI equivalent:*

```
config-transaction
Device(config)# logging host ipv6
AAAA:BBBB:CCCC:DDDD::FFFF
```

**Note** Creating and deleting the logging host configurations in same transaction causes unexpected behaviour. For example, deleting **logging host** *ipv6-address* and creating **logging host** *ipv6-address* **vrf** *vrf-name* configuration in same transaction causes both configurations to disappear from the device. We recommend you to send the two requests in separate transactions.

### Configure IPv6 Functionality for a New Prefix List

To configure an IPv6 address for a new prefix list, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. From the **Custom Options** drop-down list, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Prefix** from the list on the left and then select **New Prefix List**.
4. Click **IPv6** and enter the IPv6 address in **Add Prefix**.

*CLI equivalent:*

```
config-transaction
Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)#  sequence 11
Device(config-sequence-11)#  match
Device(config-match)# source-ip 2001:380:1::64/128
Device(config-match)# destination-ip 2001:3c0:1::64/128
```

### Configure IPv6 Functionality for a Data Prefix

To configure an IPv6 address for a new prefix list, follow these steps:

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

2. From the Custom Options drop-down list, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Data Prefix** from the list on the left and then select **New Data Prefix List**.
4. From **Internet Protocol**, click **IPv6** and enter the IPv6 address in **Add Prefix**.

*CLI equivalent:*

```
Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64
```

### Configure IPv6 Functionality for a Centralized Policy

To configure a centralized policy to apply to IPv6 address families, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. From the Custom Options drop-down menu, select **Traffic Policy** under Centralized Policy.
3. Select **Traffic Data**.
4. Select **Add Policy** and click **Create New**.
5. Click **Sequence Type** and then select **Traffic Engineering**.
6. Click **Sequence Rule**.
7. From the **Protocol** drop-down list, select **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.
8. Click **Sequence Type** and then select **QoS**.
9. Click **Sequence Rule**.
10. From the Protocol drop-down list, click **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.

*CLI equivalent:*

```
config-transaction
(config)# policy
(config-policy)# lists ipv6-prefix-list foo ipv6-prefix 1::1/64
                 ipv6-prefix-list ipv6-1
                 ipv6-prefix 1::1/128
```

### Configure IPv6 Functionality for a Localized Policy

To configure a localized policy to apply to IPv6 address families, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. From the **Custom Options** drop-down list, select **Access Control Lists** under Localized Policy.
3. Click **Add Access Control List Policy** and choose **Add IPv6 ACL Policy**. The policy you create will apply only to IPv6 address families.

*CLI equivalent:*

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
config-transaction
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```


- DHCP for IPv6, on page 831
- IPv6 as Preferred Address Family in a Dual Stack Environment, on page 841
- Information About IPv6 as Preferred Address Family in a Dual Stack Environment, on page 842
- Benefits of IPv6 as Preferred Address Family in a Dual Stack Environment, on page 842
- Use Cases for IPv6 as Preferred Address Family in a Dual Stack Environment, on page 843
- Configure IPv6 as Preferred Address Family in a Dual Stack Environment, on page 843
- Configure IPv6 as Preferred Address Family in a Dual Stack Environment Using a CLI Template, on page 846
- Monitor IPv6 as Preferred Address Family in a Dual Stack Environment, on page 847
- Monitor IPv6 as Preferred Address Family in a Dual Stack Environment Using the CLI , on page 847
- Troubleshooting , on page 848
- Configuration Example for IPv6 as Preferred Address Family in a Dual Stack Environment, on page 848


# DHCP for IPv6

*Table 223: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| DHCP for IPv6 | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a<br><br>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.<br><br>Assigning of IPv6 addresses is accomplished using SLAAC, DHCPv6, DHCPv6 Prefix Delegation, or DHCPv6 Relay.<br><br>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. |

## Prerequisites for DHCPv6

- Basic IPv6 connectivity for assigning IPv6 addresses to hosts connected to the Cisco IOS XE Catalyst SD-WAN devices.

## Restrictions For DHCPv6

- This feature is supported only through CLI configuration.

- A unique DHCPv6 pool name must be provied for each VRF.

# Information About DHCPv6

You can configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to assign addresses on an IPv6-enabled network. Alternatively, you can also configure Stateless Address Autoconfiguration (SLAAC) to assign addresses on an IPv6-enabled network.

### SLAAC

The most common method for IPv6 client address assignment is SLAAC. SLAAC provides simple plug-and-play connectivity where hosts self-assign an address based on the IPv6 prefix.

SLAAC is configured as follows:

- Host sends a router solicitation message.
- Hosts waits for a Router Advertisement (RA) message.
- Hosts take the first 64 bits of the IPv6 prefix from the RAmessage and combines it with the 64 bit EUI-64 address (in the case of ethernet, this is created from the MAC Address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the RA message, as its default gateway.
- Duplicate Address Detection (DAD) is performed by IPv6 clients in order to ensure that random addresses that are picked do not collide with other clients.
- The choice of algorithm is up to the client and is often configurable.

The last 64 bits of the IP v6 address can be learned based on the following 2 algorithms:

- EUI-64 which is based on the MAC address of the interface, or
- Private addresses that are randomly generated.

### SLAAC and DHCPv6

#### DHCPv6

IPv6 devices use multicast to acquire IP addresses and to find DHCPv6 servers. The basic DHCPv6 client-server concept is similar to DHCP for IPv4. If a client wants to receive configuration parameters, it sends out a request on the attached local network to detect available DHCPv6 servers. The server responds with the requested information in a Reply message.

The DHCPv6 client knows whether to use DHCPv6 based upon the instruction from a router on its link-local network. The default gateway has two configurable bits in its RA available for this purpose:

- O bit—When this bit is set, the client can use DHCPv6 to retrieve other configuration parameters (for example, TFTP server addressor DNS server address ) but not the client's IP address.
- M bit—When this bit is set, the client can use DHCPv6 to retrieve a managed IPv6 address and other configuration parameters from a DHCPv6 server.

#### Stateless DHCP

Stateless DHCPv6 is a combination of SLAAC and DHCPv6. With this option SLAAC is still used to retrieve an IP address while DHCP is used to obtain additional information such as TFTP server addressor, DNS server

address. In this case, the device sends an RA with the O bit set but does not set the M bit. This is known as Stateless DHCPv6 because the DHCPv6 server does not have to track the client address bindings.

#### Stateful DHCP

Stateful DCHPv6 functions exactly the same as DHCP IPv4 in which hosts receive both their IPv6 address and additional parameters from the DHCP server. When a device sends an RA with the M bit set, this indicates that clients must use DHCP to obtain their IP addresses. When the M bit is set, the setting of the O bit is irrelevant because the DHCP server also returns other configuration information together with the addresses. This is known as Stateful DHCPv6 because the DHCPv6 server tracks the client address bindings.

#### DHCPv6 Prefix Delegation

The DHCPv6 prefix delegation feature is a stateful mode of operation for simple delegation of prefixes from a delegating edge device (DHCP server) to requesting edge device (DHCP clients).

DHCPv6 prefix delegation feature is ideal for the following situations where:

- A delegating edge device that does not have the information about the topology of the networks to which the requesting edge device is attached to.
- A delegating edge device does not require other information apart from the identity of the requesting edge device to choose a prefix for delegation. This mechanism is appropriate for use by an ISP to delegate a prefix to a subscriber. After the ISP has delegated prefixes to a subscriber, the subscriber may further subnet and assign prefixes to the links within the subscriber's network.

#### DHCPv6 Relay

A DHCPv6 relay agent is an edge device, residing on the client's network, is used to relay messages between the client and the server when a DHCPv6 server is not in the same network as the DHCPv6 clients.

## Benefits of DHCPv6

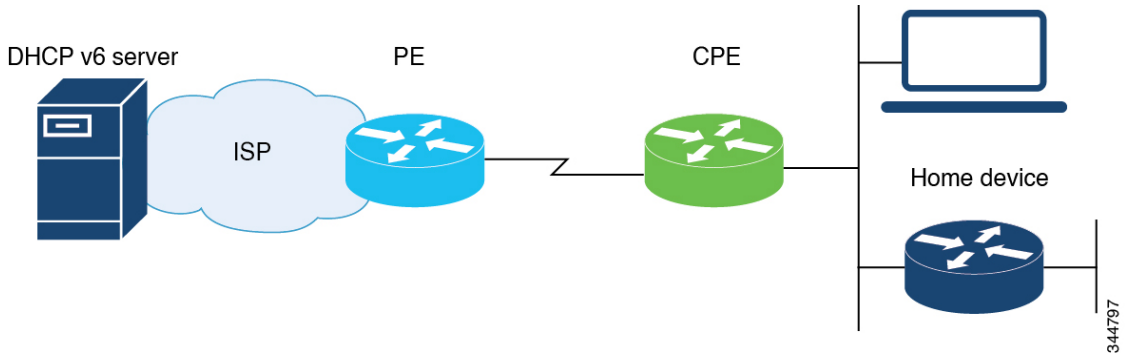
Configuring DHCP for IPv6 allows you to have more IP address compared to IPv4. With IPv6, there can be no depletion of IP addresses.

## Use Cases For DHCPv6

Cisco IOS XE Catalyst SD-WAN devices can be configured for DHCPv6 as a server, client, or a relay agent. As a server, a Cisco IOS XE Catalyst SD-WAN device can be configured for SLAAC, Stateless DHCP or for prefix delegation.

#### SLAAC with DHCP

The figure below shows a typical broadband deployment.



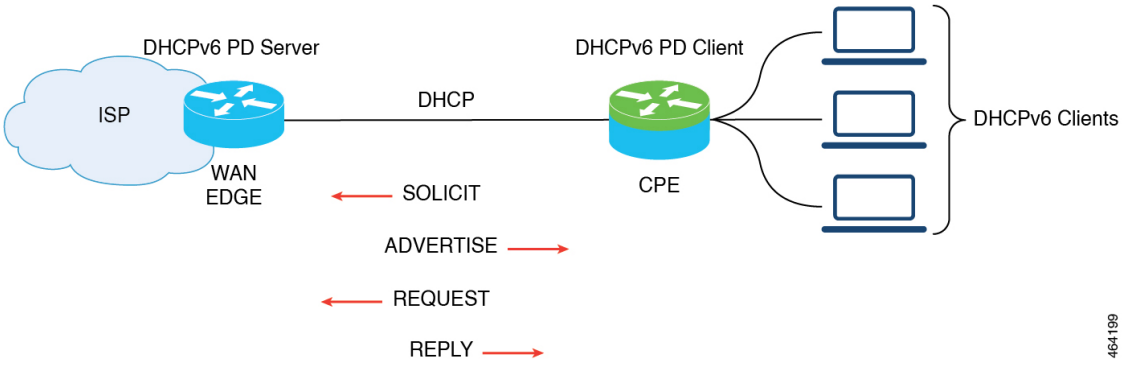

A Cisco IOS XE Catalyst SD-WAN device deployed on a customer premises (CPE) and connected to a ISP edge (PE) device can be a stateless or stateful DHCPv6 client. In either case, the ISP-side DHCPv6 server might provide configuration parameters such as Domain Name System (DNS) server addresses, domain names, and Simple Network Time Protocol (SNTP) servers to the DHCP client on the CPE. Such information can be specific to ISPs.

In addition to being a DHCPv6 client (toward the ISP), the CPE can act as a DHCPv6 server to the home network. For example, neighbor discovery followed by a stateless or stateful DHCPv6 client can occur on the link between the CPE and the home devices. In some cases, the information to be provided to the home network is the same as that obtained from the ISP-side DHCPv6 server. Therefore, the DHCPv6 component on the CPE allows automatic importing of configuration parameters from the DHCPv6 client to the DHCPv6 server pool.

### DHCPv6 Prefix Delegation

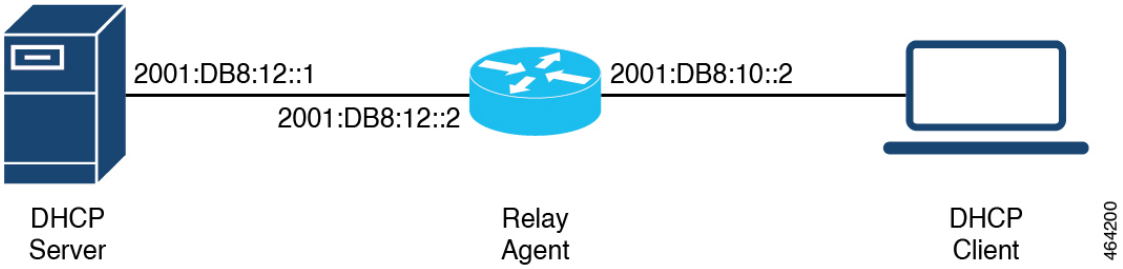
The model of operation for prefix delegation is as follows. In this sample topology, an edge device is configured as a DHCP server which is provisioned with prefixes to be delegated to a DHCP client. A Cisco IOS XE Catalyst SD-WAN device is configured as a DHCP client and requests prefix(es) from the server. The server chooses prefix(es) for delegation and responds with prefix(es) to the DHCP client. The DHCP client is then responsible for the delegated prefix(es).

For example, the client might assign a subnet from a delegated prefix to one of its interfaces and begin sending Router Advertisements for the prefix on that link. Each prefix has an associated preferred lifetime and valid lifetime, which constitute an agreement about the length of time over which the client is allowed to use the prefix. A client can request an extension of the lifetimes on a delegated prefix and is required to terminate the use of a delegated prefix if the valid lifetime of the prefix expires.



### DHCPv6 Relay

In this sample topology, the DHCP server is not in the same network as DHCP client. A Cisco IOS XE Catalyst SD-WAN device residing on the client's network acts as a relay agent to relay messages between the client and the server.




# Configure DHCPv6

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 SLAAC

This example shows how to configure SLAAC on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
```

```
device(config-if)# ipv6 enable
device(config-if)# end
```

This example shows how to configure SLAAC on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

# Configure SLAAC and DHCPv6 Pool for Options

This example shows how to configure SLAAC and DHCPv6 pool on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

This example shows how to configure SLAAC and DHCPv6 pool on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd other-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

# Configure DHCPv6 (stateful) Address Assignment

This example shows how to configure DHCPv6 address assignment on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

This example shows how to configure DHCPv6 address assignment on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
```

```
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# address prefix 2010:AB8:0:1::1/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

# Configure DHCPv6 with Prefix Delegation (stateful)

This example shows how to configure DHCPv6 with prefix delegation on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client pd prefix_from_provider
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

This example shows how to configure DHCPv6 with prefix delegation on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 nd ra interval 20
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool1 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
device(config)# ipv6 local pool dhcpv6-pool1 2001:DB8:1200::/40 48
```

# Configure DHCPv6 with Relay

This example shows how to configure DHCPv6 with relay on the client side.

```
device(config)# interface GigabitEthernet3
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp client pd pr-from-pd
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# no mop enabled
```

```
device(config-if)# no mop sysid
device(config-if)# end
```

This example shows the configurations on the client facing WAN edge device that acts as the relay agent.

```
device(config)# interface TenGigabitEthernet0/0/5
device(config-if)# vrf forwarding 10
device(config-if)# load-interval 30
device(config-if)# ipv6 address 2001:BB:1000::10/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp relay destination 2001:BB8:1200::2
device(config-if)# ipv6 dhcp relay option vpn
device(config-if)# end
```

This example shows the configurations on the server facing WAN edge device.

```
device(config)# interface GigabitEthernet0/0/3
device(config-if)# vrf forwarding 10
device(config-if)# no ip address
device(config-if)# negotiation auto
device(config-if)# ipv6 address 2001:BB8:1200::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

This example shows how to configure DHCPv6 with relay on the server side.

```
device(config)# interface GigabitEthernet2
device(config-if)# ipv6 address 2001:BB8:1200::2/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool10 lifetime infinite infinite
device(config-dhcpv6)# address prefix 2001:BB:1000::/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:BB:1200::42
device(config-dhcpv6)# domain-name relay.com
device(config)# ipv6 local pool dhcpv6-pool10 8001:ABCD::/40 48
```

# Verify DHCPv6 Client and Server Configuration

### Verify DHCPv6 Interface Information

The following is a sample output from the **show ipv6 dhcp interface** command that provides details about DHCPv6 address allocation.

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 00:01:09
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x00080001, T1 100, T2 160
        Address: 2010:AB8:0:1:95D1:CFC:F227:23FB/128
                preferred lifetime 200, valid lifetime 200
                expires at Oct 26 2021 07:28 AM (170 seconds)
```

```
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

The following is a sample output from the **show ipv6 dhcp interface** command that provides details about DHCPv6 prefix delegation.

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:01:34
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00080001, T1 100, T2 160
        Prefix: 2001:DB8:1202::/48
                preferred lifetime 200, valid lifetime 200
                expires at Oct 26 2021 07:30 AM (194 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
  Prefix name: prefix_from_server
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

The following is a sample output from the **show ipv6 dhcp interface** command that provides details about SLAAC with DHCP.

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE (0)
  Information refresh timer expires in 23:59:49
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

### View DHCPv6 Pool Information

The following is a sample output from the **show ipv6 dhcp pool** command that provides details about DHCPv6 address allocation.

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (1 in use,
0 conflicts)
```

```
              preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

The following is a sample output from the **show ipv6 dhcp pool** command that provides details about DHCPv6 prefix delegation.

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (0 in use,
0 conflicts)
              preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

### View DHCPv6 Bindings

The following is a sample output from the **show ipv6 dhcp binding** command that provides details about DHCPv6 address allocation.

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  IA NA: IA ID 0x00080001, T1 10000, T2 16000
    Address: 5001:DB8:1234:42:500C:B3FA:54A7:F63D
             preferred lifetime 20000, valid lifetime 20000
             expires at Oct 26 2021 01:17 PM (19925 seconds)
```

The following is a sample output from the **show ipv6 dhcp binding** command that provides details about DHCPv6 prefix delegation.

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  Interface : GigabitEthernet0/0/3
  IA PD: IA ID 0x00080001, T1 100, T2 160
    Prefix: 2001:BB8:1602::/48
             preferred lifetime 200, valid lifetime 200
             expires at Oct 26 2021 08:01 AM (173 seconds)
```

### View DHCPv6 Database

The following is a sample output from the **show ipv6 dhcp database** command.

```
Device# show ipv6 dhcp database
Database agent bootflash:
  write delay: 300 seconds, transfer timeout: 300 seconds
  last written at Oct 26 2021 08:01 AM, write timer expires in 250 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2
  failed write times 0
```

### View DHCPv6 Relay Bindings

The following is a sample output from the **show ipv6 dhcp relay bindings** command that provides details about DHCPv6 relay.

```
Device# show ipv6 dhcp relay binding

Relay Bindings associated with default vrf:

Relay Bindings associated with vrf 10:
Prefix: 2001:AA8:1100::/48 (GigabitEthernet3)
  DUID: 00030001001E49674C00
  IAID: 851969
  lifetime: INFINITE
  expiration: INFINITE
Summary:
  Total number of Relay bindings = 1
  Total number of IAPD bindings = 1
  Total number of IANA bindings = 0
  Total number of Relay bindings added by Bulk lease = 0
```

# IPv6 as Preferred Address Family in a Dual Stack Environment

*Table 224: 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<br>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.<br>For Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller, configure IPv6 as the preferred address family by using the feature template or the CLI template. For Cisco IOS XE Catalyst SD-WAN devices, configure IPv6 as the preferred address family using the Configuration Groups, Quick Connect or a CLI template. |

# Information About IPv6 as Preferred Address Family in a Dual Stack Environment

Cisco Catalyst SD-WAN provides you the option to select a preferred address family—IPv4 or IPv6—to establish control and data connections in a dual stack network environment. Use the **Dual Stack IPv6 Default** drop-down list in Cisco SD-WAN Manager to set IPv6 or IPv4.

On a Cisco IOS XE Catalyst SD-WAN device, when you choose the **True** option from the **Dual Stack IPv6 Default** drop-down list, the device establishes an IPv6 control connection with Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller it is connected to. When you choose the **False** option from the **Dual Stack IPv6 Default** drop-down list, an IPv4 connection is established to connect to Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller.

Data connections or Bidirectional Forwarding Detection (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.

When you choose the **True** option from the **Dual Stack IPv6 Default** drop-down list in Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Controller, IPv6 connections to other Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller instances are established. When you choose the **False** option from the **Dual Stack IPv6 Default** drop-down list, an IPv4 connection is established.

**Note**

- The connections from Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller and Cisco IOS XE Catalyst SD-WAN devices to the Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual stack network environment whether the **Dual Stack IPv6 Default** drop-down list options set to **True** or **False.**
- The **Dual Stack IPv6 Default** drop-down list options applies to Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller, and not to Cisco Catalyst SD-WAN Validator.
- An IPv6 connection can be configured on Cisco IOS XE Catalyst SD-WAN devices in sites that are behind NAT44 and NAT66.

# Benefits of IPv6 as Preferred Address Family in a Dual Stack Environment

You have the option to migrate from IPv4 to IPv6, which allows you to have more IP addresses compared to IPv4. With IPv6, there can be no depletion of IP addresses.

# Use Cases for IPv6 as Preferred Address Family in a Dual Stack Environment

From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco Catalyst SD-WAN Control Components Release 20.10.1—to migrate from IPv4 to IPv6, you have the option to select a default connectivity option—IPv4 or IPv6—for control connections and data connections.

# 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.

## 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 IPv6 as Preferred Address Family in a Dual Stack Environment Using a CLI Template

### Configure Cisco IOS-XE SD-WAN Devices for IPv6 in Dual IP Stack Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

This section provides sample CLI configurations of IPv6 as the preferred address family in Cisco IOS XE Catalyst SD-WAN devices:

1. Enable IPv6 on the tunnel interface:

```
interface tunnel1
no shutdown
ipv6 enable
```

2. Enable IPv6:

```
system
ipv6-strict-control true
```

The following example shows how to configure IPv6 as the preferred address family in Cisco IOS XE Catalyst SD-WAN devices.

```
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 tunnel source GigabitEthernet1
 tunnel mode sdwan
 ipv6 enable
exit

system
gps-location latitude 32.0
gps-location longitude -100.0
system-ip 10.16.255.14
domain-id 1
site-id 400
ipv6-strict-control true
admin-tech-on-failure
organization-name "Cisco"
vbond vbond
```

### Configure Cisco SD-WAN Manager and Cisco SD-WAN Controller for IPv6 in a Dual IP Stack Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

The following example shows how to configure IPv6 as the preferred address family in a Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager:

Enable IPv6:

```
system
ipv6-strict-control true
```

Here is the complete configuration example for configuring IPv6 as the preferred address family on a Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager.

```
system
host-name vm9
system-ip 10.16.255.19
site-id 400
ipv6-strict-control true
port-offset 9
no daemon-restart
admin-tech-on-failure
no vrrp-advt-with-phymac
organization-name "Cisco"
vbond vbond
```

# Monitor IPv6 as Preferred Address Family in a Dual Stack Environment

After you successfully configure an IPv6 connection, the BFD connections will be up and running in Cisco SD-WAN Manager. To view the BFD connections in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**
2. Verify the status of the connection under the **BFD** column.

# Monitor IPv6 as Preferred Address Family in a Dual Stack Environment Using the CLI

Use the following **show** commands to view control and data connection information for IPv4 and IPv6.

### Cisco IOS XE Catalyst SD-WAN Devices

- **show sdwan control connections**
- **show sdwan control local-properties**
- **show sdwan bfd sessions**
- **show sdwan omp tlocs**

- **show sdwan bfd tloc-summary-list**

For more information on these **show** commands, see the chapter Troubleshooting Commands in the Cisco IOS XE SD-WAN Qualified Command Reference guide.

### Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller

- **show control connections**
- **show control local-properties**

For more information on these **show** commands, see the chapter Operational Commands.

# Troubleshooting

### Problem

BFD sessions are down.

### Possible Causes

Verify the IP address connections.

### Solution

Verify the configuration for IPv4 or IPv6 in the Cisco IOS XE Catalyst SD-WAN devices and in Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller. For more information, see Troubleshoot Common BFD Errors.

# Configuration Example for IPv6 as Preferred Address Family in a Dual Stack Environment

### Configuration Example for IPv6 configured on a Cisco IOS-XE SD-WAN Device

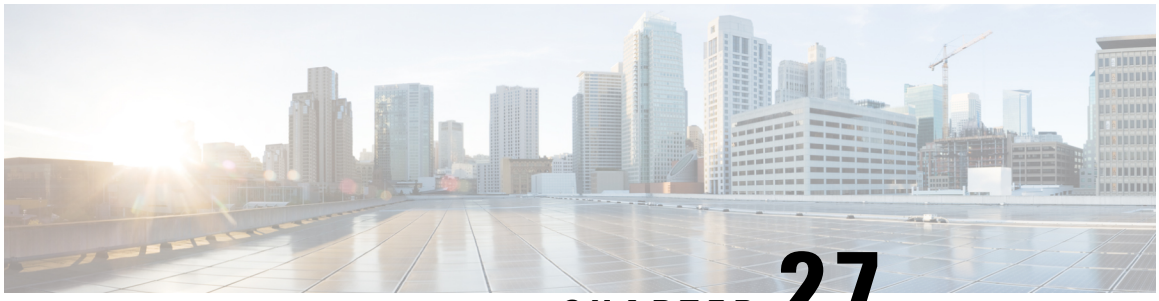
This example shows how to configure IPv6 as the preferred address family on a Cisco IOS XE Catalyst SD-WAN device.

```
show sdwan running-config system
system
gps-location latitude 32.0
gps-location longitude -100.0
system-ip 10.16.255.14
domain-id 1
site-id 400
ipv6-strict-control true
admin-tech-on-failure
organization-name "Cisco"
vbond vbond
```

### Configuration Example for IPv6 configured on Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller

This example shows how to configure IPv6 as the preferred address family on Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller.

```
show running-config system
system
host-name vm9
system-ip 10.16.255.19
site-id 400
ipv6-strict-control true
port-offset 9
no daemon-restart
admin-tech-on-failure
no vrrp-advt-with-phymac
organization-name "Cisco"
vbond vbond
```



CHAPTER 27

# IP Directed Broadcast

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.

**Note** The access control list (ACL) option for directed broadcast is not supported in Cisco SD-WAN Manager.

To enable the translation of a directed broadcast to physical broadcasts, use the ip directed-broadcast command. To disable this function, use the no form of this command. By default, ip directed-broadcast is disabled and all IP directed broadcasts are dropped.

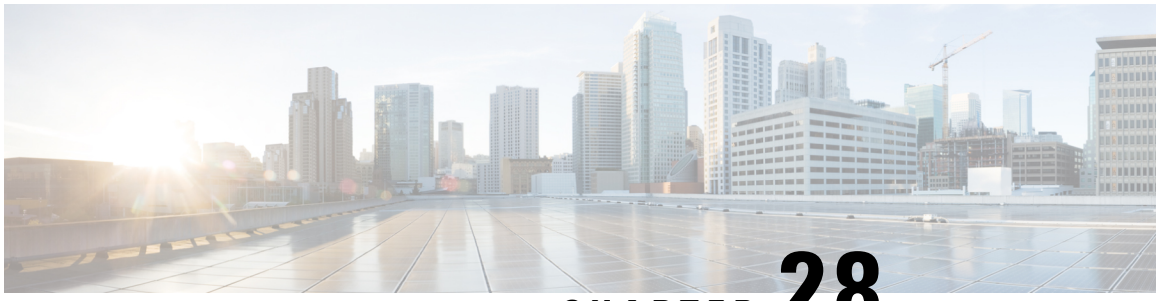
**ip directed-broadcast** and **no ip directed-broadcast**

### Example

This example shows how to enable forwarding of IP directed broadcasts on Ethernet interface 2/1:

```
device# configure-transaction
device(config)# interface ethernet 2/1
device(config-if)# ip address 10.114.114.1 255.255.255.0
```

```
device(config-if)# ip directed-broadcast
device(config-if)# end
```



CHAPTER 28

# Migrate Shared Templates to Cisco IOS XE Catalyst SD-WAN Templates

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

## Overview

In Cisco vManage 20.1.1, support is added for for additional feature templates exclusively for Cisco IOS XE Catalyst SD-WAN devices.

In releases before Cisco vManage 20.1.1, when you created a template for both Cisco vEdge and Cisco IOS XE Catalyst SD-WAN devices, the same template is shared for both device types. For these templates, the configuration is specified using Cisco vEdge commands. If the template is then used with a Cisco IOS XE device, the configuration was converted for Cisco IOS XE devices. Due to this conversion of Cisco vEdge commands, some functionality was not unavailable for Cisco IOS XE Catalyst SD-WAN devices. For example, NAT DIA.

In these releases, there are two types of shared templates:

- Shared feature templates: If you specify a Cisco IOS XE Catalyst SD-WAN device when creating a feature template, a shared feature template is created.
- Shared device templates: A device template that contains a shared feature template.

In Cisco vManage 20.1.1 and onwards, feature templates have been separated for Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices. These feature templates that are exclusively created for Cisco IOS XE Catalyst SD-WAN devices enable support for additional features. To use these feature templates, you can migrate your shared feature templates to the exclusive templates.

### List of Migrated Templates

The following table lists the shared templates and their corresponding exclusive templates for Cisco IOS XE Catalyst SD-WAN devices available in Cisco vManage 20.1.1 and onwards.

**Note** The AAA feature template is not supported with the exclusive Cisco IOS XE Catalyst SD-WAN device feature templates.

If your existing template contains an AAA feature template, you can replace it either before migration or after migration:

- Before migration—Replace it with the AAA-Cisco template that was introduced in 19.1.

  or
- After migration—After the migration is complete, manually create a Cisco AAA template and attach it to your device template.

| Shared Feature Template | Shared Template Type | Exclusive Cisco IOS XE Catalyst SD-WAN Device Feature Template | Exclusive Cisco IOS XE Catalyst SD-WAN Device Feature Template Type |
|---|---|---|---|
| Banner | banner | Cisco Banner | cisco_banner |
| BFD | bfd-vedge | Cisco BFD | cisco_bfd |
| BGP | bgp | Cisco BGP | cisco_bgp |
| DHCP Server | dhcp-server | Cisco DHCP Server | cisco_dhcp_server |
| Logging | logging | Cisco Logging | cisco_logging |
| NTP | ntp | Cisco NTP | cisco_ntp |
| OMP | omp-vedge | Cisco OMP | cisco_omp |
| OSPF | ospf | Cisco OSPF | cisco_ospf |
| Security | security-vedge | Cisco Security | cisco_security |
| SNMP | snmp | Cisco SNMP | cisco_snmp |
| System | system-vedge | Cisco System | cisco_system |
| VPN Interface GRE | vpn-vedge-interface-gre | Cisco VPN Interface GRE | cisco_vpn_interface_gre |
| VPN Interface IPsec | vpn-vedge-interface-ipsec | Cisco VPN Interface IPsec | cisco_vpn_interface_ipsec |
| VPN Interface Ethernet | vpn-vedge-interface | Cisco VPN Interface Ethernet | cisco_vpn_interface |
| VPN | vpn-vedge | Cisco VPN | cisco_vpn |

### Migrate Shared Templates

You can continue using the older shared templates, however the shared templates may not have access to the latest features. We recommend migrating existing templates to enable access to the latest features. For example,

if you are using the `VPN Interface Ethernet` shared template, the template still continues to work. However to use new features, such as NAT DIA, you must migrate to the exclusive feature template called `Cisco VPN Interface Ethernet`.

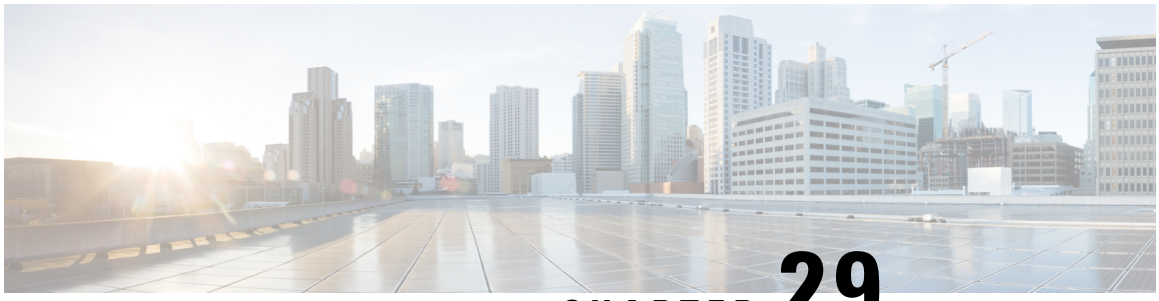
### Migrate Shared Templates Using the Cisco SD-WAN Manager Migration Tool

Prerequisites:

- At least one Cisco IOS XE Catalyst SD-WAN device template should exist with shared Cisco IOS XE Catalyst SD-WAN device feature templates attached prior to upgrading to Cisco vManage 20.1.1 or higher.

To migrate existing shared templates using Cisco SD-WAN Manager, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Template Migration**.
2. Click **Migrate All Templates**.
3. Enter a prefix for the new migrated templates. For example `Migrated_`. All migrated templates are prefixed with this identifier.
4. To migrate the templates, click **OK**.
5. Once the migration begins, click **Tasks** to track the status of the migration.
6. Once the migration is complete, you must manually attach the migrated templates to your devices. For each of the migrated templates, click **...** and choose **Attach Devices to Migrated Template**.



CHAPTER 29

# CLI Templates for Cisco IOS XE Catalyst SD-WAN 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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

You can configure CLI templates for Cisco IOS XE Catalyst SD-WAN devices in the following ways.

**Note** If you generate a CLI template in a higher version of Cisco SD-WAN Manager and then try to apply it in a lower version, it may not be supported depending on the configuration. In this case, Cisco SD-WAN Manager might also deny access and generate an error message. We recommend that you use a CLI template generated in an earlier version of Cisco SD-WAN Manager. For example, if you are using Cisco vManage Release 20.7.x, you can use a CLI template generated in Cisco vManage Release 20.6.x and earlier releases.


- Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices, on page 857
- Intent-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices, on page 859


# Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices

Cisco SD-WAN Manager configures Cisco IOS XE Catalyst SD-WAN devices using a combination of feature templates and policies (localized policies, security policies). In Cisco vManage 20.1.1 and onwards, Cisco SD-WAN Manager allows you to specify CLI templates that use the device configuration with Cisco IOS XE Catalyst SD-WAN devices. You can use these templates to push the device configuration (yang-cli) to devices directly.

In a single operation, Cisco SD-WAN Manager pushes the difference between the device configuration and configuration provided by the user in the template directly to the Cisco IOS XE Catalyst SD-WAN devices. Cisco SD-WAN Manager also displays a preview of the configuration before it is pushed to the device, as it does with other templates. The described workflow also applies if you want to make any additions, changes, or removals to the template.

**Note** To configure features not accessible using Cisco SD-WAN Manager, we recommend doing the following:

1. Use the relevant feature template in addition to a CLI add-on feature template. For more information, see Qualified CLIs for CLI Add-On Feature Templates, on page 887.
2. For situations where the previous option is not sufficient, use the device configuration-based CLI templates as described in this section.

### Feature Information for CLI Template for Cisco XE SD-WAN Routers

*Table 225: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Device Configuration CLI Templates | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r<br>Cisco vManage 20.1.1 | The CLI Templates feature has been updated to support device configuration-based CLIs. You can use these templates to push the device configuration (yang-cli) to devices directly. |

### Limitations

**Auxiliary ports**: When using a CLI template for Cisco Integrated Services Routers that have an auxiliary port, do not include commands for auxiliary ports, such as **line aux 0**. Doing so results in an error. These commands may be executed directly on the device.

When you import the CLI template configuration using the command, `show sdwan running-config`, you need to add quotes manually for the CLI template on the Cisco SD-WAN Manager.

### Configure CLI Templates in 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 as **Device**.

3. From the **Create Template** drop-down list, select **CLI Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. In **Template Name**, enter a name for the template.

The name can be up to 128 characters and can contain only alphanumeric characters.

6. In **Template Description**, enter a description of the template.

   The description can be up to 2048 characters and can contain only alphanumeric characters.

7. Choose **Device configuration**. Using this option, you can provide IOS-XE configuration commands that appear in the output of the `show sdwan running-config` command.

8. (Optional) To load the running config of a connected device, select it from the Load Running config from reachable device list and click **Search**.

9. In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

10. 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}}.

    These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

11. To save the feature template, click **Add**. The new device template is displayed in the Device Template table.

# Intent-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices

The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allows you to configure intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager. Intent-based CLI template refer to the command line interface configuration that are based on the Cisco vEdge device syntax. Using CLI templates, Cisco SD-WAN Manager enables pushing Cisco vEdge syntax-based commands to Cisco IOS XE Catalyst SD-WAN device in Cisco IOS XE Syntax.

**Note** With the support of device configuration-based CLI templates, the intent-based CLI templates will be deprecated. We recommend using the device configuration-based CLI templates as described in Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices, on page 857.

Using Cisco SD-WAN Manager CLI templates significantly reduces the effort to configure feature templates.

### Feature Information for CLI Template for Cisco IOS XE Catalyst SD-WAN devices

*Table 226: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| CLI Template for Cisco XE SD-WAN Routers | Cisco IOS XE Release 16.11.1a<br>Cisco SD-WAN release 19.1 | The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allows to you configure intent-based CLI templates for Cisco XE SD-WAN routers using Cisco SD-WAN Manager. |
| VRF Configuration | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | Support for VRF configuration increased from a total of 100 to a total of 300 VRFs. Supported on: Cisco ASR 1001-HX and Cisco ASR 1002-HX |

### Benefits of CLI Templates

- You can reuse any Cisco vEdge-specific Cisco SD-WAN Manager feature templates for Cisco IOS XE Routers. When you create a device template using Cisco XE SDWAN Feature Templates, Cisco SD-WAN Manager displays the intent-based configuration (vEdge CLI syntax) and the corresponding device-based (Cisco XE SDWAN Routers) configuration. You can examine the intent-based configuration and repurpose that to create a separate CLI template for XE SDWAN routers.
- You can make multiple changes to a CLI template in a single edit.
- You can use a single configuration across multiple devices of the same device models. Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.
- You can define custom length for variables in CLI Templates.
- You can use any existing IOS-XE device intent configuration as input for CLI template.
- Content of a CLI template can be used across multiple IOS-XE device types (common CLIs like VPN, VPN interface, BGP, OSPF and so on).

### Limitations

**Auxiliary ports**: When using a CLI template for Cisco Integrated Services Routers that have an auxiliary port, do not include commands for auxiliary ports, such as **line aux 0**. Doing so results in an error. These commands may be executed directly on the device.

### Configuring CLI Templates in Cisco SD-WAN Manager

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 as **Device**.

3. From the **Create Template** drop-down list, select **CLI Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. In **Template Name**, enter a name for the template.

   The name can be up to 128 characters and can contain only alphanumeric characters.
6. In **Template Description**, enter a description of the template.

   The description can be up to 2048 characters and can contain only alphanumeric characters.
7. The configuration of the CLI template can either be intent-based or based on the device configuration.
   - **Intent**: If you specify **Intent**, you specify commands in the Cisco vEdge format. If the device you've selected is a Cisco IOS XE Catalyst SD-WAN device, Cisco SD-WAN Manager converts the configuration for the device.
   - **Device configuration**: This option is available from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and onwards and only for Cisco IOS XE Catalyst SD-WAN devices. For this option, you must specify the entire device configuration as it appears in `show sd-wan running config`.

**Note** You can only use this feature with the qualified CLIs detailed in Qualified CLIs for CLI Add-On Feature Templates, on page 887.

You can upload a configuration file using **Select a File** or copy and paste the CLI configuration. Following is an example of an intent-based CLI with variables.

```
system

   host-name {{hostname}}
   system-ip {{system_ip}}
   domain-id 1

   site-id {{site_id}}
   port-offset           1
   admin-tech-on-failure
   organization-name "XYZ"
   logging
    disk
     enable
! !
```

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

8. To save the feature template, click **Add**.

**Note** See the Attach Devices to a Device Template section in this topic to know more about attaching a device to a template and reusing a template for multiple devices of the same device model.

## Sample Configurations for CLI Template

### System Level Configuration

*Table 227: System Level Parameters*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| system<br> host-name pm4<br> system-ip 172.16.255.14<br> overlay-id 1<br> site-id 400<br> control-session-pps 300<br>admin-tech-on-failure<br><br>sp-organization-name "XYZ Inc Regression"<br>organization-name "XYZ Regression"<br>console-baud-rate 115200<br>vbond 10.0.12.26 port 12346 | system<br><br>host-name<br> pm4<br>system-ip<br> 172.16.255.14<br>overlay-id<br> 1<br>site-id 400<br>control-session-pps 300<br>admin-tech-on-failure<br>sp-organization-name “XYZ Inc Regression”<br>organization-name “XYZ Inc Regression”<br>console-baud-rate 11520<br>vbond 10.0.12.26 port 12346 |

## AAA Configuration - Authentication, authorization, and accounting (AAA) with RADIUS and TACACS+

*Table 228: AAA Configuration*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| aaa<br> auth- order local radius tacacs<br> usergroup basic<br><br> task system read write<br> task interface read write<br>!<br><br>usergroup netadmin<br>!<br><br>usergroup operator<br>task system read<br>task interface read<br>task policy read<br>task routing read<br>task security read<br>!<br>user admin password<br><br>$6$nbbLkA==$ae/DO78l/wluPUohhBU2L6h/<br>Q.PLkurGvxjRlS9OWB9iTtFwSGNQcABV6F<br>MW57vuEHvo3zp3qdYVinLmMIu/p/<br>secret<br>$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c<br><br>! !<br>radius<br><br> server 10.99.144.200<br>  source-interface GigabitEthernet0/0/1<br> exit<br> server 10.99.144.201<br><br>  source-interface GigabitEthernet0/1/0<br> exit<br>!<br>tacacs<br><br> server 10.0.1.1<br>  auth-port 50<br><br>  vpn 0<br><br>  source-interface GigabitEthernet0/0/1<br><br>  key 1<br><br>  secret-key<br>$8$Kcuva0CM871E8czESwV5g/YX4Q8pY1LSNk/+PIDrpCg=<br><br> exit !<br>! | aaa group server tacacs+ server-10.0.1.1<br>  server-private 10.0.1.1 timeout 5 key<br>$8$vs5hzVg/Z6EeuUdNHTzOwWPsUv9V/50xmcRfShWp3YI=<br><br> ip tacacs source-interface<br>GigabitEthernet0/0/1<br>!<br>aaa group server radius server-10.99.144.200<br><br> server-private 10.99.144.200 auth-port 1812<br> timeout 5 retransmit 3<br> ip radius source-interface<br>GigabitEthernet0/0/1<br>!<br><br>aaa group server radius server-10.99.144.201<br><br> server-private 10.99.144.201 auth-port 1812<br> timeout 5 retransmit 3<br> ip radius source-interface<br>GigabitEthernet0/1/0<br>!<br>aaa authentication login default local group<br> radius group tacacs+<br>aaa authorization exec default local group<br>radius group tacacs+ a<br>aa session-id common --- added by default<br><br>username admin privilege 15 secret 9<br>$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c |

### Logging configuration - Configures logging to either the local hard drive or a remote host

*Table 229: Logging Configuration*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| logging<br>disk<br>enable<br>file size 12<br>file rotate 6<br>!<br>server 192.168.13.1<br>vpn 0<br>source-interface Loopback1<br>priority alert<br>exit<br>! | logging<br>disk<br>enable<br>!<br>!<br>logging persistent size 75497472 filesize 12582912<br>logging buffered 512000 --- added by default<br><br>logging host 192.168.13.1<br>no logging rate-limit<br>logging source-interface Loopback1<br>logging persistent |

### Switch Port and VLAN configuration

*Table 230: Switch Port Configuration*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| interface GigabitEthernet0/1/4<br>switchport<br>mode trunk<br>access vlan vlan 10<br>access vlan name "DHCP Vlan"<br>trunk allowed vlan 10<br>!<br>no shutdown<br><br>vpn 10<br>name "DHCP VPN"<br>interface Vlan10<br>description "Vlan 10 Mgmt interface"<br>ip address 10.29.35.1/24<br>no shutdown<br>!<br>! | interface GigabitEthernet0/1/4<br>switchport ios-sw:mode trunk<br>switchport ios-sw:trunk allowed vlan 10<br>no shutdown<br>no ip address<br>exit<br><br>interface Vlan10<br>description Vlan 10 Mgmt interface<br>no shutdown<br>arp timeout 1200<br>vrf forwarding 10<br>ip address 10.29.35.1 255.255.255.0<br>ip mtu 1500<br>exit |

## Cellular Configuration

*Table 231: Cellular Configuration - Configures cellular controllers and cellular interfaces*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| vpn 0<br>  interface Cellular0/2/0<br>  description "Cellular interface"<br>  no shutdown<br>  !<br><br><br>  controller cellular 0/2/0<br>  lte sim max-retry 1<br>  lte failovertimer 7<br>  profile id 1 apn Broadband<br>  ! | interface Cellular0/2/0<br>  description Cellular interface<br>  no shutdown<br>  ip address negotiated<br>  ip mtu 1428<br>  mtu  1500<br>  exit<br><br>  controller Cellular 0/2/0<br>  lte sim max-retry 1<br>  lte failovertimer 7<br>  profile id 1 apn Broadband authentication none pdn-type ipv4 |

### BGP, OSPF, and EIGRP - Configures BGP, OSPF, and EIGRP Routing Protocols under Transport or Service VPN

*Table 232: BGP, OSPF, and EIGRP Configuration*

| CLI Template Configuration | Configuration on the Device |
|---|---|

| CLI Template Configuration | Configuration on the Device |
|---|---|
| vpn1<br>  bgp 2<br>  shutdown<br>  distance external 30<br>  distance internal 250<br>  distance local 10<br>  address-family ipv4-unicast<br>  network 10.0.100.0/24<br>  redistribute static route-policy route_map<br>  redistribute connected route-policy route_map<br>  !<br>  neighbor 10.0.100.1<br>  no shutdown<br>  remote-as  3<br>  timers<br>  keepalive  12<br>  holdtime  20<br>  connect-retry  300<br>  advertisement-interval 123<br>  !<br>  update-source GigabitEthernet0/0/1<br>  ebgp-multihop 1<br>  password $8$9pou4PH9b60B072hcw3MmSSdLCfJk8bVys12lLVb+08=<br><br>  address-family ipv4-unicast<br><br><br>vpn 1<br>  router<br>  ospf<br>  router-id 172.16.255.15<br>  compatible rfc1583<br>  timers spf 200 1000 10000<br>  redistribute connected route-policy route_map<br>  max-metric router-lsa administrative<br>  area 23<br>  stub<br>  interface GigabitEthernet0/0/1<br>  cost 23<br>  authentication type message-digest<br>  authentication authentication-key key1<br><br>  exit<br>  exit<br>  !<br><br>vpn 1<br>router<br>  eigrp 1<br>  af-interface GigabitEthernet0/0/2<br>  no split-horizon<br>  exit-af-interface<br>  !<br>address-family ipv4 network 10.1.10.1/32<br>address-family ipv4 topology base<br>redistribute omp<br>exit-af-topology | |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| | router bgp 2<br>bgp log-neighbor-changes<br>distance bgp 30 250 10<br>address-family ipv4 unicast vrf 1<br>neighbor 10.0.100.1 remote-as 3<br>neighbor 10.0.100.1 activate<br>neighbor 10.0.100.1 ebgp-multihop 1<br>neighbor 10.0.100.1 maximum-prefix 2147483647 100<br>neighbor 10.0.100.1 password 0 password<br>neighbor 10.0.100.1 send-community both<br>neighbor 10.0.100.1 timers 12 20<br>neighbor 10.0.100.1 update-source GigabitEthernet0/0/1<br>network 10.0.100.0 mask 255.255.255.0<br>redistribute connected<br>redistribute static route-map route_map<br>exit-address-family<br>!<br>timers bgp 60 180<br><br>router ospf 1 vrf 1<br>auto-cost reference-bandwidth 100<br>max-metric router-lsa<br>timers throttle spf 200 1000 10000<br>router-id 172.16.255.15<br>default-information originate<br>distance ospf external 110<br>distance ospf inter-area 110<br>distance ospf intra-area 110<br>redistribute connected subnets route-map route_map<br>!<br>interface GigabitEthernet0/0/1<br>no shutdown<br>arp timeout 1200<br>vrf forwarding 1<br>ip address 10.1.100.14 255.255.255.0<br>ip redirects<br>ip mtu 1500<br>ip ospf 1 area 23<br>ip ospf network broadcast<br>mtu 1500<br>negotiation auto<br>exit<br>!<br>router eigrp eigrp-name<br>address-family ipv4 vrf 1 autonomous-system 1<br>af-interface GigabitEthernet0/0/2<br>hello-interval 5<br>hold-time 15<br>no split-horizon<br>exit-af-interface<br>!<br>network 10.1.10.1 0.0.0.0<br>topology base<br>redistribute omp<br>exit-af-topology<br>!<br>exit-address-family |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| | !<br>! |

### VPN, Interface, and Tunnel Configuration for WAN and LAN interfaces

***Table 233: VPN, Interface, and Tunnel Configuration***

| CLI Template Configuration | Configuration on the Device |
|---|---|
| vpn 0<br>  interface GigabitEthernet0/2/0<br>    ip address 10.1.14.14/24<br>    tunnel-interface<br>     encapsulation ipsec<br>     color lte<br>     no allow-service bgp<br>     allow-service dhcp<br>     allow-service dns<br>     allow-service icmp<br>     no allow-service sshd<br>     no allow-service netconf<br>     no allow-service ntp<br>     no allow-service ospf<br>     no allow-service stun<br>     allow-service https<br>    !<br>    autonegotiate<br>    no shutdown<br>   !<br>  ip route 0.0.0.0/0 10.1.14.13<br><br><br><br>vpn 512<br>interface GigabitEthernet0<br>    ip dhcp-client<br>ipv6 dhcp-client autonegotiate<br>no shutdown<br>! ! | ip route 0.0.0.0 0.0.0.0 10.1.14.13 1<br><br>interface GigabitEthernet0/2/0<br>   no shutdown<br>   arp timeout 1200 – added by default<br>   ip address 10.1.14.14 255.255.255.0<br>   ip redirects --> added by default<br>   ip mtu    1500<br>   mtu 1500<br>   negotiation auto --> added by default<br>  exit<br><br>interface Tunnel20 ---> based on the interface<br>0/2/0<br>   no shutdown<br>   ip unnumbered GigabitEthernet0/2/0<br>   no ip redirects<br>   ipv6 unnumbered GigabitEthernet0/2/0<br>   no ipv6 redirects<br>   tunnel source GigabitEthernet0/2/0<br>   tunnel mode sdwan<br><br>sdwan<br>   interface GigabitEthernet0/2/0<br>    tunnel-interface<br>     encapsulation ipsec weight 1<br>     color lte<br>     no last-resort-circuit<br>     vmanage-connection-preference 5<br>     no allow-service all<br>     no allow-service bgp<br>     allow-service dhcp<br>     allow-service dns<br>     allow-service icmp<br>     no allow-service sshd<br>     no allow-service netconf<br>     no allow-service ntp<br>     no allow-service ospf<br>     no allow-service stun<br><br><br>interface GigabitEthernet0<br>no shutdown<br>arp timeout 1200<br>vrf forwarding Mgmt-intf<br>ip address dhcp client-id GigabitEthernet0 ip<br>redirects<br>ip dhcp client default-router distance 1 ip<br>mtu 1500<br>mtu 1500<br>negotiation auto |

## Network Address Translation (NAT) over Direct Internet Access (DIA)

*Table 234: NAT over DIA*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| vpn 201<br>interface GigabitEthernet0/0/2.2901<br>description gigi21<br>ip address 10.201.201.1/24<br>mtu 1496<br>no shutdown<br>vrrp 100<br>track-omp<br>ipv4 10.201.201.3<br>!<br>!<br>!<br><br>dhcp-server<br>address-pool 10.201.201.0/24<br>exclude 10.201.201.1-10.201.201.10<br>10.201.201.20-10.201.201.22<br>offer-time 600<br>lease-time 86400<br>admin-state up<br>options<br>default-gateway 10.201.201.1<br>dns-servers 10.99.139.201<br>tftp-servers 10.99.139.201<br>!<br>!<br>!<br>ip route 0.0.0.0/0 vpn 0<br>!<br><br>vpn 0<br>interface GigabitEthernet0/0/0<br>ip address 172.16.10.1/24<br>nat<br>udp-timeout 3<br>tcp-timeout 40<br>respond-to-ping<br>!<br>! | interface GigabitEthernet0/0/2.2901<br>no shutdown<br>encapsulation dot1Q 2901<br>vrf forwarding 201<br>ip address 10.201.201.1 255.255.255.0<br>ip mtu 1496<br>vrrp 100 address-family ipv4<br>vrrpv2<br>address 10.201.201.3<br>priority 100<br>track omp shutdown<br>exit<br>exit<br><br>ip dhcp excluded-address vrf 201 10.201.201.1<br>10.201.201.10<br>ip dhcp excluded-address vrf 201<br>10.201.201.20 10.201.201.22<br>ip dhcp pool<br>vrf-201-GigabitEthernet0/0/2.2901<br>option 150 ip 10.99.139.201<br>vrf 201<br>lease 1 0 0<br>default-router 10.201.201.1<br>dns-server 10.99.139.201<br>network 10.201.201.0 255.255.255.0<br>exit<br>ip dhcp use hardware-address client-id<br>no ip dhcp use class<br>ip dhcp use vrf remote<br><br>ip nat inside source list<br>nat-dia-vpn-hop-access-list interface<br>GigabitEthernet0/0/0 overload<br>ip nat translation tcp-timeout 40<br>ip nat translation udp-timeout 3<br>ip nat route vrf 201 0.0.0.0 0.0.0.0 global<br><br>interface GigabitEthernet1/0/2<br>no shutdown<br>arp timeout 1200<br>ip address 10.1.15.15 255.255.255.0<br>ip nat outside<br>ip redirects<br>ip mtu 1500<br>mtu 1500<br>negotiation auto |

## NAT64 Configuration

***Table 235: NAT64 Configuration***

| | |
|---|---|
| vpn 1<br>  nat64<br>  v4 pool pool1 start-address 10.1.1.10<br>  v4 pool pool1 end-address 10.1.1.100<br>  !<br>  interface GigabitEthernet3<br>  ip address 10.1.19.15/24<br>  nat64<br>  !<br>  autonegotiate<br>  no shutdown<br>  ! | interface GigabitEthernet3<br>  no shutdown<br>  arp timeout 1200<br>  vrf forwarding 1<br>  ip address 10.1.19.15 255.255.255.0<br>  negotiation auto<br>  nat64 enable<br>  nat64 prefix stateful 2001::F/64 vrf 1<br><br>  nat64 v4 pool pool1 10.1.1.10 10.1.1.100<br>  nat64 v6v4 list global-list pool pool1 vrf 1<br>  nat64 translation timeout tcp 60<br>  nat64 translation timeout udp 1 |

## Multilink and T1/E1 - Configures T1/E1 Controller and Serial, Multilink Interfaces

***Table 236: Configuring Multilink***

| CLI Template Configuration | Configuration on the Device |
|---|---|
| card type t1 0 2<br>  controller T1 0/2/0<br>  framing esf<br>  clock source internal<br>  linecode b8zs<br>  cablelength long 0db<br>  channel-group 1 timeslots 15<br>  channel-group 2 timeslots 12<br>  channel-group 3 timeslots 10<br>  channel-group 4 timeslots 10<br>!<br>interface Multilink1<br>  no shutdown<br>  encapsulation ppp<br>  ip address 10.1.10.30 255.255.255.0<br>  ppp pap sent-username admin password admin<br>ppp authentication pap<br>  ppp multilink<br>  ppp multilink links minimum 1<br>  ppp multilink fragment disable<br>  ppp multilink group 1<br>exit<br>interface Serial0/2/0:1<br>  no shutdown<br>  encapsulation ppp<br>  bandwidth 1536<br>  no ip address<br>  load-interval 30<br>  ppp pap sent-username admin password admin<br>ppp authentication pap<br>  ppp multilink<br>  ppp multilink group 1<br>exit | interface Multilink1<br>ip address 10.1.10.30/24 shutdown<br>controller T1 0/2/0<br>  linecode b8zs<br>  channel-group 1<br>  channel-group 3<br>!<br>ppp pap sent-username admin password admin<br>ppp authentication pap<br>ppp multilink<br>ppp multilink group 1 |

## Local QoS Policy

*Table 237: Local QoS Policy*

| CLI Template Configuration | Configuration on the Device |
|---|---|

| CLI Template Configuration | Configuration on the Device |
|---|---|
| vpn 1<br>interface GigabitEthernet0/0/1<br>ip address 10.2.54.15/24<br>no shutdown<br>access-list MyACL in<br>!<br>policy<br>class-map<br>class best-effort queue 3<br>class bulk-data queue 2<br>class critical-data queue 1<br>class voice queue 0<br>!<br>access-list MyACL<br>sequence 10<br>match<br>dscp 46<br>!<br>action accept<br>class voice<br>!<br>!<br>sequence 20<br>match<br>source-ip 10.1.1.0/24<br>destination-ip 192.168.10.0/24<br>!<br>action accept<br>class bulk-data<br>set<br>dscp 32<br>!<br>!<br>!<br>sequence 30<br>match<br>destination-ip 192.168.20.0/24<br>!<br>action accept<br>class critical-data<br>set<br>dscp 22<br>!<br>!<br>!<br>sequence 40<br>action accept<br>class best-effort<br>set<br>dscp 0<br>!<br>!<br>!<br>default-action accept<br>!<br>qos-scheduler be-scheduler<br>class best-effort<br>bandwidth-percent 20<br>buffer-percent 20<br>drops red-drop<br>!<br>qos-scheduler bulk-scheduler | interface GigabitEthernet0/0/1<br>access-list MyACL in<br>exit<br>class-map match-any best-effort<br>match qos-group 3<br>!<br>class-map match-any bulk-data<br>match qos-group 2<br>!<br>class-map match-any critical-data<br>match qos-group 1<br>!<br>class-map match-any voice<br>match qos-group 0<br>!<br>policy-map MyQoSMap<br>class best-effort<br>random-detect<br>bandwidth percent 20<br>!<br>class bulk-data<br>random-detect<br>bandwidth percent 20<br>!<br>class critical-data<br>random-detect<br>bandwidth percent 40<br>!<br>class voice<br>priority percent 20<br>!<br>!<br>policy<br>no app-visibility<br>no flow-visibility<br>no implicit-acl-logging<br>log-frequency 1000<br>class-map<br>class best-effort queue 3<br>class bulk-data queue 2<br>class critical-data queue 1<br>class voice queue 0<br>!<br>access-list MyACL<br>sequence 10<br>match<br>dscp 46<br>!<br>action accept<br>class voice<br>!<br>!<br>sequence 20<br>match<br>source-ip 10.1.1.0/24<br>destination-ip 192.168.10.0/24<br>!<br>action accept<br>class bulk-data<br>set<br>dscp 32<br>! |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| class bulk-data<br>bandwidth-percent 20<br>buffer-percent 20<br>drops red-drop<br>!<br>qos-scheduler critical-scheduler<br>class critical-data<br>bandwidth-percent 40<br>buffer-percent 40<br>drops red-drop<br>!<br>qos-scheduler voice-scheduler<br>class voice<br>bandwidth-percent 20<br>buffer-percent 20<br>scheduling llq<br>!<br>qos-map MyQoSMap<br>qos-scheduler be-scheduler<br>qos-scheduler bulk-scheduler<br>qos-scheduler critical-scheduler<br>qos-scheduler voice-scheduler<br>! | !<br>!<br>sequence 30<br>match<br>destination-ip 192.168.20.0/24<br>!<br>action accept<br>class critical-data<br>set<br>dscp 22<br>!<br>!<br>sequence 40<br>action accept<br>class best-effort<br>set<br>dscp 0<br>!<br>!<br>default-action accept |

## Security Policy (ZBFW, IPS/IDS, URL-Filtering) Configuration

*Table 238: Security Policy (ZBFW, IPS/IDS, URL-Filtering)*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| policy<br>zone internet<br>vpn 0<br>!<br>zone zone1<br>vpn 1<br>!<br>zone zone2<br>vpn 2<br>!<br>zone-pair ZP_zone1_internet_fw_policy<br>source-zone zone1<br>destination-zone internet<br>zone-policy fw_policy<br>!<br>zone-pair ZP_zone1_zone2_fw_policy<br>source-zone zone1<br>destination-zone zone2<br>zone-policy fw_policy<br>!<br>zone-based-policy fw_policy<br>sequence 1<br>match<br>source-data-prefix-list subnet1<br>!<br>action inspect<br>!<br>!<br>default-action pass<br>!<br>zone-to-nozone-internet deny<br>lists<br>data-prefix-list subnet1<br>ip-prefix 10.0.10.0/24<br>!<br>!<br>url-filtering url_filter<br>web-category-action block<br>web-categories games<br>block-threshold moderate-risk<br>block text<br>"<![CDATA[<h3>Access" to the requested<br>page has been denied]]>"<br>target-vpns 1<br>!<br>intrusion-prevention intrusion_policy<br>security-level connectivity<br>inspection-mode protection<br>log-level err<br>target-vpns 1<br>!<br>failure-mode open<br>!<br>!<br>! | |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| | ip access-list extended fw_policy-seq-1-acl_<br>11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any<br>!<br>ip access-list extended utd-nat-acl<br>10 permit ip any any<br>!<br>class-map type inspect match-all fw_policy-seq-1-cm_<br>match access-group name fw_policy-seq-1-acl_<br>!<br>policy-map type inspect fw_policy<br>class fw_policy-seq-1-cm_<br>inspect<br>!<br>class class-default<br>pass<br>!<br>!<br>object-group service fw_policy-seq-1-service-og_<br>ip<br>!<br>parameter-map type inspect-global<br>alert on<br>log dropped-packets<br>multi-tenancy<br>vpn zone security<br>!<br>parameter-map type umbrella global<br>token A5EA676087BF66A42DC4F722C2AFD10D00256274<br>dnscrypt<br>vrf 1<br>dns-resolver umbrella<br>match-local-domain-to-bypass<br>!<br>!<br>zone security internet<br>vpn 0<br>!<br>zone security zone1<br>vpn 1<br>!<br>zone security zone2<br>vpn 2<br>!<br>zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet<br>service-policy type inspect fw_policy<br>!<br>zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2<br>service-policy type inspect fw_policy<br>!<br>app-hosting appid utd<br>app-resource package-profile cloud-low<br>app-vnic gateway0 virtualportgroup 0 |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| | guest-interface 0<br>  guest-ipaddress 192.168.1.2 netmask 255.255.255.252<br>  !<br>  app-vnic gateway1 virtualportgroup 1 guest-interface 1<br>  guest-ipaddress 192.0.2.2 netmask 255.255.255.252<br>  !<br>  start<br>  !<br>  utd multi-tenancy<br>  utd engine standard multi-tenancy<br>  web-filter block page profile block-url_filter<br>  text <\![CDATA[<h3>Access to the requested page has been denied</h3><p>Please contact your Network Administrator</p>]]><br>  !<br>  web-filter url profile url_filter<br>  categories block<br>  games<br>  !<br>  block page-profile block-url_filter<br>  log level error<br>  reputation<br>  block-threshold moderate-risk<br>  !<br>  !<br>  threat-inspection profile intrusion_policy<br><br>  threat protection<br>  policy connectivity<br>  logging level err<br>  !<br>  utd global<br>  !<br>  policy utd-policy-vrf-1<br>  all-interfaces<br>  vrf 1<br>  threat-inspection profile intrusion_policy<br><br>  web-filter url profile url_filter<br>  exit<br>  ! |

### Configuring NTP

*Table 239: Configuring NTP*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| ntp<br>server 10.29.43.1<br>source-interface GigabitEthernet1<br>version 4<br>exit<br>!<br>! | ntp server 198.51.241.229 source<br>GigabitEthernet1 version 4 |

### IPv6 Configuration

*Table 240: IPv6 Configuration*

| CLI Template Configurartion | Configuration on the Device |
|---|---|
| vpn 1<br>interface GigabitEthernet3<br>ipv6 address 2671:123A::1/128<br>shutdown<br>!<br>! | interface GigabitEthernet3<br>shutdown<br>arp timeout 1200<br>vrf forwarding 1<br>no ip address<br>ip redirects<br>ip mtu 1500<br>ipv6 address 2671:123A::1/128<br>ipv6 redirects<br>mtu 1500<br>negotiation auto<br>exit<br>vrf definition 1<br>rd 1:1<br>address-family ipv4<br>exit-address-family<br>!<br>address-family ipv6<br>exit-address-family<br>!<br>! |

### Service Configuration

In Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and earlier, only the following configurations under **service** can be configured via CLI templates:

```
service pad
service config
service tcp-keepalives-in
service tcp-keepalives-out
service tcp-small-servers
service udp-small-servers
```

### VRF Configuration

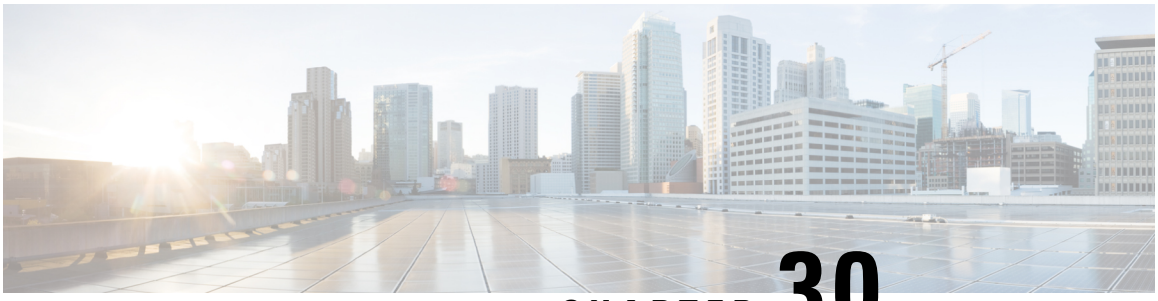
Configure up to 300 VRFs, with a corresponding subinterface for each VRF. The example configures two VRFs.

**Note** Do not configure VLAN 1. It is reserved for the native VLAN.

| CLI Template Configuration | Configuration on the Device |
|---|---|
| ! vpn 2 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.2.2 no shutdown remote-as 2 ! ipv6-neighbor 2001:DB8:2::2 remote-as 2 ! ! interface GigabitEthernet0/0/0.2 ip address 192.0.2.1/24 ipv6 address 2001: DB8:2::1/64 mtu 1496 no shutdown ! ! vpn 3 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.3.2 no shutdown remote-as 3 ! ipv6-neighbor 2001: DB8:3::2 remote-as 3 ! ! interface GigabitEthernet0/0/0.3 ip address 192.0.3.1/24 ipv6 address 2001: DB8:3::1/64 mtu 1496 no shutdown ! | |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| | vrf definition 2<br>rd 1:2<br>address-family ipv4<br>  route-target export 1000:2<br>  route-target import 1000:2<br>  exit-address-family<br>!<br>address-family ipv6<br>  exit-address-family<br>!<br>!<br>router bgp 1000<br>bgp log-neighbor-changes<br>distance bgp 20 200 20<br>!<br>address-family ipv4 vrf 2<br>  redistribute omp<br>  neighbor 192.0.2.2 remote-as 2<br>  neighbor 192.0.2.2 activate<br>  neighbor 192.0.2.2 send-community both<br>exit-address-family<br>!<br>address-family ipv6 vrf 2<br>  redistribute omp<br>  neighbor 2001:DB8:2::2 remote-as 2<br>  neighbor 2001: DB8:2::2 activate<br>  neighbor 2001: DB8:2::2 send-community both<br>exit-address-family<br>!<br>interface GigabitEthernet0/0/0.2<br>encapsulation dot1Q 2<br>vrf forwarding 2<br>ip address 192.0.2.1 255.255.255.0<br>ip mtu 1496<br>ipv6 address 2001:DB8:2::1/64<br>end<br><br>vrf definition 3<br>rd 1:3<br>address-family ipv4<br>  route-target export 1000:3<br>  route-target import 1000:3<br>  exit-address-family<br>!<br>address-family ipv6<br>  exit-address-family<br>!<br>!<br>router bgp 1000<br>bgp log-neighbor-changes<br>distance bgp 20 200 20<br>!<br>address-family ipv4 vrf 3<br>  redistribute omp<br>  neighbor 192.0.3.2 remote-as 3<br>  neighbor 192.0.3.2 activate<br>  neighbor 192.0.3.2 send-community both<br>exit-address-family<br>!<br>address-family ipv6 vrf 3<br>  redistribute omp<br>  neighbor 2001:DB8:3::2 remote-as 3 |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| | neighbor 2001: DB8:3::2 activate<br>neighbor 2001: DB8:3::2 send-community both<br>exit-address-family<br>!<br>interface GigabitEthernet0/0/0.3<br>encapsulation dot1Q 3<br>vrf forwarding 3<br>ip address 192.0.3.1 255.255.255.0<br>ip mtu 1496<br>ipv6 address 2001:DB8:3::1/64<br>end |



CHAPTER 30

# CLI Add-On Feature Templates

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 241: Feature History Table*

| Feature Name | Release Information | Description |
|---|---|---|
| CLI Add-On Feature Templates | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r<br>Cisco vManage 20.1.1 | This feature adds a new feature template called the CLI add-on feature template. You can use this feature template to attach specific CLI configurations to a device. If a configuration cannot be specified using Cisco SD-WAN Manager but can be configured using the CLI on the device, then you can use this feature template to specify such configurations. You can also use CLI add-on feature templates to add small pieces of CLI configuration, instead of an entire running configuration.<br>This feature is not intended to replace existing feature templates but instead to enhance their functionality. Note that not all CLIs are qualified. For more information, see Qualified CLIs for Cisco IOS XE Release 17.2.1r. |
| Additional Commands Qualified for CLI Add-On Feature Templates | Cisco IOS XE Release Amsterdam 17.2.1v<br>Cisco SD-WAN Release 20.1.12 | With each release, we qualify commands for use with the CLI add-on feature templates feature. In this release, we qualified additional commands. See the Appendix in Cisco IOS XE SD-WAN Qualified Command Reference. |


- Overview of the CLI Add-On Feature Templates, on page 884
- Restrictions for CLI Add-On Feature Templates, on page 885
- Create a CLI Add-On Feature Template, on page 885
- Qualified CLIs for CLI Add-On Feature Templates, on page 887


# Overview of the CLI Add-On Feature Templates

If you attach a device template containing both a feature template and the new CLI add-on feature template, the configurations are merged. The merge gives priority to the new CLI add-on feature templates. Cisco SD-WAN Manager first generates the configurations based on the feature template. After the configuration is generated, it uses the configuration from the CLI add-on feature templates to merge it into the feature template config output that was previously generated. Hence, using this feature, you can add specific device configurations that are not provided by the existing feature templates or you can override the configurations of existing feature templates.

When you specify commands using the template, use the commands as per the syntax displayed in the `show sdwan running-config` output. When you attach the template to the device, Cisco SD-WAN Manager takes the information from all feature templates and also takes the data you specified using the CLI add-on feature template to create the device configuration. The commands that you specify in the CLI add-on feature template overwrites any equivalent commands in the corresponding feature template.

In addition to changing existing commands, the CLI add-on feature template can also be used to specify commands that are not available in Cisco SD-WAN Manager but are qualified for the device. For example, for Cisco AAA, the `attempts login` command is not available in Cisco SD-WAN Manager. By using a CLI add-on feature template, you can specify the `aaa authentication attempts login` *`number`* command for a device. After you create the feature template, ensure that you add it to the device template.

**Note** You must define the CLI add-on feature template before you use it in a device template.

For a list of CLIs that are qualified, see Qualified CLIs for CLI Add-on Feature Templates.

# Restrictions for CLI Add-On Feature Templates

The following restrictions apply when using the CLI add-on feature templates:

- This feature is only supported on Cisco IOS XE Catalyst SD-WAN devices running Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or onwards.
- Only one CLI add-on template can be attached per device template.
- Ensure that you only use configuration commands as they appear in the output of the `show sdwan running-config` command. Before using a command in the CLI add-on feature template, verify the command by logging in and running it on the intended device.
- Unsupported commands in your configuration cause errors and results in a failure when pushing the configuration to the device. For example, "login local" is an unsupported command.

  For a release-wise list of commands qualified for use in the CLI add-on feature template, see Qualified CLI Commands for CLI Add-on Feature templates.

# Create a CLI Add-On Feature Template

To create a CLI add-on feature template, do the following:

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

3. From **Select Devices**, select the devices for which you are creating the template.
4. From **Select Template**, scroll down to the **OTHER TEMPLATES** section.

5. Click **CLI Add-On Template**.
6. In **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.
7. In **Description**, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.
8. In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file.
9. 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}}`.
10. Click **Save**.

    The new feature template is displayed in the Feature Template table.
11. To use the CLI add-on feature template, edit the device template as follows:
    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. Select the device template for which you want to add the CLI add-on feature template.
    d. Click **...**, and choose **Edit**.
    e. Scroll to **Additional Templates**.
    f. From **CLI Add-On Template**, select the CLI add-on feature template that you previously created.
    g. Click **Update**.

**Note** In Cisco IOS XE Catalyst SD-WAN Release 17.7.x, while creating a CLI template, if the following CLIs are visible in the template, then ensure that you manually delete the CLIs from the template before attaching the template to the device:

licensing config enable false

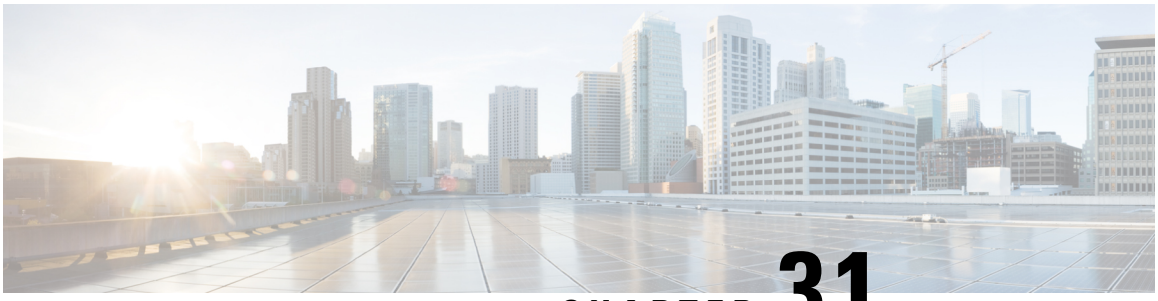
licensing config privacy hostname false

licensing config privacy version false

licensing config utility utility-enable false

# Qualified CLIs for CLI Add-On Feature Templates

For a release-wise list of CLI commands that are qualified for use in Cisco SD-WAN Manager CLI templates, see the Appendix in Cisco IOS XE SD-WAN Qualified Command Reference.



CHAPTER 31

# Cisco Catalyst SD-WAN EtherChannel

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 242: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Catalyst SD-WAN EtherChannel | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1 | This feature allows you to configure EtherChannels on Cisco IOS XE Catalyst SD-WAN devices on the service side.<br>An EtherChannel provides fault-tolerant high speed link, redundancy, and increased bandwidth between Cisco IOS XE Catalyst SD-WAN devices and other devices such as routers, switches, or servers connected in a network.<br>You can configure EtherChannels only using the CLI device templates and CLI add-on feature templates. |

| Feature Name | Release Information | Description |
|---|---|---|
| Support for EtherChannels on the Transport Side | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a<br>Cisco Catalyst SD-WAN Manager Release 20.13.1 | Adds support for configuring EtherChannels on the transport side of a Cisco IOS XE Catalyst SD-WAN device.<br>This feature also introduces support for aggregate EtherChannel Quality of Service (QoS) on the transport side.<br>By combining EtherChannel and QoS, you can optimize network utilization, enhance performance, and maintain quality for specific traffic types.<br>**Note** This feature has limited availability. |
| Support for Load Balancing for EtherChannels on the Transport Side | Cisco IOS XE Catalyst SD-WAN Release 17.14.1a<br>Cisco Catalyst SD-WAN Manager Release 20.14.1 | This feature adds the ability to configure load balancing for EtherChannels on the transport side for Cisco IOS XE Catalyst SD-WAN devices using the global configuration command **port-channel load-balance-hash-algo sdwan**. |

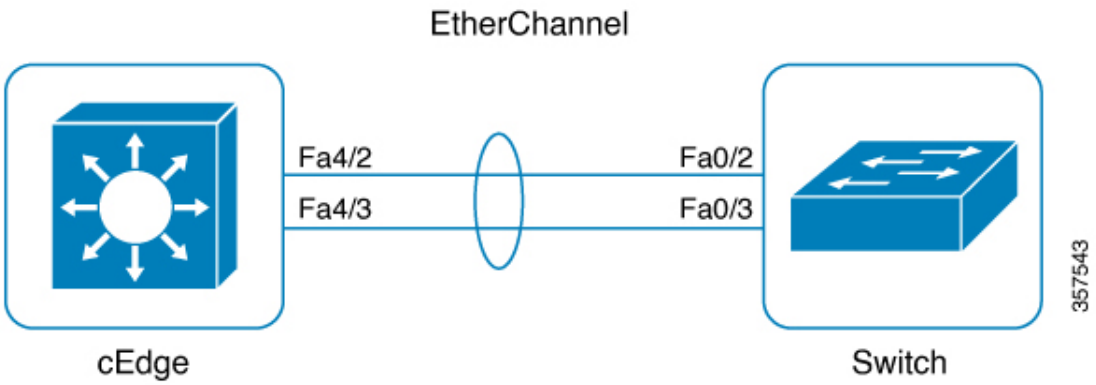

- Information About Cisco Catalyst SD-WAN EtherChannel, on page 890
- EtherChannels on the Service Side, on page 895
- EtherChannels on the Transport Side, on page 900
- Monitor Configured EtherChannel Using CLI, on page 903
- Aggregate EtherChannel Quality of Service, on page 904


# Information About Cisco Catalyst SD-WAN EtherChannel

An EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use the EtherChannel to increase bandwidth between the wiring closets and the data center, and also deploy it at any place in a network where bottlenecks are likely to occur. An EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, an EtherChannel redirects traffic from the failed link to the remaining links in the channel.

An EtherChannel comprises a channel group and a port-channel interface. The channel group binds physical ports to the port-channel interface. Configuration changes applied to the port-channel interface apply to all the physical ports bound together in the channel group.

*Figure 7: EtherChannel*




- Using EtherChannels in a network provides increased bandwidth and resilience.
  - Bandwidth: An EtherChannel allows multiple links to be combined into one logical link. Because an EtherChannel offers redundancy of links, you can configure EtherChannels to increase the speed in a network.
  - Resilience: An EtherChannel also provides network resilience. Even if a link within an EtherChannel fails, traffic that is previously carried over the failed link switches to the remaining links within the EtherChannel. Thus, EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links.
- The number of supported port channels differs based on the specific device model.
- The number of supported member interfaces for a port channel differs based on the specific device model.
- EtherChannel supports the following combinations:
  - Two active links
  - Active and passive links
  - Single member link
  - Loopback interface in bind or unbind mode to the port channel

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, EtherChannels configured on the transport side support the following:

- Control and management connections (DTLS, OMP) to Cisco Catalyst SD-WAN Manager, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Controller
- IPSEC tunnels for data traffic
- IPv4 forwarding
- L2 TLOC extension
- Explicit ACL (Access Control Lists)
- Implicit ACL on a port channel TLOC

- IPv4 static routing
- Loopback TLOC (ability to bind loopback to port channel)
- Port channel sub-interfaces
- Control policies on Cisco Catalyst SD-WAN Controller

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1, EtherChannels configured on the transport side support the following:

- IPv6 for EtherChannels, allowing for the transmission of IPv6 traffic across aggregated links.
- Handling traffic through Generic Routing Encapsulation (GRE) tunnels, facilitating the encapsulation of various network protocols.
- Advanced routing protocols such as OSPF and BGP over EtherChannels enables dynamic routing in Cisco Catalyst SD-WAN.
- NAT-DIA across EtherChannels, providing direct internet access by converting private IP addresses to public ones for efficient internet-bound traffic routing. For more information, see Configure NAT.

### EtherChannel in Cisco Catalyst SD-WAN

To create an EtherChannel, begin by configuring a port channel. A port channel is a logical interface on a Cisco IOS XE Catalyst SD-WAN device. After you create an EtherChannel, the configuration changes that are applied to the port-channel interface are also applied to all the physical ports assigned to the port-channel interface.

The maximum number of interfaces that can be combined into a single EtherChannel using LACP is eight, although the actual limit may depend on the specific model of the device.

You can configure an EtherChannel using one these methods:

- Link Aggregation Control Protocol (LACP) mode
- Static mode

  Use the LACP mode to configure an EtherChannel if it is supported on both ends of a device. If either of the device does not support LACP mode, use a static mode to configure an EtherChannel.

### LACP Mode

LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between the Ethernet ports.

This table shows the user-configurable EtherChannel LACP modes.

*Table 243: EtherChannel LACP Modes*

| Mode | Description |
|---|---|
| **active** | Places a port in an active negotiating state in which the port starts negotiations with other ports by sending LACP packets. |

| Mode | Description |
|---|---|
| **passive** | Places a port in a passive negotiating state in which the port responds to the packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets. |

Both the **active** and **passive** modes enable ports to negotiate with partner ports based on port speed.

Ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A port in the **active** mode can form an EtherChannel with another port that is in the **active** or **passive** mode.
- A port in the **passive** mode cannot form an EtherChannel with another port that is also in the **passive** mode because neither port starts LACP negotiation.

In addition to the standard LACP configuration, the following LACP-related commands are supported:

- **lacp min-bundle**
- **lacp max-bundle**
- **lacp system-priority**
- **lacp port-priority**
- **lacp fast-switchover**
- **lacp rate fast**

### Static Mode

You can manually create an EtherChannel by using the **interface port-channel** command in the global configuration mode. You then use the **channel-group interface** command in the global configuration mode to assign an interface to the EtherChannel. After you configure an EtherChannel, the configuration changes applied to the port-channel interface are applied to all the physical ports assigned to the port-channel interface. Unlike an LACP mode, in a static mode, no packets are sent for negotiations with the other ports. Instead, you must manually configure the ports as part of an EtherChannel.

Information related to LACP on port-channel interfaces can be obtained using the **show lacp** command. See show lacp.

## EtherChannel Load Balancing

An EtherChannel balances traffic load across the links in a channel. You can specify one of several different load-balancing modes. EtherChannels can use either dynamic flow-based load balancing or virtual LAN (VLAN) manual load balancing.

You can configure the load-balancing method globally for all the port channels or directly on specific port channels. The global configuration applies only to those port channels for which you have not explicitly configured load balancing. The port-channel configuration overrides the global configuration.

The following load-balancing methods are supported on Cisco IOS XE Catalyst SD-WAN devices:

- Flow-Based

VLAN-Based

**Flow-Based Load Balancing**

Flow-based load balancing is the default load-balancing method, and is enabled by default at the global level. Flow-based load balancing identifies different flows of traffic based on the key fields in the data packet. For example, IPv4 source and destination IP addresses can be used to identify a flow. The various data traffic flows are then mapped to the different member links of a port channel. After the mapping is done, the data traffic for a flow is transmitted through the assigned member link. The flow mapping is dynamic and changes when there is any change in the state of a member link to which a flow is assigned. The flow mapping is dynamic when member links are added or deleted.

**VLAN-Based Load Balancing**

VLAN-based load balancing allows you to configure static assignment of user traffic, as identified by a VLAN ID, to a given member link of an EtherChannel. You can manually assign VLAN subinterfaces to a primary and secondary link. This feature allows load balancing to downstream equipment regardless of vendor equipment capabilities, and provides failover protection by redirecting traffic to the secondary member link if the primary link fails. Member links are supported with up to 16 bundles per chassis.

### EtherChannels Load Balancing on the Transport Side of Cisco IOS XE Catalyst SD-WAN Devices

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1.

Load balancing for EtherChannels on the transport side is achieved by using the inner IP headers, which include the original source and destination IP addresses found in encapsulated packets. Cisco IOS XE Catalyst SD-WAN devices use a hash algorithm to analyze the inner IP addresses for distribution of network traffic across available paths.

Configure load balancing for EtherChannels on the transport side using the **port-channel load-balance-hash-algo sdwan** command. With load balancing configured, a router distributes network traffic among all available paths within the EtherChannel. By default, **sdwan** uses the inner packet source and destination IP address.

# Benefits of Cisco Catalyst SD-WAN EtherChannel

- Provides fault-tolerance. If any one of the links in an EtherChannel fail, the EtherChannel automatically redistributes traffic across the remaining links.
- Helps increase bandwidth between Cisco IOS XE Catalyst SD-WAN devices and other devices such as switches and servers that are connected in a network.

# EtherChannels on the Service Side

## Supported Devices for Cisco Catalyst SD-WAN EtherChannel on the Service Side

### Service Side

The following platforms support EtherChannel and also offer load balancing for EtherChannel on the service side:

- Cisco 4000 Series Integrated Services Routers
  - Cisco 4451-X Integrated Services Router
  - Cisco 4461 Integrated Services Router
  - Cisco 4431 Integrated Services Router
  - Cisco 4331 Integrated Services Router
  - Cisco 4351 Integrated Services Router
- Cisco ASR 1000 Series Aggregation Services Routers
  - Cisco ASR 1001-X Router
  - Cisco ASR 1006-X Router
  - Cisco ASR 1001-HX Router
  - Cisco ASR 1002-HX Router
  - Cisco ASR 1002-X Router
- Cisco Catalyst 8000V Edge Software
- Cisco Catalyst 8200 Router
- Cisco Catalyst 8300 Router
- Cisco Catalyst 8500 Series Edge Router

### Supported NIMs

The following NIMs are supported on Integrated Services Routers, for service side:

- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- SM-X-4x1G-1x10G
- SM-X-6X1G
- C-NIM-2T

- C-NIM-1X
- C-NIM-1M

**Note** Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the service side.

# Prerequisites for Cisco Catalyst SD-WAN EtherChannel on the Service Side

- All the LAN ports in each EtherChannel must be of the same speed.
- All the LAN ports must be configured on Layer 3 service-side ports.

# Restrictions for Cisco Catalyst SD-WAN EtherChannel on the Service Side

- The maximum number of port channel interfaces that a device can support varies, depending on the particular model of the device.
- You can configure EtherChannels on a device by using the CLI, or using only the CLI templates or CLI add-on feature templates in Cisco SD-WAN Manager.
- Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the service side.
- The EtherChannel Quality of Service (QoS) feature on port channels is not supported on the service side.
- The Aggregate EtherChannel QoS feature on port channels is not supported on the service side.
- An EtherChannel does not support Digital Signal Processor (DSP) farm services and voice services.
- Sub interfaces cannot be added as member of EtherChannel.

# Configure a Service-Side EtherChannel Using a CLI Template

In Cisco Catalyst SD-WAN Manager, you can configure EtherChannels on the service side using CLI templates. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

1. Configure a Layer 3 port channel.

```
config-transaction
 interface Port-channel channel-number
 ip address ip-address mask  <For IPv4 addressess>
 ipv6 address ipv6-address/prefix length <For IPv6 addressess>
 vrf forwarding vrf-value
```

2. Assign Interfaces to Layer 3 port channel with LACP active or passive options.

```
config-transaction
 interface GigabitEthernet slot/subslot/port
 no ip address
 channel-group port-channel-group-number mode {active passive}
 exit
```

Configure EtherChannel with LACP Paramaters.

```
config-transaction
 lacp system-priority priority
 interface GigabitEthernet slot/subslot/port
 lacp port-priority priority
```

3. Configure a Static EtherChannel.

```
config-transaction
 interface GigabitEthernet slot/subslot/port
 no ip address
 channel-group channel-group-number
```

This example shows how to configure a Layer 3 EtherChannel, and how to asssign two ports to channel 5 with the LACP mode as active and passive:

```
interface Port-channel5
 vrf forwarding 150
 ip address 11.0.0.1 255.255.255.0

interface Gigabitethernet 0/1/0
 no ip address
 channel-group 5 mode active

interface Gigabitethernet 0/1/2
 no ip address
 channel-group 5 mode passive
```

The following is a complete configuration example for creating an EtherChannel in static mode:

```
interface Port-channel2
 vrf forwarding 150
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
!

interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
interface GigabitEthernet2/1/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

# Configure Load Balancing for EtherChannels on the Service Side Using CLI Commands

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

### Enable Flow Based Load Balancing Per Port Channel

```
interface Port-channel channel-number
load-balancing flow
```

### Hash Algorithms for Flow-based Load Balancing

```
port-channel load-balance-hash-algo {dst-ip dst-mac src-dst-ip src-dst-mac
  src-dst-mixed-ip-port src-ip src-mac}
```

**Note** The default hash algorithm for flow-based load balancing is **src-dst-ip**.

**Note** The **Hash Algorithms For Flow-based Load Balancing** feature is supported only on Cisco Aggregation Services Routers platforms, where the hardware load-balancing for Etherchannel is supported. This command is not supported on Cisco Integrated Services Routers and Cisco Catalyst Router platforms.

This example shows a configuration where flow-based load balancing is configured on port channel 2 while the VLAN manual method is configured globally:

```
!
port-channel load-balancing vlan-manual

.
.
.
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
 load-balancing flow
!

interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
interface GigabitEthernet2/1/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

### Manual Traffic Distribution Based on VLAN ID

**port-channel load-balancing vlan-manual**

**Note** This command is available for configuration in the global configuration mode, and applies to all the port-channel configured on the device.

This example shows how the load-balancing configuration can be globally applied to define policies for handling traffic by using the **port-channel load-balancing** command.

```
port-channel load-balancing vlan-manual

!
interface Port-channel1
!
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
 secondary GigabitEthernet 1/2/1
 ip address 10.16.2.100 255.255.255.0
!
interface Port-channel1.200
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 10.16.3.200 255.255.255.0
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.16.4.300 255.255.255.0
 !
interface GigabitEthernet 1/1/1
 no ip address
 channel-group 1!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1
```

### Enable VLAN Load Balancing Per Port Channel on the Service Side

**interface Port-channel** *channel-number*
**load-balancing vlan**

Example of Configuring VLAN Load Balancing on the Service Side.

**interface Port-channel** *channel-number*
**interface GigabitEthernet** *slot/subslot/port*
**channel-group** *channel-group-number*
**interface GigabitEthernet** *slot/subslot/port*
**channel-group** *channel-group-number*
**interface Port-channel** *channel-number*
**load-balancing vlan**
**interface Port-channel** *channel-number*
**encapsulation dot1Q** *vlan_id* **primary** *interface1* **secondary***interface2*

**Note** Interface 1 and interface 2 must be member ports of a port channel when **encapsulation dot1q** is configured.

# EtherChannels on the Transport Side

## Supported Devices for Cisco Catalyst SD-WAN EtherChannel on the Transport Side

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the following platforms support EtherChannels on the transport side. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the following platforms support load balancing:

- Cisco 4000 Series Integrated Services Routers
  - Cisco 4461 Integrated Services Router
- Cisco ASR 1000 Series Aggregation Services Routers
  - Cisco ASR 1001-HX Router
  - Cisco ASR 1002-HX Router
- Cisco Catalyst 8300 Series Routers
- Cisco Catalyst 8500 Series Edge Routers

**Note** Starting with Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the load balancing configuration command **portchannel load-balance-hash-algo sdwan** is supported only on the Cisco 4461 Integrated Services Router and Cisco Catalyst 8300 Series routers.

## Prerequisites for Cisco Catalyst SD-WAN EtherChannel on the Transport Side

- All the member links in each EtherChannel must be of the same speed.
- All the member links must be configured on Layer 3 transport side ports.

## Restrictions for Cisco Catalyst SD-WAN EtherChannel on the Transport Side

- The maximum number of port channel interfaces that a device can support varies, depending on the particular model of the device.
- You can configure EtherChannels on a device by using the CLI, or using only the CLI templates or CLI add-on feature templates in Cisco SD-WAN Manager.
- Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the transport side.
- The Multichassis Link Aggregation Group (LAG), which involves different member links connecting to different switches, is not supported.
- The use of port channel on virtual devices such as Cisco Catalyst 8000V is not supported.

- Cisco IOS XE Catalyst SD-WAN Release 17.13.1a does not include support for an endpoint tracker on port-channel TLOCs.
- Platforms such as the Cisco Catalyst 8500 Series Edge Routers support multi-rate interfaces, allowing 1G SFP modules to be used in default 10G interfaces. Despite this, in the output of **show** commands, the interfaces appear as TenGigabitEthernet x/x/x. You can bundle the 1G SFP interfaces together to form a port channel.

# Configure a Transport Side EtherChannel Using a CLI Template

In Cisco Catalyst SD-WAN Manager, you can configure EtherChannels on the transport side using CLI templates. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

1. Configure a Layer 3 port channel.

```
interface Port-channel channel-number
ip address ip-address mask
ipv6 address ipv6-address/prefix-length
```

2. Assign Interfaces to a Layer 3 port channel with LACP active or passive options.

   a.
   ```
   interface GigabitEthernet slot/subslot/port
   no ip address
   channel-group channel-group-number mode {active passive}
   exit
   ```

   b. Configure EtherChannel with LACP Paramaters.

   ```
   lacp system-priority priority
   interface GigabitEthernet slot/subslot/port
   lacp port-priority priority
   ```

   c. Configure a static EtherChannel.

   ```
   interface GigabitEthernet slot/subslot/port
   no ip address
   channel-group channel-group-number
   ```

3. Configure tunnels.

```
interface Tunnel tunnel-number
ip unnumbered Port-channel channel-group-number
no ip redirects
tunnel source  Port-channel channel-group-number
tunnel mode sdwan
```

```
sdwan
 interface Port-channel channel-group-number
  tunnel-interface
   encapsulation {ipsec gre}
   color color-type
```

This example shows how to configure a Layer 3 EtherChannel, and how to assign two ports to channel 1 with the LACP mode as active and passive:

```
interface Port-channel1
ip address 10.48.48.15 255.255.255.0
ip ospf priority 0
ip ospf 65535 area 51
load-interval 30
no negotiation auto

interface GigabitEthernet0/0/0
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode active
end

interface GigabitEthernet0/0/4
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode passive
end
```

The following is a configuration example for creating an EtherChannel on the transport side.

```
interface Tunnel2
ip unnumbered Port-channel1
tunnel source Port-channel1
tunnel mode sdwan

interface Port-channel1
  tunnel-interface
   encapsulation ipsec
   color lte
```

# Configure Load Balancing for EtherChannels on the Transport Side Using CLI Commands

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

1. Enable load balancing for EtherChannels on the transport side.

   **port-channel load-balance-hash-algo sdwan**

**Note** In this command, **port-channel load-balance-hash-algo sdwan**, the **sdwan** option was added in Cisco IOS XE Catalyst SD-WAN Release 17.14.1a.

2. Configure the algorithm used for load balancing.

   To configure load balancing for IPv4 addresses, which is the default setting, use the following configuration:

   ```
   sdwan
   ip load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
   ```

   To configure load balancing for IPv6 addresses, use the following configuration:

   ```
   sdwan
   ipv6 load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
   ```

   - **src-dst-ip**: Balances traffic based on both source and destination IP addresses.
   - **ip-and-ports**: Balances traffic using a combination of IP addresses and port numbers.
   - **src-ip-only**: Balances traffic based solely on the source IP address.

   The **ip load-sharing algorithm** command is a global configuration that applies to all Cisco Catalyst SD-WAN tunnels. Changing the algorithm with options such as **src-dst-ip** or **src-dst-mixed-ip-port** affects the load-sharing mechanism for other Cisco Catalyst SD-WAN tunnel traffic as well.

   When you configure a port channel on both the service side and the transport side, using the **port-channel load-balance-hash-algo sdwan** command applies load balancing to the transport side. For the Service side, the port channel defaults to the **src-dst-ip** load balancing mode. For more information, see Configure Network Interfaces.

   To change the load-balancing algorithm for the Service side when a Transport-VPN port-channel is also configured, use the **port-channel load-balance-hash-algo** command. This command allow you to switch from the default **sdwan** mode to alternative modes such as **dst-ip**, **dst-mac**, **src-dst-ip**, **src-dst-mac**, **src-dst-mixed-ip-port**, **src-ip**, or **src-mac**. However, this change disables the SD-WAN-based load balancing for the transport side.

Here's the complete configuration for enabling load balancing and apply the desired hash algorithm for traffic distribution on the transport side of Cisco IOS XE Catalyst SD-WAN devices.

```
port-channel load-balance-hash-algo sdwan
sdwan
 ip load-sharing algorithm src-dst-ip

port-channel load-balance-hash-algo sdwan
sdwan
 ipv6 load-sharing algorithm src-dst-ip
```

# Monitor Configured EtherChannel Using CLI

### Example 1

The following is a sample output from the **show etherchannel summary** command. This example shows summary for each channel group.

```
Device# show etherchannel summary

Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
```

```
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

**Example 2**

The following is a sample output from the **show etherchannel load-balancing** command. This example displays the load-balancing method that is applied to each port channel.

```
Device# show etherchannel load-balancing

EtherChannel Load-Balancing Method:
Global LB Method: flow-based
LB Algo type: SDWAN Inner packet LB

 Port-Channel:                       LB Method
    Port-channel1                   :  flow-based (SDWAN Inner packet LB)
```

# Aggregate EtherChannel Quality of Service

The Aggregate EtherChannel Quality of Service (QoS) feature improves the quality of service by effectively managing various network parameters, such as delay, jitter (or delay variation), bandwidth, and packet loss. Its primary function is to offer improved services for specific types of network traffic. The feature allows the application of an aggregate egress-queuing policy-map on the main or sub-interface of a port channel. Furthermore, it facilitates QoS support on the aggregate port channel's main interface on Cisco IOS XE Catalyst SD-WAN devices.

## Prerequisites for Aggregate EtherChannel Quality of Service

- Identify aggregate port channel interfaces before creating them using the **platform qos port-channel-aggregate** command.
- In a port channel, all member links must be of the same speed.

## Restrictions for Aggregate EtherChannel Quality of Service

- The aggregate port channel can support four member links and eight aggregate port channel interfaces.

- You can apply a policy map to the aggregate a port channel's main interface or sub-interface only. Member link QoS is not supported.
- You cannot spontaneously convert port channels to and from the aggregate status. You must delete the interface port-channel from the configurations before adding or removing the matching **platform qos port-channel-aggregate** command.
- QoS applications which are used to manage, prioritize and control the behavior of data transmission over a network are not supported on port channel member links.

  QoS policies applied to aggregate port channel main interfaces and port channel sub-interfaces are not supported.
- When you enable aggregate QoS, it is not possible to directly modify a channel group on a member link. To make changes, the old channel group needs to be removed and the new one must be added. First push one template to remove the old member link and port channel configuration, then another template to add the new configuration.

# Configure Aggregate EtherChannel Quality of Service Using a CLI Template

In Cisco Catalyst SD-WAN Manager, you can configure aggregate EtherChannel QoS using the CLI templates. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

1. Create the aggregated port channel.

```
platform qos port-channel-aggregate port-channel-number
 interface Port-channel channel-number
 no shutdown
 ip address ip-address mask
```

2. Assign member links to port channel.

```
interface GigabitEthernet slot/subslot/port
 no negotiation auto
 channel-group channel-group-number mode {active passive}
 exit
```

3. Configure tunnels.

```
interface Tunnel tunnel-number
 no shutdown
 ip unnumbered port-channel-interface
 tunnel source port-channel-interface
 tunnel mode sdwan

sdwan
 interfacechannel-group-number
  tunnel-interface
```

```
encapsulation ipsec
color public-internet
```

4. Configure QoS.

```
interface channel-group-number
 service-policy output pre-defined qos policy-map
```

Here's the complete configuration example for configuring aggregate EtherChannel QoS.

```
!
class-map match-any Best-Effort
 match qos-group 2
!
class-map match-any Bulk
 match qos-group 3
!
class-map match-any Business
 match qos-group 1
!
class-map match-any Critical
 match qos-group 0
!
policy-map qos_template
 class Critical
  police rate percent 15
  !
  priority level 1
 !
 class Business
  bandwidth remaining percent 55
 !
 class Best-Effort
  bandwidth remaining percent 10
 !
 class Bulk
  bandwidth remaining percent 20
 !
!
policy-map shape_Port-channel1
 class class-default
  service-policy qos_template
  shape average 100000000
 !
!
interface TenGigabitEthernet0/1/6
 no shutdown
 no negotiation auto
 channel-group 1 mode active
 lacp rate fast
exit
interface TenGigabitEthernet0/1/7
 no shutdown
 no negotiation auto
 channel-group 1 mode active
 lacp rate fast
exit
interface Port-channel1
 no shutdown
 ip address 10.1.15.15 255.255.255.0
 ipv6 nd ra suppress all
 service-policy output shape_Port-channel1
```

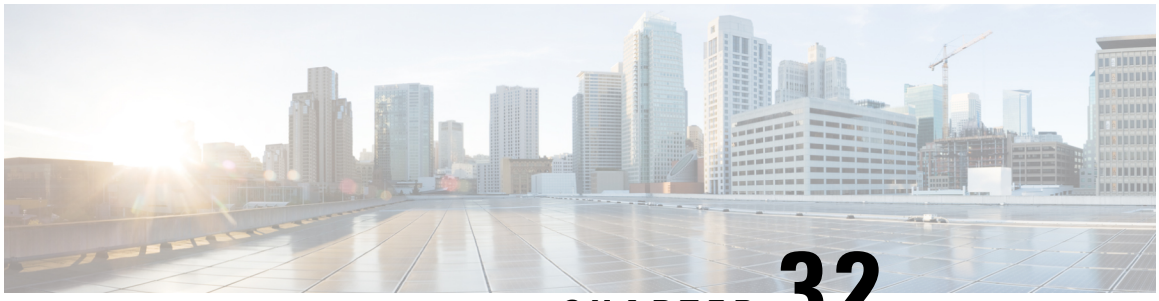
```
exit
interface Tunnel1
 no shutdown
 ip unnumbered Port-channel1
 tunnel source Port-channel1
 tunnel mode sdwan
exit
!
sdwan
 interface Port-channel1
  tunnel-interface
   encapsulation ipsec
   color lte
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no 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
 exit
```

# Verify Aggregate EtherChannel Quality of Service

To view QoS issues on a port channel interface, use the **show policy-map interface Port-channel** command.

```
Device# show policy-map interface Port-channel 1
Port-channel1

  Service-policy output: shape_Port-channel1

    Class-map: class-default (match-any)
      121 packets, 20797 bytes
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 121/20797
      shape (average) cir 100000000, bc 400000, be 400000
      target shape rate 100000000

      Service-policy : qos_template

        queue stats for all priority classes:
          Queueing
          priority level 1
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 121/20797

        Class-map: Critical (match-any)
          121 packets, 20797 bytes
          5 minute offered rate 2000 bps, drop rate 0000 bps
          Match: qos-group 0
          police:
              rate 15 %
```

```
      rate 15000000 bps, burst 468750 bytes
    conformed 121 packets, 20797 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 2000 bps, exceeded 0000 bps
  Priority: Strict, b/w exceed drops: 0

  Priority Level: 1

Class-map: Business (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 1
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 55%

Class-map: Best-Effort (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 2
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 10%

Class-map: Bulk (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 3
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 20%

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any

  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```



CHAPTER 32

# 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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.


- Cisco Catalyst SD-WAN Multitenancy, on page 910
- Information About Cisco Catalyst SD-WAN Multitenancy, on page 910
- Supported Devices and Controller Specifications, on page 914
- Restrictions, on page 916
- Initial Setup for Multitenancy, on page 917
- Expand a Multitenant Deployment to Support More Tenants and Tenant Devices, on page 925
- Manage Tenants, on page 927
- Cisco SD-WAN Manager Dashboard for Multitenancy, on page 932
- Manage Tenant WAN Edge Devices, on page 938
- Tenant-Specific Policies on Cisco SD-WAN Controller, on page 939
- Manage Tenant Data, on page 939
- View OMP Statistics per Tenant on a Cisco SD-WAN Controller, on page 943
- View Tenants Associated with a Cisco SD-WAN Controller, on page 944
- Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment, on page 944
- Migrate a Tenant from a Multitenant Cisco Catalyst SD-WAN Overlay to Single-Tenant Cisco Catalyst SD-WAN Deployment , on page 947
- Migrate Multitenant Cisco Catalyst SD-WAN Overlay, on page 951
- Upgrade Cisco Catalyst SD-WAN Controller and Edge Device Software, on page 954
- Multitenant Cisco SD-WAN Manager: Disaster Recovery, on page 955
- Multitenant Cisco SD-WAN Manager: Disaster Recovery in an Overlay Network with Virtual Routers, on page 960
- Multitenant Cisco SD-WAN Manager: Disaster Recovery After a Failed Data Center Becomes Operational, on page 967

• Replace Faulty Cisco SD-WAN Controller, on page 972
• RADIUS and TACACS Support for Multitenancy, on page 973

# Cisco Catalyst SD-WAN Multitenancy

*Table 244: 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<br>Cisco Catalyst SD-WAN Manager Release 20.12.1 | This feature is enhanced to support consistent user experience in tenant and service providers dashboard.<br>The Cisco Catalyst SD-WAN Manager dashboard provides visibility into the available resources on shared devices. |
| Migration of a Tenant from a Multitenant Overlay to a Single-Tenant Deployment | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a<br>Cisco Catalyst SD-WAN Manager Release 20.13.1 | This feature supports the migration of a tenant from a multitenant overlay to a single-tenant deployment. To migrate a tenant between two Cisco Catalyst SD-WAN deployments, move the tenant configurations, statistical data, and WAN edge devices from one deployment to another. |
| Multitenancy Support for Cisco Catalyst Cellular Gateways | Cisco IOS CG Release 17.14.1<br>Cisco Catalyst SD-WAN Control Components Release 20.14.1 | Added multitenancy support for Cisco Catalyst Cellular Gateways. |

# Information About Cisco Catalyst SD-WAN Multitenancy

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. The tenants share the same set of underlying Cisco SD-WAN controllers: Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Controller. The tenant data is logically isolated on these shared controllers.

The service provider accesses Cisco SD-WAN Manager using a domain name mapped to the IP address of a Cisco SD-WAN Manager cluster and manages the multitenant deployment. Each tenant is provided a subdomain to access a tenant-specific Cisco SD-WAN Manager view and manage the tenant deployment. For example, a service provider using the domain name `managed-sp.com`, can assign tenants Customer1 and Customer2 the subdomains `customer1.managed-sp.com` and `customer2.managed-sp.com` and manage them on the same set of Cisco SD-WAN controllers, instead of providing each customer a single-tenant setup with a dedicated set of Cisco SD-WAN controllers.

Following are the key features of Cisco Catalyst SD-WAN multitenancy:

- Full enterprise multitenancy: Cisco Catalyst SD-WAN supports multitenancy and offers enterprises the flexibility of segregated roles such as service provider and tenants. Service providers can use multitenancy to provide Cisco Catalyst SD-WAN service offerings to their customers.
- Multi-tenant Cisco SD-WAN Manager
- Multi-tenant Cisco Catalyst SD-WAN Validators
- Multi-tenant Cisco Catalyst SD-WAN Controllers
- Tenant-specific WAN Edge Devices
- Overlapping VPN numbers: A particular VPN or a set of common VPNs is assigned to a specific tenant, with their own configurations and monitoring dashboard environment. These VPN numbers can overlap where they are used by other tenants.
- On-prem and cloud deployment models: Cisco Catalyst SD-WAN controllers can be deployed in an organization data center on servers running the VMware ESXi 6.7 or later, or the Kernel-based Virtual Machine (KVM) hypervisor. Cisco Catalyst SD-WAN controllers can also be hosted on Amazon Web Services (AWS) servers by Cisco CloudOps.
- Tenant-specific Cisco SD-WAN Analytics: Cisco SD-WAN Analytics is a cloud-based service that offers insights into the performance of applications and the underlying SD-WAN network infrastructure. Each tenant can obtain Cisco SD-WAN Analytics insights for their overlay network by requesting a tenant-specific Cisco SD-WAN Analytics instance and enabling data collection on Cisco SD-WAN Manager. The service provider must enable cloud services on Cisco SD-WAN Manager in the provider view to facilitate the onboarding of the Cisco SD-WAN Analytics instance for the tenant overlay network.

**Note** Starting from Cisco SD-WAN Manager Release 20.13.1, a single node multitenancy is supported. Expand a single node cluster into a multitenant deployment.

### Multi-tenant Cisco SD-WAN Manager

Cisco SD-WAN Manager is deployed and configured by the service provider. The provider enables multitenancy and creates a Cisco SD-WAN Manager cluster to serve tenants. Only the provider can access a Cisco SD-WAN Manager instance through the SSH terminal.

Cisco SD-WAN Manager offers service providers an overall view of the SD-WAN multi-tenant deployment and allows a provider to manage the shared Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller devices. Cisco SD-WAN Manager also allows service providers to monitor and manage the deployments of each tenant.

Cisco SD-WAN Manager allows tenants to monitor and manage their deployment. Through Cisco SD-WAN Manager, tenants can deploy and configure WAN edge devices. Tenants can also configure custom policies on assigned Cisco Catalyst SD-WAN Controllers.

### Multi-tenant Cisco Catalyst SD-WAN Validators

Cisco Catalyst SD-WAN Validators are deployed and configured by the service provider. Only the provider can access a Cisco Catalyst SD-WAN Validator through the SSH terminal.

Cisco Catalyst SD-WAN Validators serve WAN edge devices of multiple tenants as the devices are added to the overlay network.

### Multi-tenant Cisco Catalyst SD-WAN Controllers

Cisco Catalyst SD-WAN Controllers are deployed by the service provider. Only the provider can create and attach device and feature templates to Cisco Catalyst SD-WAN Controllers, and can access a Cisco Catalyst SD-WAN Controller through the SSH terminal.

- When a tenant is created, Cisco SD-WAN Manager assigns two Cisco Catalyst SD-WAN Controllers for the tenant. The Cisco Catalyst SD-WAN Controllers form an active-active cluster.

  Each tenant is assigned only two Cisco Catalyst SD-WAN Controllers. Before a tenant is created, two Cisco Catalyst SD-WAN Controllers must be available to serve the tenant.

- When more than one pair of Cisco Catalyst SD-WAN Controllers are available to serve a tenant, Cisco SD-WAN Manager assigns to the tenant the pair of Cisco Catalyst SD-WAN Controllers connected to the lowest number of forecast devices. If two pairs of Cisco SD-WAN Controllers are connected to the same number of devices, Cisco SD-WAN Manager assigns to the tenant the pair of Cisco SD-WAN Controllers serving the lowest number of tenants.

- From Cisco vManage Release 20.9.1, 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 Controllers, if necessary. For more information, see Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers.

- Each pair of Cisco Catalyst SD-WAN Controllers can serve a maximum of 24 tenants.

- Tenants can configure custom policies on the Cisco Catalyst SD-WAN Controllers assigned to them. Cisco SD-WAN Manager notifies the Cisco Catalyst SD-WAN Controllers to pull the policy templates. Cisco Catalyst SD-WAN Controllers pull the templates and deploy the policy configuration for the specific tenant.

- Only the provider can view events, audit logs, and OMP alarms for a Cisco Catalyst SD-WAN Controller on Cisco SD-WAN Manager.

### Tenant-Specific WAN Edge Devices

A tenant or the provider acting on behalf of a tenant can add WAN edge devices to the tenant network, configure the devices, and remove the devices from the tenant network, or access the device through the SSH terminal.

A provider can manage the WAN edge devices only from provider-as-tenant view. In the provider view, Cisco SD-WAN Manager does not show any WAN edge device information.

Cisco SD-WAN Manager reports WAN edge device events, logs, and alarms only in the Tenant Role and the provider-as-tenant views.

# User Roles in Multitenant Environment

A multi-tenant environment includes the service provider and tenant roles. Each role has distinct privileges, views, and functions.

### Provider Role

The provider role entitles system-wide administrative privileges. A user with the provider role has the default username **admin**. The provider user can access Cisco SD-WAN Manager using the domain name of the service

provider or by using the Cisco SD-WAN ManagerIP address. When using a domain name, the domain name has the format `https://managed-sp.com`.

The **admin** user is part of the user group **netadmin**. Users in this group are permitted to perform all operations on the controllers and the WAN edge devices of the tenants. You can add additional users to the **netadmin** group.

You cannot modify the privileges of the **netadmin** group. On Cisco SD-WAN Manager, you can view the privileges of the user group from the **Administration** > **Manage Users** > **User Groups** page.

**Note** When you create a new provider user in Cisco SD-WAN Manager, including a **netadmin** user, by default, the user is not allowed SSH access to the Cisco SD-WAN Manager VM. To enable SSH access, configure SSH authentication using a AAA template and push the template to Cisco SD-WAN Manager. For more information on enabling SSH authentication, see SSH Authentication using Cisco SD-WAN Manager on Cisco IOS XE Catalyst SD-WAN Devices.

For more information about configuring users and user groups, see Configure User Access and Authentication.

Cisco SD-WAN Manager offers two views to a provider:

- **Provider View**

  When a provider user logs in to multi-tenant Cisco SD-WAN Manager as **admin** or another **netadmin** user, Cisco SD-WAN Manager presents the provider view and displays the provider dashboard.

  You can perform the following functions from the provider view:

  - Provision and manage Cisco SD-WAN Manager, Cisco SD-WAN Validators and Cisco SD-WAN Controllers.
  - Add, modify, or delete tenants.
  - Monitor the overlay network.

- **Provider-as-Tenant View**

  When a provider user selects a specific tenant from the **Select Tenant** drop-down list at the top of the provider dashboard, Cisco SD-WAN Manager presents the provider-as-tenant view and displays the tenant dashboard for the selected tenant. The provider user has the same view of Cisco SD-WAN Manager as a tenant user would when logged in as **tenantadmin**. From this view, the provider can manage the tenant deployment on behalf of the tenant.

  In the provider dashboard, a table of tenants presents a status summary for each tenant. A provider user can also launch the provider-as-tenant view by clicking on a tenant name in this table.

### Tenant Role

The tenant role entitles tenant administrative privileges. A user with the tenant role has the default username **tenantadmin**. The default password is **Cisco#123@Viptela**. We recommend that you change the default password on first login. For information on changing the default password, see Hardware and Software Installation.

The **tenantadmin** user is part of the user group **tenantadmin**. Users in this group are permitted to perform all operations on the WAN edge devices of the tenants. You can add additional users to the **tenantadmin** group.

You cannot modify the privileges of the **tenantadmin** group. On Cisco SD-WAN Manager, you can view the privileges of the user group from the **Administration** > **Manage Users** > **User Groups** page.

For more information about configuring users and user groups, see Configure User Access and Authentication.

A tenant user can log in to Cisco SD-WAN Manager using a dedicated URL and the default username **tenantadmin**. For example, the dedicated URL of a tenant could be `https://customer1.managed-sp.com` for a provider using the domain name `https://managed-sp.com`. When the user logs in, Cisco SD-WAN Manager presents the tenant view and displays the tenant dashboard.

**Tip** If you cannot access the dedicated tenant URL, update the subdomain details in the `/etc/hosts` file on the local machine. Alternatively, if you use an external DNS server, add a DNS entry for the tenant subdomain.

A tenant user with administrative privileges can perform the following functions:

- Provision and manage tenant routers
- Monitor overlay network of the tenant
- Create custom policies on the assigned Cisco SD-WAN Controller
- Upgrade the software on the tenant routers.

# Supported Devices and Controller Specifications

The following Cisco Catalyst SD-WAN edge devices support multitenancy.

***Table 245: Supported Devices***

| Platform | Device Models |
|---|---|
| Cisco IOS XE Catalyst SD-WAN device | • Cisco ASR 1000 Series Aggregation Services Routers<br>• Cisco ISR 1000 Series Integrated Services Routers<br>• Cisco ISR 4000 Series Integrated Services Routers<br>• Cisco Catalyst 8200 Series Edge Platforms<br>• Cisco Catalyst 8300 Series Edge Platforms<br>• Cisco Catalyst 8500 Series Edge Platforms<br>• Cisco Catalyst 8000V Edge Software<br>• Cisco ENCS Platforms |

| Platform | Device Models |
|---|---|
| Cisco Catalyst Cellular Gateways | (From Cisco IOS CG Release 17.14.1 and Cisco Catalyst SD-WAN Control Components Release 20.14.1)<br>• CG418-E<br>• CG522-E |

The following hypervisors are supported for multitenancy:

- VMware ESXi 6.7 or later
- KVM
- AWS (cloud-hosted and managed by Cisco CloudOps)
- Microsoft Azure (cloud-hosted and managed by Cisco CloudOps)

From Cisco vManage Release 20.6.1, a multitenant Cisco SD-WAN Manager instance can have one of the following three personas. The personas enable a predefined set of services on the Cisco SD-WAN Manager instance.

***Table 246: Cisco SD-WAN Manager Personas***

| Persona | Services |
|---|---|
| Compute+Data | Cluster Oracle, Service Proxy, Messaging Service, Coordination Service, Configuration Database, Data Collection Agent, Statistics Database, and Application Server |
| Data | Cluster Oracle, Service Proxy, Application Server, Data Collection Agent, and Statistics Database |
| Compute | Cluster Oracle, Service Proxy, Messaging Service, Coordination Service, Configuration Database, and Application Server |

The supported hardware specifications for the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and the Cisco SD-WAN Controllers are as follows:

### Hardware Specifications to Support 50 Tenants and 1000 Devices

For more information on supported hardware specifications for the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

### Hardware Specifications to Support 75 Tenants and 2500 Devices

For more information on supported hardware specifications for the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

### Hardware Specifications to Support 100 Tenants and 5000 Devices

For more information on supported hardware specifications for the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

### Hardware Specifications to Support 150 Tenants and 7500 Devices

For more information on supported hardware specifications for the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

# Restrictions

- Do not use a user-configured system IP address to connect to a device through SSH. Instead, use the IP address of the `vmanage_system` interface; this IP address is assigned by Cisco SD-WAN Manager.

  To find the IP address of the `vmanage_system` interface, use one of the following methods:

  - Launch the device SSH terminal from Cisco SD-WAN Manager and find the `vmanage_system` IP address from the first line of the log-in prompt.
  - Run the **show interface description** command and find the `vmanage_system` IP address from the command output.

- If you add a second tenant immediately after adding a tenant, Cisco SD-WAN Manager adds them sequentially, and not in parallel.
- 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**.
- For Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and earlier releases, single node Cisco SD-WAN Manager is not supported on a multitenant deployment. A minimum of 3-Node Cisco SD-WAN Manager cluster is required for a multitenant deployment.
- When a Cisco SD-WAN Controller or Cisco SD-WAN Validator upgrade is in progress, upgrade of tenant edge devices is not supported.

### Restrictions for Migration of a Tenant from a Multitenant Overlay to a Single-Tenant Deployment

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

- Change in the tenant organization name is not supported when the tenant moves from the Cisco Catalyst SD-WAN source to destination deployment.
- Tenant migration with multitenant WAN edge devices is not supported.
- Data traffic loss is expected during migration as devices are migrating from one set of Cisco SD-WAN Controllers to another.
- All user passwords are set to the default Cisco password on the destination overlay. The default password is **Cisco#123@Viptela**.

- Statistical data of the tenant that can be relearned by destination Cisco SD-WAN Manager is not migrated.
- The migration procedure does not support multiple imports on the same destination Cisco SD-WAN Manager. Reinitialize the destination Cisco SD-WAN Manager to allow import again.

# Initial Setup for Multitenancy

### Prerequisites

- Download and install software versions as recommended in the following table:

***Table 247: Minimum Software Prerequisites for Cisco Catalyst SD-WAN Multitenancy***

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.6.1 |
| Cisco SD-WAN Validator | Cisco SD-WAN Release 20.6.1 |
| Cisco SD-WAN Controller | Cisco SD-WAN Release 20.6.1 |
| Cisco IOS XE Catalyst SD-WAN Device | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a |

A configuration in which one or more controllers, or WAN edge devices, are running software versions earlier than those mentioned in the table above is not supported.

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

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

- Follow the recommended hardware specifications in the *Supported Devices and Controller Specifications* section of this document.
- Log in to Cisco SD-WAN Manager as the provider **admin** user.

1. Create Cisco SD-WAN Manager cluster.
   a. To support 50 tenants and 1000 devices across all tenants, Create a 3-Node Cisco SD-WAN Manager Multitenant Cluster.
   b. To support 100 tenants and 5000 devices across all tenants, Create a 6-Node Cisco SD-WAN Manager Multitenant Cluster.
   c. From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, Create a 6-Node Cisco SD-WAN Manager Multitenant Cluster.
2. Create and configure Cisco SD-WAN Validator instances. See Deploy Cisco SD-WAN Validator.

While configuring Cisco SD-WAN Validator instances, configure the service provider organization name (`sp-organization-name`) and the organization name (`organization-name`). See Configure Organization Name in Cisco SD-WAN Validator.

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

3. Create Cisco SD-WAN Controller instances. See Deploy the Cisco SD-WAN Controller.
   - To support 50 tenants and 1000 devices across all tenants, deploy 6 Cisco SD-WAN Controller instances.
   - To support 100 tenants and 5000 devices across all tenants, deploy 10 Cisco SD-WAN Controller.
   - From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy 16 Cisco SD-WAN Controllers.

   a. Add Cisco SD-WAN Controller to the overlay network.

4. Onboard new tenants. See Add a New Tenant, on page 928.

# Create a 3-Node Cisco SD-WAN Manager Multitenant Cluster

1. Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.
2. Create three Cisco SD-WAN Manager instances (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

**Important**

- Deploy Cisco SD-WAN Manager servers having the hardware specifications in the table *Hardware Specifications to Support 50 Tenants and 1000 Devices* from the *Supported Devices and Controller Specifications* section of this document.
- Choose the **Compute+Data** persona for each Cisco SD-WAN Manager instance.

3. Complete the following operations on vManage1:

   a. Configure the following using the CLI:
      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)
      - Organization-name
      - Cisco SD-WAN Validator IP address
      - VPN 0 Transport/Tunnel interface
      - VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
      - VPN 512 Management interface

**Note** Configure only one default route in VPN 0.

**b.** Enable Multitenancy on Cisco SD-WAN Manager, on page 922.

**c.** (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

**d.** Complete the following through the Cisco SD-WAN Manager:

1. Generate a Certificate Signing Request
2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.

**e.** Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

Before proceeding to the next step, ensure that the **Manager IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

**4.** Complete the following operations on vManage2 and vManage 3:

**Important** Do not enable multitenancy on vManage2 and vManage3.

**a.** Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface

**b.** (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

**c.** Complete the following through the Cisco SD-WAN Manager:

1. Generate a Certificate Signing Request
2. After Symantec or your enterprise root CA has signed the certificates, install signed certificate.

d. Log in to the Cisco SD-WAN Manager Web Application Server.

e. Ping the OOB interfaces on the other two Cisco SD-WAN Manager instances and ensure they are reachable.

f. Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

Before proceeding to the next step, ensure that the **Manager IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

5. Log in to the vManage1 GUI and add vManage2 to the cluster.

vManage2 reboots before being added to the cluster.

While vManage2 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage2 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage2 to the cluster.

When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both vManage1 and vManage2, and their node personas.

6. Repeat **Step 5** and add vManage3 to the cluster.

**Note** After rebooting, you have to select persona (non-cloud setup) from CLI and services starts running on the node according to the selected persona.

# Create a 6-Node Cisco SD-WAN Manager Multitenant Cluster

1. Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.
2. Create six Cisco SD-WAN Manager instances by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

**Important**

- To support 100 tenants and 5000 devices across all tenants, deploy Cisco SD-WAN Manager servers having the hardware specifications in the table *Hardware Specifications to Support 100 Tenants and 5000 Devices* from the *Supported Devices and Controller Specifications* section of this document.

  From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy Cisco SD-WAN Manager servers having the hardware specifications in the table *Hardware Specifications to Support 150 Tenants and 7500 Devices* from the *Supported Devices and Controller Specifications* section of this document.

- Choose the **Compute+Data** persona for three Cisco SD-WAN Manager instances (say vManage1, vManange2, and vManage 3). Choose the **Data** persona for the other three Cisco SD-WAN Manager instances (say vManage4, vManage5, and vManage6).

3. Complete the following operations on vManage1:
   a. Configure the following using the CLI:
      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)
      - Organization-name
      - Cisco SD-WAN Validator IP address
      - VPN 0 Transport/Tunnel interface
      - VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
      - VPN 512 Management interface

**Note** Configure only one default route in VPN 0.

   b. Enable Multitenancy on Cisco SD-WAN Manager, on page 922.
   c. (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

   d. Complete the following through the Cisco SD-WAN Manager:
      1. Generate a Certificate Signing Request
      2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.
   e. Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

      Before proceeding to the next step, ensure that the **Manager IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

4. Complete the following operations on vManage2 through vManage6:

**Important** Do not enable multitenancy on vManage2 through vManage6.

   a. Configure the following using the CLI:
      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)

- Organization-name
- Cisco SD-WAN Validator IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface

**b.** (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

**c.** Complete the following through the Cisco SD-WAN Manager:

1. Generate a Certificate Signing Request
2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.

**d.** Log in to the Cisco SD-WAN Manager Web Application Server.

**e.** Ping the OOB interfaces on the other Cisco SD-WAN Manager instances and ensure they are reachable.

**f.** Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

Before proceeding to the next step, ensure that the **Manager IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

**5.** Log in to the vManage1 GUI and add vManage2 to the cluster.

vManage2 reboots before being added to the cluster.

While vManage2 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage2 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage2 to the cluster.

When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both vManage1 and vManage2, and their node personas.

**6.** Repeat **Step 5** and add vManage3 through vManage6 to the cluster.

# 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** > **Tenancy Mode**. If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.
3. In the **Tenancy** field, click **Multitenant**.
4. In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).
5. Enter a **Cluster Id** (for example, cluster-1 or 123456).
6. Click **Save**. If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, 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

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**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

4. Click **Add Controller**.
5. In the **Add Controller** dialog box, do the following:
   a. In the **Controller 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 **Validator 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 **Manager Mode** by attaching a template to the device.

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

       For more information on configuration using CLI template, see Device Configuration-Based CLI 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 **Manager Mode**. The new Cisco SD-WAN Controller is ready to be used in your mutitenant deployment.

# Expand a Multitenant Deployment to Support More Tenants and Tenant Devices

As a service provider, suppose you have deployed a C to the overlay to support up to 100 tenants and 5000 devices. From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, you can expand the Cisco SD-WAN Manager cluster and add additional Cisco SD-WAN Controllers to the overlay to support up to 150 tenants and 7500 devices.

### Prerequisites

A multitenant Cisco Catalyst SD-WAN overlay that supports up to 50 tenants and 1000 devices, deployed according to the steps outlined in the *Initial Setup for Multitenancy* section of this document.

1. Expand a 3-Node Cluster to a 6-node Cluster.
2. To support up to 100 tenants and 5000 devices, you must have 10 Cisco SD-WAN Controllers in the overlay. So, deploy 4 Cisco SD-WAN Controllers in addition to the 6 existing Cisco SD-WAN Controllers in the overlay.

   To support up to 150 tenants and 7500 devices, you must have 16 Cisco SD-WAN Controllers in the overlay. So, deploy 10 Cisco SD-WAN Controllers in addition to the 6 existing Cisco SD-WAN Controllers in the overlay.

   a. Create Cisco SD-WAN Controller instances. See Deploy the Cisco SD-WAN Controller.

   b. Add Cisco SD-WAN Controller to the overlay network.

You can now add more tenants or allow your existing tenants to add more devices subject to the relevant limits.

**Note** Starting from Cisco SD-WAN Manager Release 20.13.1, you can expand a single node cluster into 3 or 6 node clusters.

# Expand a 3-Node Cluster to a 6-node Cluster

**Note** You can only expand a 3-node Cisco SD-WAN Manager cluster to a 6-node Cisco SD-WAN Manager cluster. Expansion of the 3-node cluster to other cluster sizes is not supported.

1. To support 100 tenants and 5000 devices: Upgrade the three Cisco SD-WAN Manager servers in the existing 3-node cluster to the hardware specifications in the table *Hardware Specifications to Support 100 Tenants and 5000 Devices* from the *Supported Devices and Controller Specifications* section of this document.

   From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices: Upgrade the three Cisco SD-WAN Manager servers in the existing 3-node cluster to the hardware

specifications in the table *Hardware Specifications to Support 150 Tenants and 7500 Devices* from the *Supported Devices and Controller Specifications* section of this document.

2. Download the Cisco vManage Release 20.6.1 or a later release software image from Cisco Software Download.
3. Create three Cisco SD-WAN Manager instances (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

**Important**

- Deploy Cisco SD-WAN Manager servers having the hardware specifications in the table *Hardware Specifications to Support 100 Tenants and 5000 Devices* from the *Supported Devices and Controller Specifications* section of this document.

  From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices, deploy Cisco SD-WAN Manager servers having the hardware specifications in the table *Hardware Specifications to Support 150 Tenants and 7500 Devices* from the *Supported Devices and Controller Specifications* section of this document.

- Choose the **Data** persona for each Cisco SD-WAN Manager instance.

4. Complete the following operations on vManage1 through vManage3:

**Important** Do not enable multitenancy on vManage1 through vManage3.

   a. Configure the following using the CLI:
      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)
      - Organization-name
      - Cisco SD-WAN Validator IP address
      - VPN 0 Transport/Tunnel interface
      - VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
      - VPN 512 Management interface

**Note** Configure only one default route in VPN 0.

   b. (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

c. Complete the following through the Cisco SD-WAN Manager:

1. Generate a Certificate Signing Request
2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.

d. Log in to the Cisco SD-WAN Manager Web Application Server.

e. Ping the OOB interfaces on the other Cisco SD-WAN Manager instances and ensure they are reachable.

f. Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

Before proceeding to the next step, ensure that the **Manager IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

5. Log in to the GUI of the existing 3-node Cisco SD-WAN Manager cluster and add vManage1 to the cluster.

vManage1 reboots before being added to the cluster.

While vManage1 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage1 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage1 to the cluster.

When the operation is completed, on the **Administration** > **Cluster Management** page, you can view vManage1 and its node persona listed along with the three Cisco SD-WAN Manager instances that were part of the original 3-node cluster.

6. Repeat **Step 4** and add vManage2 and vManage3 to the cluster.

# Manage Tenants

*Table 248: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Tenant Device Forecasting | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1 | With this feature, a service provider can control the number of WAN edge devices a tenant can add to their overlay network. By doing so, the provider can utilize Cisco Catalyst SD-WAN controller resources efficiently. |

### Tenant Device Forecasting

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.

In a multitenant deployment, a tenant can add a maximum of 1000 devices to their overlay network.

**Note** From Cisco IOS XE Release 17.6.2, Cisco vManage Release 20.6.2, you can modify the device forecast for a tenant after the tenant is added. This modification is not supported in Cisco IOS XE Release 17.6.1a, Cisco vManage Release 20.6.1.

**Benefits:**

- The service provider can ensure that the Cisco Catalyst SD-WAN controller resources are used more efficiently.
- Depending on the configuration, a multitenant deployment can support a fixed number of WAN edge devices across all tenants. By forecasting the number of devices a tenant may add, the service provider can assign a quota for each tenant from the overall pool of edge devices that the deployment can support.

# Add a New Tenant

**Prerequisites**

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

  A Cisco SD-WAN Controller enters the `Manager` 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 `Manager`.
- 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 **Validator** controller profile for the tenant on **Plug and Play Connect**. The fields in the following table are mandatory.

*Table 249: 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>`.<br>**Note** The organization name can be up to 64 characters.<br>A mismatch of organization name format of the controller profile and the tenant creation leads to a failure in device sync up. |
| **Primary Controller** | Enter the host details for the primary Cisco SD-WAN Validator. |

For a cloud deployment, the **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.

A mismatch of organization name format of the controller profile and the tenant creation leads to a failure in device sync up.

   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.

# View Tenant information

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

You can view the following tenant information from the **Tenant Management** > **Tenants** page:

- **Tenant Name**
- **Description**
- **Controllers**
- **Forcasted Edge Count**
- **Total Edge Count**: Total number of both multi-tenant and single-tenant edge devices.
- **Multi Tenant WAN Edge Count**: To view the number of multi-tenant edge device, click the non-zero number.
- **Tenant-Provider VPN Mapping**: To view the tenant and device VPN mappings for the tenant, click the non-zero number.

# 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, on page 939.

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**.

# Cisco SD-WAN Manager Dashboard for Multitenancy

After enabling Cisco SD-WAN Manager for multitenancy, you can view the multitenant dashboard when you log in to Cisco SD-WAN Manager. Cisco SD-WAN Manager multitenant dashboard is a portal where the provider or tenant can view and provision the underlying system.

The bar at the top of every Cisco SD-WAN Manager multitenant screen includes icons that allow smooth navigation.

## View Cisco Catalyst SD-WAN Validator Health Dashlet

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

You can view the state of each Cisco Catalyst SD-WAN Validator, which is the cumulative state of the Cisco Catalyst SD-WAN Validator in a selected time window, and the number of Cisco Catalyst SD-WAN Validators in each state in the **Validator Health** dashlet on **Monitor Overview** dashboard.

You can filter the Cisco Catalyst SD-WAN Validator dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

# View Cisco SD-WAN Manager Health Dashlet

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

You can view the state of Cisco SD-WAN Manager in the **Manager Health** dashlet on **Monitor Overview** dashboard.

You can filter the Cisco SD-WAN Manager dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

# View Cisco Catalyst SD-WAN Controller Health Dashlet

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

You can view the list of tenants hosted on a particular device by clicking the **Controller** bar. You can view the state of each Cisco Catalyst SD-WAN Controller, which is the cumulative state of the Cisco Catalyst SD-WAN Controller in a selected time window, and the number of Cisco Catalyst SD-WAN Controllers in each state in the **Controller Health** dashlet on **Monitor Overview** dashboard.

You can filter the Cisco Catalyst SD-WAN Controller dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

# View Multi Tenant WAN Edge Health Dashlet

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

You can view the state of each WAN edge device, which is the cumulative state of the devices in a selected time window, and the number of WAN edge devices in each state in the **Multi Tenant WAN Edge Health** dashlet on **Monitor Overview** dashboard.

You can view the list of tenants hosted on a particular device by clicking the multi-tenant WAN edge device bar. You can filter the Multi Tenant WAN Edge Health dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

# View Tenant Activity, Device, and Network Information

When you log in to a multitenant Cisco SD-WAN Manager as an administrator, the provider dashboard displays the following components. To return to the provider dashboard from other Cisco SD-WAN Manager screens, click **Dashboard**.

- Device pane — runs across the top of the multitenant dashboard screen. The device pane displays the number of active Cisco Catalyst SD-WAN Controllers, Cisco SD-WAN Validator, and Cisco SD-WAN Manager instances, the connectivity status of devices, and information on certificates that have expired or about to expire.
- Tenants pane — displays the total number of tenants and a summary of the control status, site health, router health, and Cisco Catalyst SD-WAN Controller status of all tenants.
- Table of tenants in the overlay network — List of individual tenants, with separate information about the control status, site health, WAN edge device health, and Cisco Catalyst SD-WAN Controller status for each tenant.

  To display tenant-specific status summary information,

  1. Click a tenant name from the tenant list.

     A dialog box opens on the right side of the screen that provides additional information about the status of the tenant.

  2. To access the tenant dashboard for the selected tenant, click **<Tenant name> Dashboard**.

     Cisco SD-WAN Manager presents the provider-as-tenant view and displays the tenant dashboard. To return to the provider view, click **Provider** at the top of page.

  3. To close the dialog box, click the tenant name from the tenant list.

# View Detailed Information of a Tenant Setup

Cisco SD-WAN Manager displays the tenant dashboard, which provides information about a tenant deployment when

- a provider **admin** user selects a specific tenant from the **Select Tenant** drop-down list in the provider dashboard. This view is called the provider-as-tenant view.
- a **tenantadmin** user logs in to Cisco SD-WAN Manager. This view is called the tenant view.

### View All Network Connections in the Tenant Overlay Network

The **Device** pane runs across the top of the tenant dashboard and displays the number of control connections from Cisco SD-WAN Manager to the Cisco SD-WAN Controllers and routers in the overlay network of a tenant. For each WAN edge device, the Device pane shows

- Total number of control connections between Cisco SD-WAN Controllers and WAN edge devices
- Number of valid control connections between Cisco SD-WAN Controllers and WAN edge devices
- Number of invalid control connections between Cisco SD-WAN Controllers and WAN edge devices

Click a connection number, or the **Up** or **Down** arrow, to display a table with detailed information about each connection. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Network** screen, or access the **Tools** > **SSH Terminal** Screen.

Click a connection number, or the **Up** or **Down** arrow, to display a table with detailed information about each connection. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen, or access the **Tools** > **SSH Terminal** Screen.

**Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

### View Information About Device Reboots

The **Reboot** pane displays the total number of reboots in the last 24 hours for all devices in the network. It includes soft and cold reboots and reboots that occurred as a result of power-cycling a device. For each reboot, the following information is listed:

- System IP and hostname of the device that rebooted.
- Time when the device was rebooted.
- Reason for the device reboot

If the same device reboots more than once, each reboot option is reported separately.

Click the **Reboot** pane to open the **Reboot** dialog box. In the **Reboot** dialog box, click the **Crashes** tab. For all device crashes, the following information is listed:

- System IP and hostname of the device on which the crash occurred.
- Crash index of the device
- Core time when the device crashed.
- File name of the device crash log

### View Network Connections

The **Control Status** pane displays whether Cisco SD-WAN Controller and WAN edge devices are connected. Each Cisco SD-WAN Controller must connect to all other Cisco SD-WAN Controllers in the network. Each WAN edge device must connect to the maximum number of configured Cisco SD-WAN Controllers. The **Control Status** pane displays three network connection counts:

- Control Up — total number of devices with the required number of operational control plane connections to a Cisco SD-WAN Controller
- Partial — total number of devices with some, but not all, operational control plane connection to Cisco SD-WAN Controllers.
- Control Down — total number of devices with no control plane connection to a Cisco SD-WAN Controller

To display a table with device details, click a row from the **Control Status** dialog box. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen.

**Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

### View State of Data Connections for a Site

The **Site Health** pane displays the state of data connections for a site. When a site has multiple WAN edge devices, this pane displays the state for the entire site and not for individual devices. The Site Health pane displays three connectivity states:

- Full WAN Connectivity — total number of sites where all BFD sessions on all routers are in the up state.
- Partial WAN Connectivity — total number of sites where tunnel and all BFD sessions on all routers are in the down state. These sites still have limited data plane connectivity.
- No WAN Connectivity — total number of sites where all BFD sessions on all routers are in the down state. These sites have no data plane connectivity.

To display a table with detailed information about each site, node, or tunnel, click a row from the **Site Health** dialog box. Click the **More Actions** icon at the right of each row in the table to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen, or access the **Tools** > **SSH Terminal** screen.

**Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

### View Interface Usage for WAN Edge Interfaces

The **Transport Interface Distribution** pane displays interface usage in the last 24 hours for all WAN edge interfaces in VPN 0. It includes all TLOC interfaces. Click the pane to view details of interface usage in the **Transport Interface Distribution** dialog box.

### View WAN Edge Device Counts

The **WAN Edge Inventory** pane provides four WAN edge device counts:

- Total — total number of authorized serial numbers for WAN edge devices that have been uploaded on Cisco SD-WAN Manager. The serial number is uploaded on the **Configuration** > **Devices** screen.
- Authorized — total number of authorized WAN edge devices in the overlay network These WAN edge devices are marked as **Valid** in the **Configuration** > **Certificates** > **WAN Edge List** screen.
- Deployed — total number of deployed WAN edge devices. These are WAN edge devices that are marked as Valid and are now operational in the network.
- Staging — total number of WAN edge devices you configure at a staging site before they are made a part of the overlay network. These routers do not take part in any routing decisions and do not affect network monitoring through Cisco SD-WAN Manager.

  Click the pane to view hostname, system IP, site ID, and other details of each router from the **WAN Edge Inventory** dialog box.

### View Aggregated State of WAN Edge Devices

The **WAN Edge Health** pane offers an aggregated view of the state of WAN edge devices by providing a count of the number of devices in each state, therefore describing the health of the hardware nodes. The three WAN edge device states are:

- Normal — number of WAN edge devices with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as, normal.
- Warning — number of WAN edge devices with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as, warning
- Error — number of WAN edge devices with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as, error.

  Click a number or the WAN edge device state to display a table with the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the **More Actions** icon at the right of each row in the table to access the following:

  - **Hardware Environment**
  - **Real Time** view from the **Monitor** > **Network** screen

**Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

  - **Tools** > **SSH Terminal** screen.

### View WAN Edge Device Loss, Latency, Jitter

The **Transport Health** pane displays the aggregated average loss, latency, and jitters for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

From the **Type** drop-down arrow, choose loss, latency, or jitter.

Click the icon to select a time period for which to display the transport health.

Click the icon to open the **Transport Health** dialog box. This dialog box displays a more detailed view. To display information in a tabular format, click the **Details** tab. You can choose to change the displayed health type and time period.

### View SAIE Flow Information of WAN Edge Devices

The **Top Applications** pane displays SD-WAN Application Intelligence Engine (SAIE) flow information for traffic transiting routers in the overlay network.

**Note**
- In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is known as deep packet inspection (DPI).
- The SAIE flow information is shown only for the last 24 hours. To view SAIE flow information for a time before the last 24 hours, you must check the information for the specific device.

Click the icon to select a time period for which to display data. From the **VPN** drop-down list, select a VPN to display SAIE information for all flows in that VPN.

Click the icon to open the **Top Applications** dialog box. This dialog box displays a more detailed view of the same information. You can change the VPN and time period.

### View Tunnels Data

The **Application-Aware Routing** pane allows you to choose the following tunnel criteria from the **Type** drop-down arrow:

- Loss
- Latency
- Jitter

Based on the tunnel criteria, the pane displays the 10 worst tunnels. For example, if you choose loss, the pane shows 10 tunnels with the greatest average loss over the last 24 hours.

Click the icon against a row to display a graphical representation of the data. Select a time period for which to display data or click **Custom** to display a drop-down arrow for specifying a custom time period.

Click the icon to open the **Application-Aware Routing** dialog box. This dialog box displays the 25 worst tunnels based on criteria you choose from the **Type** drop-down arrow, the criteria being loss, latency, and jitter.

# 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.

# Tenant-Specific Policies on Cisco SD-WAN Controller

A provider **admin** user (from the Cisco SD-WAN Manager provider-as-tenant view) or a **tenantadmin** user (from the Cisco SD-WAN Manager tenant view) can create and deploy tenant-specific policies on the Cisco SD-WAN Controller serving the tenant. The user can configure a CLI policy or create the policy using the UI policy configuration wizard.

When you activate or deactivate a policy,

1. Cisco SD-WAN Manager identifies the Cisco SD-WAN Controllers serving the tenant.
2. Cisco SD-WAN Manager notifies the Cisco SD-WAN Controllers to pull the policy configuration.
3. Cisco SD-WAN Controllers pull and deploy the policy configuration.
4. Cisco SD-WAN Manager reports the status of the policy pull by the Cisco SD-WAN Controllers.

# Manage Tenant Data

## Back Up Tenant Data

The tenant data backup solution of Cisco SD-WAN Manager multitenancy provides the following functionalities:

- Create, Extract, and List Configuration Data Backup File.

- Back up configuration database of a specific tenant with an option to restore it later. See Restore and Delete Tenant Data Backup File.
- Delete back up files of a tenant stored in Cisco SD-WAN Manager. For deleting tenant data backup files, see Restore and Delete Tenant Data Backup File.

The following factors are applicable when using data backup solution:

- The tenant data backup solution operations can be performed by a tenant administrator in the tenant view and or by a provider administrator in the provider-as-tenant view. To know how to access tenant dashboard through different views, see User Roles in Multitenant Environment, on page 912.
- A tenant is allowed to perform the following backup operations at a particular time and must complete an operation before starting a new operation:
  - Back up a single configuration database
  - Download the backup file.
  - Restore or import backup files
  - Delete backup files.
  - List backup files
- A tenant backup file format is as follows:

  `Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz`
- The tenant data backup operation is a readonly operation on the configuration database. However, to ensure data consistency and prevent data loss, do not perform any major changes on the network while the operation is in progress.
- Multiple tenants can perform back-up and restore operations in parallel.
- A tenant is not allowed to perform other backup operations when the restore operation of the tenant database is in-progress. So, a tenant can perform a single backup operation and when this operation is in-progress, all new backup operation requests are rejected.

  The remaining tenants can continue with their backup operations.
- A tenant must perform backup and restore operations on Cisco SD-WAN Manager instances running identical Cisco SD-WAN Manager software versions.
- A tenant can store a maximum of three backup files in Cisco SD-WAN Manager and can download to store them outside Cisco SD-WAN Manager repository. If the tenant already has three backup files, a subsequent backup operation results in the earliest backup file being deleted and a new backup file being generated.
- Ensure that the following parameter values match in both the backup file and the setup where tenant has requested for a restore operation:
  - Tenant Id
  - Organization Name
  - SP Organization Name

- The tenant data backup solution creates a task in the tenant view of Cisco SD-WAN Manager. Therefore, the tenant can monitor the progress of the operation from the task view of the tenant dashboard.
- A provider cannot back up provider data using this solution. Therefore, the provider can back up all tenants information at once by backing up all tenants configuration database using CLI.

# Create, Extract, and List Configuration Data Backup File

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. In the address bar, modify the URL path with `dataservice` for the REST API connection.

   **Example:** `https://<tenant_URL>/dataservice`

3. Create a configuration backup file by using the following API:
   `https://<tenant_URL>/dataservice/tenantbackup/export`.

4. If the configuration backup file has been created successfully, Cisco SD-WAN Manager task view indicates that the backup file has been generated. You can view the process identifier of the created process or task.

   **Example:**

   ```
   {
      "processId": "72d69805-b987-436f-9b7a-afef2f3f9061",
   "status": "in-progress"
   }
   ```

5. Verify the task status using the obtained process identifier.

   **Example:**
   `https://<tenant_URL>/dataservice/device/action/status/72d69805-b987-436f-9b7a-afef2f3f9061`

   The verification generates the details of the task in the JSON file format.

6. After the task is completed, extract or download the backed-up file available under the **data** section of the JSON task file.

   **Example:** To extract or download the backup file, use the following API:
   `https://<tenannt_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz`

7. List backup files stored in Cisco SD-WAN Manager using the following API.

   **Example:** `https://<tenant_URL>//dataservice/tenantbackup/list`

# Restore and Delete Tenant Data Backup File

**Before you begin:**

To run the restore and delete tenant data backup files API, you can download and install Postman tool or any other alternative tool for testing http applications and services. In this document, the procedure to restore and delete tenant data backup files has been explained using the Postman tool. Postman is a software tool used as an API development environment. You can download the tool from the Postman website.

1. Open Google Chrome, or another browser, and enable developer mode on it.
2. 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**.
3. To get header information of the restore API, do as follows:
   a. On the right side of the screen, click the **Network** tab to get the network capture view.
   b. In the network capture view, click the **Name** column to sort the listed items.
   c. Search and click **index.html**.
   d. Click the **Headers** tab and expand **Request Headers**.
   e. Choose all text under **Request Headers** and copy it to the clipboard.
4. Import backup files through the Postman UI:
   a. Open the Postman UI.
   b. To disable SSL certificate verification, click **Postman** > **Preferences** > **General** > **Request**. Turn off **SSL Certificate Verification**.
   c. In the Postman UI, create a new tab.
   d. Click **Headers** and then click **Bulk Edit**.
   e. Paste the text that was copied in step 3 from the **Request Headers** block into an editable form.
   f. From the **GET** method drop-down list, choose **POST**.
   g. In the **Paste request URL** field, paste the dedicated URL of the tenant and include `dataservice/tenantbackup/import`.

      **Example:** `https://customer1.managed-sp.com/dataservice/tenantbackup/import`
   h. Click the **Body** tab and select **form-data**.
   i. Under **KEY** column, enter *bakup.tar.gz*
   j. Under **VALUE** column, click **Select Files** and select a backup file to be imported.
   k. To run the API, click **Send**.

      In the **Response** section of the Postman UI, you can view the JSON information that indicates the file that was restored.
5. Monitor the restoration of backup files in either of the following ways:
   a. Use Cisco SD-WAN Manager task view that indicates if backup file has been imported successfully. You can view the process identifier of the created process or task.

      **Example:**

      ```
      {"processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
          "status": "Import Successfully Submitted for tenant 1579026919487"
      }
      ```

**b.** Use the following URL to get the status,
`https://<tenant_URL>/dataservice/device/action/status/<processId>`

**Example:**
`https://customer1.managed-sp.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d`

6. Delete tenant data backup file through Postman UI.
   **a.** In the Postman UI, create a new tab.
   **b.** Click **Headers** and then click **Bulk Edit**.
   **c.** Paste the text that was copied in step 3 from the **Request Headers** block into an editable form.
   **d.** From the **GET** method drop-down list, choose **DELETE**.
   **e.** In the **Paste request URL** field, paste the dedicated URL of the tenant and include `dataservice/tenantbackup/delete?fileName='filename'`. The filename can either be name of the backup file or all.

   **Example:**
   `https://customer1.managed-sp.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz`

   **Example:** `https://customer1.managed-sp.com/dataservice/tenantbackup/delete?fileName=all`
   **f.** To run the API, click **Send**.

   In the **Response** section of the Postman UI, you can view the JSON information that indicates the files that were deleted.

   **Example:**

```
{
    "Deleted": [
        "bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz"
    ]
}
```

# 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 **Controller** 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.

# Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment

### Before You Begin

- Before you begin the migration,
  - Migration of a single-tenant overlay to a multitenant deployment is only supported with the Cisco Catalyst SD-WAN controllers deployed on-premises. Migration is yet to be supported with cloud-hosted Cisco Catalyst SD-WAN controllers.
  - Ensure that the edge devices in the single-tenant deployment can reach the Cisco SD-WAN Validator in the multitenant deployment
  - Ensure that the template, routing, and policy configuration on the edge devices is synchronized with the current configuration on Cisco SD-WAN Manager
  - Configure a maintenance window for the single-tenant overlay before performing this procedure. See Configure or Cancel SD-WAN Manager Server Maintenance Window.
- Minimum software requirements for the single-tenant overlay to be migrated:

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.6.1 |
| Cisco SD-WAN Validator | Cisco SD-WAN Release 20.6.1 |
| Cisco Catalyst SD-WAN Controller | Cisco SD-WAN Release 20.6.1 |
| Cisco IOS XE Catalyst SD-WAN device | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a |

- Minimum software requirements for the multitenant deployment to which the single-tenant overlay must be migrated:

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.6.1 |
| Cisco SD-WAN Validator | Cisco SD-WAN Release 20.6.1 |

| Device | Software Version |
|---|---|
| Cisco Catalyst SD-WAN Controller | Cisco SD-WAN Release 20.6.1 |
| Cisco IOS XE Catalyst SD-WAN device | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a |

- The software versions of the Cisco Catalyst SD-WAN controllers and WAN edge devices must be identical in both the single-tenant and multitenant deployments.
- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.

### Migration Procedure

1. Export the single-tenant deployment and configuration data from a Cisco SD-WAN Manager instance controlling the overlay.

| | |
|---|---|
| Method | `POST` |
| URL | `https://ST-vManage-IP-address` |
| Endpoint | `/dataservice/tenantmigration/export` |
| Authorization | Admin user credentials. |
| Body | Required<br>Format: Raw JSON<br>`{ "desc": <tenant_description>, "name": <tenant_name>, "subdomain": <tenant_name>.<domain>, "orgName": <tenant_orgname > }`<br>Field Description:<br>• `desc`: A description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters.<br>• `name`: Unique name for the tenant in the multitenant deployment.<br>• `subdomain`: Fully qualified sub-domain name of the tenant. The sub-domain name must include the domain name of the service provider. For example, if `managed-sp.com` is the domain name of service provider, and the tenant name is `Customer1`, the tenant sub-domain name would be `customer1.managed-sp.com`.<br>• `orgName`: Name of the tenant organization. The organization name is case-sensitive. |
| Response | Format: JSON<br>`{ "processId": <vManage_process_ID>, }` |

While exporting the data, Cisco SD-WAN Manager attempts to detach any CLI templates from the edge devices in preparation for the migration to the multitenant deployment. If prompted by Cisco SD-WAN Manager, detach CLI templates from the edge devices and execute the export API call again.

2. Check the status of the data export task in Cisco SD-WAN Manager. When the task succeeds, download the data using the URL
`https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz`

3. On a multitenant Cisco SD-WAN Manager instance, import the data exported from the single-tenant overlay.

| | |
|---|---|
| Method | `POST` |
| URL | `https://MT-vManage-IP-address` |
| Endpoint | `/dataservice/tenantmigration/import` |
| Authorization | Provider Admin user credentials. |
| Body | Required<br>Format: form-data<br>Key Type: File<br>Value: `default.tar.gz` |
| Response | `Format: JSON`<br>`{`<br>`"processId": <vManage_process_ID>,`<br>`"migrationTokenURL": <token_URL>,`<br>`}` |

When the task succeeds, on the multitenant Cisco SD-WAN Manager, you can view the devices, templates, and policies imported from the single-tenant overlay.

4. Obtain the migration token using the token URL obtained in response to the API call in **Step 3**.

| | |
|---|---|
| Method | `GET` |
| URL | `https://MT-vManage-IP-address` |
| Endpoint | `migrationTokenURL` obtained in **Step 3**. |
| Authorization | Provider Admin user credentials. |
| Response | The migration token as a large blob of encoded text. |

5. On the single-tenant Cisco SD-WAN Manager instance, initiate the migration of the overlay to the multitenant deployment.

| | |
|---|---|
| Method | `POST` |
| URL | `https://ST-vManage-IP-address` |
| Endpoint | `dataservice/tenantmigration/networkMigration` |
| Authorization | Admin user credentials. |

| | |
|---|---|
| Body | Required<br>Format: Raw text<br>Content: Migration token obtained in **Step 4**. |
| Response | Format: JSON<br>`{ "processId": <vManage_process_ID>, }` |

In Cisco SD-WAN Manager, check the status of the migration task. As part of the migration task, the address of the multitenant Cisco SD-WAN Validator, and the service provider and tenant organization names are pushed to the WAN edge devices of the single-tenant overlay. If the task succeeds, WAN edge devices form control connections to controllers in the multitenant deployment; the WAN edge devices are no longer connected to the controllers of the single-tenant overlay.

Attach any CLI templates detached from the edge devices (in Step 1) after migration to the multitenant deployment. Before you attach the templates, update the Cisco SD-WAN Validator IP address and the Organization name to match the configuration of the multitenant deployment.

**Note** In the single-tenant deployment, if Cisco SD-WAN Manager-signed certificates are installed on cloud-based WAN edge devices, the certificates are cleared when the devices are migrated to the multitenant deployment. You must re-certify the devices on the multitenant Cisco SD-WAN Manager. If enterprise certificates are installed on the cloud-based WAN edge devices, the certificates are not affected by the migration. For more information, see Enterprise Certificates.

# Migrate a Tenant from a Multitenant Cisco Catalyst SD-WAN Overlay to Single-Tenant Cisco Catalyst SD-WAN Deployment

### Before You Begin

- Manually migrate the serial number of the WAN edge device associated to a virtual account on the source Cisco SD-WAN Manager overlay in Cisco PNP to the destination virtual account.
- Ensure that you manually create the controller profile on the destination virtual account for on-prem to on-prem or cloud to on-prem deployments.
- Ensure that the source and destination Cisco SD-WAN Manager instances have the same Certificate Authority (CA). If not, recertify the devices after the migration is complete.
- Ensure that you check the CPU, memory, and disk size requirements of the destination overlay Cisco SD-WAN Controllers before the migration to meet the WAN edge forecast requirements.
- Ensure that there is no overlap between the configured system IP addresses of edge devices and the destination overlay controllers.

- Ensure that the destination single-tenant Cisco SD-WAN Manager does not have any configurations before migration. You can configure only mandatory admin settings and all other configurations can be done after data import.
- Ensure that the Cisco SD-WAN Control Components in the source and destination overlays are using the same software release. The migration process does not check for a software release mismatch and a mismatch blocks the import of tenant data, causing the migration to fail.
- Ensure that all devices in a tenant have connectivity to the Cisco SD-WAN Validator in the destination single-tenant overlay. The migration procedure supports a Cisco SD-WAN Validator on the single-tenant deployment configured either with IP or DNS.

  Push any required static route configuration to the devices before initiating any of the migration steps.
- Ensure that the WAN edge devices that are configured using CLI, device template, or configuration groups, have an IP host mapping to the Cisco SD-WAN Validator in the destination single-tenant overlay.
- Ensure that there are valid control connections from Cisco SD-WAN Manager to the WAN edge devices in the source overlay.
- Configure a maintenance window for the multitenant overlay before performing this procedure. See Configure or Cancel SD-WAN Manager Server Maintenance Window.
- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.

### Migration Procedure

1. Export the multitenant deployment configuration and statistical data from a Cisco SD-WAN Manager instance controlling the source overlay.

| | |
|---|---|
| Method | `POST` |
| URL | `https://MT-vManage-IP-address` |
| Endpoint | `/dataservice/tenantmigration/export` |
| Authorization | Administrator user credentials. |

| | |
|---|---|
| Body | Required<br>Format: Raw JSON<br>Example:<br>`{`<br>`"name": "tenant1",`<br>`"desc": "This is tenant1",`<br>`"orgName": "vIPtela Inc MT to ST Migration Regression-Tenant1 Inc",`<br>`"subDomain": "tenant1.mtreg.com",`<br>`"wanEdgeForecast": 100,`<br>`"migrationKey="tenant1TenantMigrationKey123",`<br>`"isDestinationOverlayMT": false`<br>`}`<br>Field descriptions:<br>**Note** Ensure that the `name`, `desc`, `orgName`, `subdomain`, and `wanEdgeForecast` match the tenant you wish to migrate.<br>• `name`: Unique name for the tenant in the multitenant deployment. The name should be between 8-32 characters and can contain only alphanumeric characters.<br>• `desc`: Description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters.<br>• `orgName`: Name of the tenant organization. The organization name is case-sensitive.<br>• `subdomain`: Fully qualified sub-domain name of the tenant. The sub-domain name must include the domain name of the service provider. For example, if `managed-sp.com` is the domain name of service provider, and the tenant name is `Customer1`, the tenant sub-domain name would be `customer1.managed-sp.com`.<br>• `wanEdgeForecast`: Number of WAN edge devices that the tenant can deploy.<br>• `migrationKey`: Migration key which is used to encrypt sensitive data during migration. The migration key should be between 8-32 characters and can contain only alphanumeric characters.<br>• `isDestinationOverlayMT`: Boolean variable which speficies if the migration is happening to a mutitenant overlay or not. |
| Response | Format: JSON<br>`{`<br>`"processId": <vManage_process_ID>,`<br>`}` |

2. Check the status of the data export task in Cisco SD-WAN Manager. When the task is successfully complete, download the data from the following URL:
`https://`*`MT-vManage-IP-address`*`/dataservice/tenantmigration/download/default.tar.gz`
3. Import the data to the single-tenant instance, as follows:

**a.** Execute the following API:

| | |
|---|---|
| Method | `POST` |
| URL | `https://ST-vManage-IP-address` |
| Endpoint | `/dataservice/tenantmigration/import/{migrationKey}`<br>Use the same migration key specified earlier. |
| Authorization | Provider administrator user credentials. |
| Body | Required<br>Format: form-data<br>Key Type: File<br>Value: `default.tar.gz` |
| Response | `Format: JSON`<br>`{`<br>`"processId": <vManage_process_ID>,`<br>`"migrationTokenURL": <token_URL>,`<br>`}` |

**b.** When the task is complete, on the single-tenant Cisco SD-WAN Manager, you can view the devices, templates, and policies imported from the multitenant overlay.

**4.** After the import, update information related to the device templates, policies, and other deployment-specific parameters. Check and update the administrator settings as some of the administrator settings specific to the source overlay are not exported. The import does not override the administrator settings that are already configured in destination Cisco SD-WAN Manager.

**5.** If a centralized policy is present on the source tenant, the migration copies the policy to the destination overlay. We recommend creating Cisco SD-WAN Controller templates and attaching them to the devices. Apply the centralized policy to devices in the destination overlay before proceeding.

**6.** Obtain the migration token using the token URL from the previous step.

| | |
|---|---|
| Method | `GET` |
| URL | `https://ST-vManage-IP-address` |
| Endpoint | `migrationTokenURL` obtained in the previous step. |
| Authorization | Provider administrator user credentials. |
| Response | The migration token as a large encoded text. |

**7.** On the multitenant Cisco SD-WAN Manager instance, initiate the migration of the overlay to the single-tenant deployment.

| | |
|---|---|
| Method | `POST` |
| URL | `https://MT-vManage-IP-address` |
| Endpoint | `dataservice/tenantmigration/networkMigration` |
| Authorization | Administrator user credentials. |

| | |
|---|---|
| Body | Required<br>Format: Raw text<br>Content: Migration token obtained in the previous step. |
| Response | Format: JSON<br>`{ "processId": <vManage_process_ID>, }` |

In Cisco SD-WAN Manager, check the status of the migration task. When the task succeeds, WAN edge devices form control connections to controllers in the single-tenant deployment; the WAN edge devices are no longer connected to the controllers of the multitenant overlay.

8. After the migration is successfully complete, perform the following tasks:
   - If WAN edge devices have Cisco SD-WAN Manager signed certificates in the source setup, the certificates are cleared from the device during migration and control connections are lost. Recertify the devices in the destination.
   - The passwords are updated to the default password in the destination overlay for users created on a tenant in the source overlay. Make any configuration changes specific to the destination overlay.
   - Delete the tenant on the source overlay after migration and verification is complete.

# Migrate Multitenant Cisco Catalyst SD-WAN Overlay

*Table 250: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Migrate Multitenant Cisco Catalyst SD-WAN Overlay | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1 | This feature enables you to migrate a multitenant Cisco Catalyst SD-WAN overlay comprising shared Cisco SD-WAN Manager instances and Cisco SD-WAN Validator, and tenant-specific Cisco SD-WAN Controllers to a multitenant overlay comprising shared Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco SD-WAN Controllers. |

### Prerequisites

Minimum software requirements for Cisco Catalyst SD-WAN controllers and WAN edge devices in the multitenant overlay to be migrated:

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.3.3 |
| Cisco SD-WAN Validator | Cisco SD-WAN Release 20.3.3 |
| Cisco SD-WAN Controller | Cisco SD-WAN Release 20.3.3 |
| Cisco IOS XE Catalyst SD-WAN device | Cisco IOS XE Release 17.3.3 |

### Restrictions

- This migration procedure applies only to Cisco Catalyst SD-WAN controllers deployed on premises.
- The multitenant overlay can only be migrated to a setup in which Cisco SD-WAN Manager instances run Cisco vManage Release 20.6.1 software and Cisco Catalyst SD-WAN controllers run Cisco SD-WAN Release 20.6.1 software.
- This migration procedure cannot be used to merge two or more multitenant overlays. Only one multitenant overlay can be migrated to the new setup at a time.

### Migration Procedure

1. Upgrade the software on the three Cisco SD-WAN Manager instances in the cluster to Cisco vManage Release 20.6.1. For more information, see Upgrade Cisco SD-WAN Manager Cluster.

**Note** Run the command **request nms configuration-db upgrade** on only one of the Cisco SD-WAN Manager instances.

2. After the Cisco SD-WAN Manager software is upgraded to Cisco vManage Release 20.6.1, log in to the Cisco SD-WAN Manager.

   You're prompted to set a new password.

   a. Enter a new password that adheres to the password guidelines.

3. Upload the Cisco SD-WAN Release 20.6.1 software to Cisco SD-WAN Manager. For more information, see Add an Image to the Software Repository.
4. Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1. For more information, see Upgrade the Software Image on a Device.
5. Create two Cisco SD-WAN Controller instances running Cisco SD-WAN Release 20.6.1 software. See Deploy the Cisco SD-WAN Controller.

**Note** With two Cisco SD-WAN Controller instances, you can support up to 24 tenants. To support up to 50 tenants, create six Cisco SD-WAN Controller instances.

   a. Add Cisco SD-WAN Controller to the overlay network.

The **Provider Dashboard** shows the new Cisco SD-WAN Controllers running Cisco SD-WAN Release 20.6.1 software. The **Tenant Dashboard** shows the older Cisco SD-WAN Controllers running Cisco SD-WAN Release 20.3.3 software.

6. Enable the maintenance window on Cisco SD-WAN Manager. For more information, see Configure or Cancel SD-WAN Manager Server Maintenance Window.

   A maintenance window of 3 to 4 hours is recommended.

7. Migrate the tenant configuration from the older tenant-specific Cisco SD-WAN Controllers running Cisco SD-WAN Release 20.3.3 software to the new shared Cisco SD-WAN Controllers running Cisco SD-WAN Release 20.6.1 software.

| | |
|---|---|
| Method | `POST` |
| URL | `https://<vmanageip>:<port>` |
| Endpoint | `dataservice/tenant/vsmart-mt/migrate` |
| Authorization | Provider **admin** user credentials. |
| Body | Required<br>Format: Raw JSON<br>`{}` |
| Response | Format: JSON<br>`{`<br>`"processId": <vManage_process_ID>,`<br>`}` |

   In Cisco SD-WAN Manager, check the status of the migration task using the `processId` from the API response. During the migration task, the following changes are affected:

   a. The older Cisco SD-WAN Controllers are invalidated and deleted from the overlay network.

   b. In the tenant view, the older Cisco SD-WAN Controllers are removed from the **Tenant Dashboard**, and the **Devices** and the **Certificates** page.

   c. The tenant WAN edge devices are connected to the new Cisco SD-WAN Controllers.

8. (Optional) Upgrade the Cisco IOS XE Catalyst SD-WAN device software to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.

**Tip** It is not necessary to upgrade the tenant WAN edge device software in the same maintenance window in which you migrate the multitenant overlay. However, we recommend that you upgrade the tenant WAN edge device software within a few weeks of the migration.

### Verify the Migration

1. In the provider view, perform the following checks:

a. From the **Main Dashboard** page, verify whether the tenant WAN edge devices are connected to the new multitenant Cisco SD-WAN Controllers.

b. View Tenants Associated with a Cisco SD-WAN Controller, on page 944.

c. On the Cisco SD-WAN Controller CLI, run the command **show control connections**. In the command output, verify that control connections are established between the Cisco SD-WAN Controller and the tenant WAN edge devices.

2. In the provider-as-tenant view, verify whether the multitenant Cisco SD-WAN Controllers appear on the **Tenant Dashboard**.

# Upgrade Cisco Catalyst SD-WAN Controller and Edge Device Software

### Prerequisites

Minimum software requirements for Cisco Catalyst SD-WAN controllers and WAN edge devices:

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.4.1 or later |
| Cisco SD-WAN Validator | Cisco SD-WAN Release 20.4.1 or later |
| Cisco Catalyst SD-WAN Controller | Cisco SD-WAN Release 20.4.1 or later |
| Cisco IOS XE Catalyst SD-WAN device | Cisco IOS XE Release 17.4.1 or later |

### Upgrade Procedure

1. Upgrade the software on the three Cisco SD-WAN Manager instances in the cluster to Cisco vManage Release 20.6.1 or a later release. For more information, see Upgrade Cisco SD-WAN Manager Cluster.

**Note** Skip the step to upgrade the configuration-db service using the command **request nms configuration-db upgrade**.

2. After the Cisco SD-WAN Manager software is upgraded to Cisco vManage Release 20.6.1 or a later release, log in to the Cisco SD-WAN Manager.

3. Upload the Cisco SD-WAN Release 20.6.1 or a later release and the Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or a later release software to Cisco SD-WAN Manager. For more information, see Add an Image to the Software Repository.

4. Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1 or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.

5. Enable maintenance window on Cisco SD-WAN Manager. For more information, see Configure or Cancel SD-WAN Manager Server Maintenance Window.

6. Upgrade the Cisco Catalyst SD-WAN Controller software to Cisco SD-WAN Release 20.6.1 or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.
7. Upgrade the Cisco IOS XE Catalyst SD-WAN device software to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.

**Tip** We recommend that you upgrade the WAN edge device software in the same maintenance window. If the WAN edge device software is not upgraded within the OMP graceful restart window, traffic may be lost.

# Multitenant Cisco SD-WAN Manager: Disaster Recovery

If a Multitenant Cisco SD-WAN Manager cluster or the data center hosting the Cisco SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby Cisco SD-WAN Manager cluster. You can perform disaster recovery as follows:

1. Deploy and configure a standby Cisco SD-WAN Manager cluster.

   The standby Cisco SD-WAN Manager cluster is not part of the overlay network and is not active.
2. Back up the configuration database of the active Cisco SD-WAN Manager cluster periodically.

   Choose a Cisco SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.
3. If the active Cisco SD-WAN Manager cluster fails, restore the most recent configuration database on the standby Cisco SD-WAN Manager cluster, activate the standby Cisco SD-WAN Manager cluster, and remove the previously active Cisco SD-WAN Manager cluster from the overlay network.

   Choose a Cisco SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active Cisco SD-WAN Manager cluster.

To test disaster recovery, you can simulate a scenario in which the active Cisco SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

### Prerequisites

- The number of Cisco SD-WAN Manager nodes in the active and standby clusters must be identical.
- Each Cisco SD-WAN Manager node in the active and standby clusters must run the same Cisco SD-WAN Manager software release.
- Each Cisco SD-WAN Manager node in the active and standby clusters must be able to connect to the WAN transport IP address of the Cisco SD-WAN Validator in the overlay network.
- Initially, the tunnel interfaces of the Cisco SD-WAN Manager nodes in the standby cluster must be disabled.
- The Cisco SD-WAN Manager nodes in the standby cluster must be certified.

- The clock of every Cisco SD-WAN Manager node in the standby cluster must be synchronized with the clocks of the Cisco Catalyst SD-WAN controllers and WAN edge devices in the overlay network. If NTP is configured on the overlay, configure the same on the standby Cisco SD-WAN Manager nodes.
- The Cisco SD-WAN Manager nodes in the active and standby clusters should use identical neo4j credentials.

### Restrictions

- Do not interrupt any active processes while backing up the configuration database.
- If you wish to enable SD-AVC, you must do so before the restoring the configuration database on standby Cisco SD-WAN Manager node.

### Configure a Standby Cisco SD-WAN Manager Cluster

1. Configure the standby Cisco SD-WAN Manager nodes with a similar running configuration as the active Cisco SD-WAN Manager nodes. Install local certificates on the standby Cisco SD-WAN Manager nodes.

**Note** The running configuration on a standby Cisco SD-WAN Manager is usually identical to that of an active Cisco SD-WAN Manager node. However, you must ensure that settings such as the system IP address and the tunnel interface IP address are unique.

2. On the standby Cisco SD-WAN Manager nodes, shut down the transport interface in VPN 0: On the CLI, include the **shutdown** command in the transport interface configuration.
3. Create a standby cluster using the standby Cisco SD-WAN Manager nodes.

With the standby Cisco SD-WAN Manager nodes configured in this manner, the overlay network is not aware of the standby Cisco SD-WAN Manager cluster.

### Back Up the Active Cisco SD-WAN Manager Cluster Configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active Cisco SD-WAN Manager virtual machines.

1. Choose an active Cisco SD-WAN Manager node that hosts the configuration database service and export a backup the configuration database. On the CLI of the Cisco SD-WAN Manager node, run the following command: **request nms configuration-db backup path** *file-path*

   The command backs up the configuration database in a `.tar.gz` file and saves the file in the specified *file-path*.

   In the following example, the database is backed up to a file named `db_backup.tar.gz` in the `/home/admin/` directory.

   ```
   Active-vManage# request nms configuration-db backup path /home/admin/db_backup
   Successfully saved database to /home/admin/db_backup.tar.gz
   ```

2. Choose a standby Cisco SD-WAN Manager node that hosts the configuration database service and copy the configuration database backup to this node.

In the following example, `db_backup.tar.gz` is copied from the active Cisco SD-WAN Manager node to the `/home/admin/` directory of a standby Cisco SD-WAN Manager node.

```
Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5

admin@10.126.93.92's password:
db_backup.tar.gz                                  100%  399KB   4.4MB/s   00:00
```

### Restore Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

Restore the most recent backup of the configuration database from the active Cisco SD-WAN Manager cluster on the standby Cisco SD-WAN Manager node to which you copied this backup.

**Note**

- The restore operation does not restore all the information included in the configuration database. Cisco SD-WAN Manager configurations such as users and repositories must be configured on the standby Cisco SD-WAN Manager node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active Cisco SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

1. On the CLI of the standby Cisco SD-WAN Manager node, run the following command: **request nms configuration-db restore path** *file-path*

   In the following example, the configuration database is restored using the backup file `db_backup.tar.gz`.

   ```
   Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. Verify that the appropriate services are running on the standby Cisco SD-WAN Manager nodes: On the CLI of each standby Cisco SD-WAN Manager node, run the **request nms all status** command. From the command output, verify the services running on the node.

3. Verify that every standby Cisco SD-WAN Manager node has a list of all the active and standby Cisco SD-WAN Manager nodes.

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

   **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   b. Verify that the page displays all active and standby Cisco SD-WAN Manager nodes.

4. On the standby Cisco SD-WAN Manager nodes, enable the transport interface on VPN 0.

Use one of the following two methods:

**a.** Enable the transport interface in VPN 0: On the CLI of each standby Cisco SD-WAN Manager node, run the **no shutdown** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

**b.** Activate the tunnel interface in VPN 0: On the CLI of each standby Cisco SD-WAN Manager node, run the **tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

**5.** Add each standby Cisco SD-WAN Manager node to the overlay network.

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

**b.** Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

**c.** For a Cisco SD-WAN Validator, click **...** and click **Edit**.

**d.** In the **Edit** dialog box, enter the following details of the Cisco SD-WAN Validator: WAN transport IP address, username, and password.

**e.** Repeat **Step 5c** and **Step 5d** for every Cisco SD-WAN Validator.

**6.** Disconnect the active Cisco SD-WAN Manager nodes from the overlay network.

**Note** In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach Cisco SD-WAN Manager instances in an actual disaster scenario, you may not be able to perform this step and can omit the step.

Use one of the following two methods:

**a.** Shut down the transport interface in VPN 0: On the CLI of each active Cisco SD-WAN Manager node, run the **shutdown** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

**b.** Deactivate the tunnel interface in VPN 0: On the CLI of each active Cisco SD-WAN Manager node, run the **no tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
```

```
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

7. From the standby Cisco SD-WAN Manager, send the updated controller and device list to the Cisco SD-WAN Validator.

   Send the list of controllers:

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

   b. Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   c. Click **Send to Validator**.

      Wait for the configuration task to complete. When the task is complete,

      - The standby Cisco SD-WAN Manager nodes become the active Cisco SD-WAN Manager nodes.
      - The previously active Cisco SD-WAN Manager nodes are no longer part of the overlay network.
      - The active Cisco SD-WAN Manager nodes have the configuration from the most recent configuration database backup.
      - Every controller establishes connection with the other controllers in the network.

   d. Click **WAN Edge List**.

   e. Click **Send to Controllers**.

8. Verify that the following are intact:

   - Policies
   - Templates
   - Controller and WAN edge device lists

9. Verify the valid Cisco SD-WAN Manager nodes.

   a. Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

      In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.

   b. Log in to the CLI of a WAN edge device and run the **show control valid-vmanage-id** command.

      In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

10. Invalidate the previously active Cisco SD-WAN Manager nodes.

**Note** After you invalidate the Cisco SD-WAN Manager nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

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

b. Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

c. For each previously active Cisco SD-WAN Manager node, click **...** and click **Invalidate**.

11. Verify the valid Cisco SD-WAN Manager nodes.

    a. Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

       In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed.

    b. Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

       In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

The Cisco SD-WAN Manager cluster that was initially the standby cluster is now the active Cisco SD-WAN Manager cluster.

# Multitenant Cisco SD-WAN Manager: Disaster Recovery in an Overlay Network with Virtual Routers

If a Multitenant Cisco SD-WAN Manager cluster or the data center hosting the Cisco SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby Cisco SD-WAN Manager cluster. You can perform disaster recovery as follows:

1. Deploy and configure a standby Cisco SD-WAN Manager cluster.

   The standby Cisco SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active Cisco SD-WAN Manager cluster periodically.

   Choose a Cisco SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active Cisco SD-WAN Manager cluster fails, restore the most recent configuration database on the standby Cisco SD-WAN Manager cluster, activate the standby Cisco SD-WAN Manager cluster, and remove the previously active Cisco SD-WAN Manager cluster from the overlay network.

Choose a Cisco SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active Cisco SD-WAN Manager cluster.

To test disaster recovery, you can simulate a scenario in which the active Cisco SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

The following disaster recovery procedure applies to an overlay network in which Cisco vEdge Cloud routers are deployed at branch locations.

### Prerequisites

- The number of Cisco SD-WAN Manager nodes in the active and standby clusters must be identical.
- Each Cisco SD-WAN Manager node in the active and standby clusters must run the same Cisco SD-WAN Manager software release.
- Each Cisco SD-WAN Manager node in the active and standby clusters must be able to connect to the WAN transport IP address of the Cisco SD-WAN Validator in the overlay network.
- Initially, the tunnel interfaces of the Cisco SD-WAN Manager nodes in the standby cluster must be disabled.
- The Cisco SD-WAN Manager nodes in the standby cluster must be certified.
- The clock of every Cisco SD-WAN Manager node in the standby cluster must be synchronized with the clocks of the Cisco Catalyst SD-WAN controllers and WAN edge devices in the overlay network. If NTP is configured on the overlay, configure the same on the standby Cisco SD-WAN Manager nodes.
- The Cisco SD-WAN Manager nodes in the active and standby clusters should use identical neo4j credentials.

### Restrictions

- Do not interrupt any active processes while backing up the configuration database.
- If you wish to enable SD-AVC, you must do so before the restoring the configuration database on standby Cisco SD-WAN Manager node.

### Configure a Standby Cisco SD-WAN Manager Cluster

1. Configure the standby Cisco SD-WAN Manager nodes with a similar running configuration as the active Cisco SD-WAN Manager nodes. Install local certificates on the standby Cisco SD-WAN Manager nodes.

**Note** The running configuration on a standby Cisco SD-WAN Manager is usually identical to that of an active Cisco SD-WAN Manager node. However, you must ensure that settings such as the system IP address and the tunnel interface IP address are unique.

2. On the standby Cisco SD-WAN Manager nodes, shut down the transport interface in VPN 0: On the CLI, include the **shutdown** command in the transport interface configuration.
3. Create a standby cluster using the standby Cisco SD-WAN Manager nodes.

With the standby Cisco SD-WAN Manager nodes configured in this manner, the overlay network is not aware of the standby Cisco SD-WAN Manager cluster.

### Back Up the Active Cisco SD-WAN Manager Cluster Configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active Cisco SD-WAN Manager virtual machines.

1. Choose an active Cisco SD-WAN Manager node that hosts the configuration database service and export a backup the configuration database. On the CLI of the Cisco SD-WAN Manager node, run the following command: **request nms configuration-db backup path** *file-path*

   The command backs up the configuration database in a `.tar.gz` file and saves the file in the specified *file-path*.

   In the following example, the database is backed up to a file named `db_backup.tar.gz` in the `/home/admin/` directory.

   ```
   Active-vManage# request nms configuration-db backup path /home/admin/db_backup
   Successfully saved database to /home/admin/db_backup.tar.gz
   ```

2. Choose a standby Cisco SD-WAN Manager node that hosts the configuration database service and copy the configuration database backup to this node.

   In the following example, `db_backup.tar.gz` is copied from the active Cisco SD-WAN Manager node to the `/home/admin/` directory of a standby Cisco SD-WAN Manager node.

   ```
   Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
   admin@10.126.93.92:/home/admin
   The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
   ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
   viptela 18.4.5

   admin@10.126.93.92's password:
   db_backup.tar.gz                                  100%  399KB   4.4MB/s   00:00
   ```

### Restore Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

Restore the most recent backup of the configuration database from the active Cisco SD-WAN Manager cluster on the standby Cisco SD-WAN Manager node to which you copied this backup.

**Note**

- The restore operation does not restore all the information included in the configuration database. Cisco SD-WAN Manager configurations such as users and repositories must be configured on the standby Cisco SD-WAN Manager node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active Cisco SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

1. On the CLI of the standby Cisco SD-WAN Manager node, run the following command: **request nms configuration-db restore path** *file-path*

In the following example, the configuration database is restored using the backup file `db_backup.tar.gz`.

```
Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

2. Verify that the appropriate services are running on the standby Cisco SD-WAN Manager nodes: On the CLI of each standby Cisco SD-WAN Manager node, run the **request nms all status** command. From the command output, verify the services running on the node.
3. Verify that every standby Cisco SD-WAN Manager node has a list of all the active and standby Cisco SD-WAN Manager nodes.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   b. Verify that the page displays all active and standby Cisco SD-WAN Manager nodes.
4. Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

   In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.
5. Log in to the CLI of Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.

   In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.
6. On the standby Cisco SD-WAN Manager nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

   a. Enable the transport interface in VPN 0: On the CLI of each standby Cisco SD-WAN Manager node, run the **no shutdown** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# no shutdown
   Active-vManage(config-interface)# commit and-quit
   ```

   b. Activate the tunnel interface in VPN 0: On the CLI of each standby Cisco SD-WAN Manager node, run the **tunnel-interface** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# tunnel-interface
   Active-vManage(config-interface)# commit and-quit
   ```
7. Add each standby Cisco SD-WAN Manager node to the overlay network.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   b. Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

**c.** For a Cisco SD-WAN Validator, click **...** and click **Edit**.

**d.** In the **Edit** dialog box, enter the following details of the Cisco SD-WAN Validator: WAN transport IP address, username, and password.

**e.** Repeat **Step 7c** and **Step 7d** for every Cisco SD-WAN Validator.

**8.** Disconnect the active Cisco SD-WAN Manager nodes from the overlay network.

**Note** In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach Cisco SD-WAN Manager instances in an actual disaster scenario, you may not be able to perform this step and can omit this step.

Use one of the following two methods:

**a.** Shut down the transport interface in VPN 0: On the CLI of each active Cisco SD-WAN Manager node, run the **shutdown** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

**b.** Deactivate the tunnel interface in VPN 0: On the CLI of each active Cisco SD-WAN Manager node, run the **no tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

**9.** From the standby Cisco SD-WAN Manager, send the updated controller and device list to the Cisco SD-WAN Validator.

Send the list of controllers:

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

**b.** Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

**c.** Click **Send to Validator**.

Wait for the configuration task to complete. When the task is complete,

- The standby Cisco SD-WAN Manager nodes become the active Cisco SD-WAN Manager nodes.
- The previously active Cisco SD-WAN Manager nodes are no longer part of the overlay network.
- The active Cisco SD-WAN Manager nodes have the configuration from the most recent configuration database backup.
- Every controller establishes connection with the other controllers in the network.

**d.** Click **WAN Edge List**.

**e.** Click **Send to Controllers**.

**10.** Verify that the following are intact:

- Policies
- Templates
- Controller and WAN edge device lists

**11.** Verify the valid Cisco SD-WAN Manager nodes.

**a.** Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.

**b.** Log in to the CLI of a Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

**12.** Invalidate the previously active Cisco SD-WAN Manager nodes.

The previously active Cisco SD-WAN Manager is the certificate issuer for the cloud WAN edge devices. The active Cisco SD-WAN Manager issues certificates to the cloud WAN edge devices only after the previously active Cisco SD-WAN Manager nodes are invalidated.

**Note**

- After you invalidate the Cisco SD-WAN Manager nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.
- When you invalidate the previously active Cisco SD-WAN Manager nodes, Cisco SD-WAN Manager marks the nodes as invalid and sends an update to all controllers. However, Cisco SD-WAN Manager does not send an updated list of valid Cisco SD-WAN Manager UUIDs to Cisco SD-WAN Validator immediately because the previously active Cisco SD-WAN Manager is the CA for the cloud WAN edge devices. So, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator includes the UUIDs of the invalidated Cisco SD-WAN Manager nodes.

  Cisco SD-WAN Manager has a scheduled task that runs every 24 hours and checks to see if all the cloud WAN edges have been moved to the active Cisco SD-WAN Manager. Cisco SD-WAN Manager sends the updated list of valid Cisco SD-WAN Manager UUIDs to Cisco SD-WAN Validator only after the cloud WAN edge devices have been moved to the active Cisco SD-WAN Manager. After this list is received, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator does not include the UUIDs of the invalidated Cisco SD-WAN Manager nodes.

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

**b.** Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

**c.** For each previously active Cisco SD-WAN Manager node, click **...** and click **Invalidate**.

**13.** Verify the valid Cisco SD-WAN Manager nodes after 24 hours.

**a.** Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed.

**b.** Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controllers.

The Cisco SD-WAN Manager cluster that was initially the standby cluster is now the active Cisco SD-WAN Manager cluster.

# Multitenant Cisco SD-WAN Manager: Disaster Recovery After a Failed Data Center Becomes Operational

If a Multitenant Cisco SD-WAN Manager cluster or the data center hosting the Cisco SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby Cisco SD-WAN Manager cluster. You can perform disaster recovery as follows:

1. Deploy and configure a standby Cisco SD-WAN Manager cluster.

   The standby Cisco SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active Cisco SD-WAN Manager cluster periodically.

   Choose a Cisco SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active Cisco SD-WAN Manager cluster fails, restore the most recent configuration database on the standby Cisco SD-WAN Manager cluster, activate the standby Cisco SD-WAN Manager cluster, and remove the previously active Cisco SD-WAN Manager cluster from the overlay network.

   Choose a Cisco SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active Cisco SD-WAN Manager cluster.

To test disaster recovery, you can simulate a scenario in which the active Cisco SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

The following procedure applies to a scenario in which an initially active Cisco SD-WAN Manager cluster or the data center hosting the cluster failed and the standby Cisco SD-WAN Manager cluster was configured to be the active Cisco SD-WAN Manager cluster. If the cluster that was initially active becomes operational again, it serves as a standby cluster. By completing the following procedure, you can turn this standby cluster into the active cluster.

### Check the Configuration of the Standby Cisco SD-WAN Manager

1. Check whether the running configuration of the standby Cisco SD-WAN Manager nodes is similar to the running configuration of the active Cisco SD-WAN Manager nodes. Local certificates must be installed on the standby Cisco SD-WAN Manager nodes.

**Note** The running configuration on a standby Cisco SD-WAN Manager is usually identical to that of an active Cisco SD-WAN Manager node. However, you must ensure that settings such as the system IP address and the tunnel interface IP address are unique.

2. On the standby Cisco SD-WAN Manager nodes, shut down the transport interface in VPN 0: On the CLI, include the **shutdown** command in the transport interface configuration.

With the standby Cisco SD-WAN Manager nodes configured in this manner, the overlay network is not aware of the standby Cisco SD-WAN Manager cluster.

### Back Up the Active Cisco SD-WAN Manager Cluster Configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active Cisco SD-WAN Manager virtual machines.

1. Choose an active Cisco SD-WAN Manager node that hosts the configuration database service and export a backup the configuration database. On the CLI of the Cisco SD-WAN Manager node, run the following command: **request nms configuration-db backup path** *file-path*

   The command backs up the configuration database in a `.tar.gz` file and saves the file in the specified *file-path*.

   In the following example, the database is backed up to a file named `db_backup.tar.gz` in the `/home/admin/` directory.

   ```
   Active-vManage# request nms configuration-db backup path /home/admin/db_backup
   Successfully saved database to /home/admin/db_backup.tar.gz
   ```

2. Choose a standby Cisco SD-WAN Manager node that hosts the configuration database service and copy the configuration database backup to this node.

   In the following example, `db_backup.tar.gz` is copied from the active Cisco SD-WAN Manager node to the `/home/admin/` directory of a standby Cisco SD-WAN Manager node.

   ```
   Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
   admin@10.126.93.92:/home/admin
   The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
   ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
   viptela 18.4.5

   admin@10.126.93.92's password:
   db_backup.tar.gz                                  100%  399KB   4.4MB/s   00:00
   ```

### Restore Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

Restore the most recent backup of the configuration database from the active Cisco SD-WAN Manager cluster on the standby Cisco SD-WAN Manager node to which you copied this backup.

**Note**

- The restore operation does not restore all the information included in the configuration database. Cisco SD-WAN Manager configurations such as users and repositories must be configured on the standby Cisco SD-WAN Manager node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active Cisco SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

1. On the CLI of the standby Cisco SD-WAN Manager node, run the following command: **request nms configuration-db restore path** *file-path*

   In the following example, the configuration database is restored using the backup file `db_backup.tar.gz`.

   ```
   Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. Verify that the appropriate services are running on the standby Cisco SD-WAN Manager nodes: On the CLI of each standby Cisco SD-WAN Manager node, run the **request nms all status** command. From the command output, verify the services running on the node.
3. Verify that every standby Cisco SD-WAN Manager node has a list of all the active and standby Cisco SD-WAN Manager nodes.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   b. Verify that the page displays all active and standby Cisco SD-WAN Manager nodes.
4. On the standby Cisco SD-WAN Manager nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

   a. Enable the transport interface in VPN 0: On the CLI of each standby Cisco SD-WAN Manager node, run the **no shutdown** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

   b. Activate the tunnel interface in VPN 0: On the CLI of each standby Cisco SD-WAN Manager node, run the **tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

5. Add each standby Cisco SD-WAN Manager node to the overlay network.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   b. Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   c. For a Cisco SD-WAN Validator, click **...** and click **Edit**.
   d. In the **Edit** dialog box, enter the following details of the Cisco SD-WAN Validator: WAN transport IP address, username, and password.
   e. Repeat **Step 5c** and **Step 5d** for every Cisco SD-WAN Validator.
6. Disconnect the active Cisco SD-WAN Manager nodes from the overlay network.

**Note** In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach Cisco SD-WAN Manager instances in an actual disaster scenario, you may not be able to perform this step and can omit the step.

Use one of the following two methods:

**a.** Shut down the transport interface in VPN 0: On the CLI of each active Cisco SD-WAN Manager node, run the **shutdown** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

**b.** Deactivate the tunnel interface in VPN 0: On the CLI of each active Cisco SD-WAN Manager node, run the **no tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

**7.** From the standby Cisco SD-WAN Manager, send the updated controller and device list to the Cisco SD-WAN Validator.

Send the list of controllers:

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

**b.** Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

**c.** Click **Send to Validator**.

Wait for the configuration task to complete. When the task is complete,

- The standby Cisco SD-WAN Manager nodes become the active Cisco SD-WAN Manager nodes.
- The previously active Cisco SD-WAN Manager nodes are no longer part of the overlay network.
- The active Cisco SD-WAN Manager nodes have the configuration from the most recent configuration database backup.
- Every controller establishes connection with the other controllers in the network.

**d.** Click **WAN Edge List**.

**e.** Click **Send to Controllers**.

**8.** Verify that the following are intact:

- Policies
- Templates
- Controller and WAN edge device lists

**9.** Verify the valid Cisco SD-WAN Manager nodes.

**a.** Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.

**b.** Log in to the CLI of a WAN edge device and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

**10.** Invalidate the previously active Cisco SD-WAN Manager nodes.

**Note** After you invalidate the Cisco SD-WAN Manager nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

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

**b.** Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

**c.** For each previously active Cisco SD-WAN Manager node, click **...** and click **Invalidate**.

**11.** Verify the valid Cisco SD-WAN Manager nodes.

**a.** Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed.

**b.** Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controllers.

The Cisco SD-WAN Manager cluster that was initially the standby cluster is now the active Cisco SD-WAN Manager cluster.

# Replace Faulty Cisco SD-WAN Controller

To replace a faulty Cisco SD-WAN Controller with a new instance, follow these steps:

1. Create a Cisco SD-WAN Controller instance. See Deploy the Cisco SD-WAN Controller.
2. Add Cisco SD-WAN Controller to the overlay network.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
4. Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

5. For the faulty Cisco SD-WAN Controllers, click **...** and click **Invalidate**.

   The **Invalidate** dialog box appears.

**Note** If you have not added a new Cisco SD-WAN Controller that can replace the faulty Cisco SD-WAN Controller, Cisco SD-WAN Manager indicates this through an error message. Click **Cancel** in the **Invalidate** dialog box and add a new Cisco SD-WAN Controller before invalidating the faulty instance.

6. In the **Invalidate** dialog box, do the following:
   a. Check the **Replace Controller** check box.
   b. From the **Select Controller** drop-down list, choose the new Cisco SD-WAN Controller that should replace the faulty instance.
   c. Click **Invalidate**.

Cisco SD-WAN Manager launches the **Invalidate Device** and **Push CLI Tempalte Configuration** task. When these tasks are completed, the faulty Cisco SD-WAN Controller is invalidated and removed from the overlay network. The tenants that were served by the faulty Cisco SD-WAN Controller are now served by the new Cisco SD-WAN Controller that you chose as the replacement.

# RADIUS and TACACS Support for Multitenancy

*Table 251: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| RADIUS and TACACS Support for Multitenancy | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br>Cisco Catalyst SD-WAN Control Components Release 20.12.1 | This feature enables support for Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS) authentication in a multitenant deployment on WAN edge devices. |

## Information about RADIUS and TACACS Support for Multitenancy

From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco SD-WAN Manager supports for RADIUS and TACACS servers in a multitenant deployment.

### RADIUS

RADIUS is a distributed client and server system that secures networks that have authorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

### TACACS

TACACS is a security application that provides centralized validation of users attempting to gain access to an access point. Unlike RADIUS, TACACS does not authenticate wireless client devices accessing the network through an access point.

TACACS provides for separate and modular authentication, authorization, and accounting. Each service can be tied into its own database to take advantage of other services available on that server or on the network.

TACACS administered through the AAA security services can provide these services:

- Authentication: Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.
- Authorization: Provides fine-grained control of user privileges for the duration of the session, including access control, session duration, or protocol support. You can also enforce restrictions on the commands to execute a TACACS authorization feature.
- Accounting: Collects and sends information used for billing, auditing, and reporting to the TACACS daemon. Network managers can use the accounting feature to track administrator activity for security audit or to provide information for user billing. Accounting records include administrator identities, start and stop times, executed commands, number of packets, and number of bytes.

**Note** NAT is not supported between Cisco SD-WAN Manager and the multitenant connector.

# Prerequisites for Cloud Multitenant with On-Prem Per-tenant AAA and Provider AAA

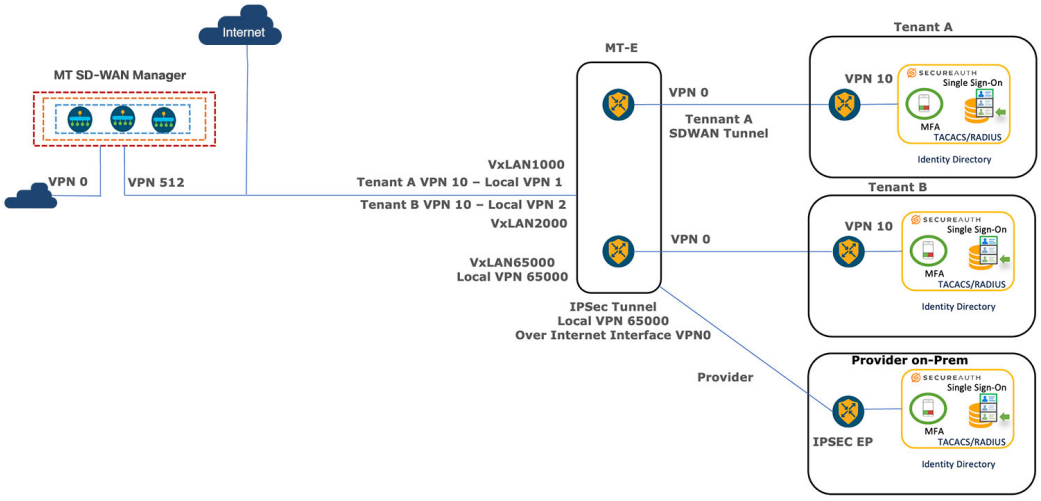
### Prerequisites for Cloud Multitenant with On-Prem Per-tenant AAA and Provider AAA

- A Multitenant edge connector is onboarded in Cisco SD-WAN Manager.
- Provider can have tenant configurations only through a device or feature template.
- The edge connector is on the same premises as the controllers.
- Cisco SD-WAN Manager is configured with VPN 512 interface.
- VxLAN tunnels must use the VPN 512 interface as the underlay.
- In a Cisco SD-WAN Manager cluster, there is a VxLAN tunnel created between each Cisco SD-WAN Manager node and the edge connector.
- A provider's RADIUS and TACACS server cannot be shared with the tenant.
- RADIUS and TACACS server authentication is within the tenant network.
- Multiple RADIUS and TACACS servers are used for the same tenant.
- A tenant's RADIUS and TACACS server is on-prem or cloud-hosted.

**Note** You must configure an external AAA server and provide mapping between the user and the Viptela groups to authentication. For example, Viptela-Group-Name as basic, tenantadmin, or operator.

The following illustration shows the architecture of the cloud multitenancy with on-prem per tenant and provider AAA.

*Figure 8: Cloud Multitenant with On-Prem Per-tenant and Provider AAA*




# Workflows to Configure Remote AAA

### Enable Multitenancy

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit** adjacent to the **Tenancy Mode Tenancy Mode**. If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.
3. Click **Multitenant**.
4. In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).
5. Enter a **Cluster Id** (for example, cluster-1 or 123456).
6. Click **Save**. If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, 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.

For information about configuring AAA using feature templates for a single tenant, see Configuring AAA using Cisco SD-WAN Manager Template.

## Configure the Tenant

To on board the Edge Connector in a Cisco SD-WAN Manager provider, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
2. Click **Edit** adjacent to the **Tenant**.

   The **Edit Tenant** window is displayed.
3. Enter the description in the **Description** field.

4. Enter the edge number in the **Forecasted Edge** field.
5. Enter the sub-domain URL in the **URL Subdomain** field.
6. Enable the **Edge Connector** option.
7. Choose the **Edge Connector IP** from the drop-down list.
8. Choose the VxLAN tunnel endpoint from the **Edge Connector VTEP Interface Name** drop-down list.
9. Click **Save**.

# Configure Remote AAA

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

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **Remote AAA**.
3. Expand the **Remote AAA** tab to configure remote AAA.
4. Enter the order in which to attempt different authentication methods in the **Authentication Order** field.
5. Choose the option in **Authentication Fallback** to fallback if higher-priority authentication fails.
6. Choose the **Admin Authentication Order** to authenticate a tenantadmin user according to the authentication order.
7. Enable or disable audit logs in the **Disable Audit Logs** field.
8. Enable or disable user accounting in the **Enable/disable user accounting** field.
9. Click **Save** to save the changes.

## Configure RADIUS

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **Remote AAA**.
3. Expand the **RADIUS** tab to configure a RADIUS server.
4. Enter the number of times you want to contact a RADIUS server in the **Retransmit Count** field.
5. Enter the duration to wait for replies from the RADIUS server in the **Timeout** field.
6. Click **New RADIUS Server** to add a new RADIUS server.

| Field | Description |
|---|---|
| **Timeout** | Enter the duration to wait for a reply from the RADIUS server. |
| **Retransmit Count** | Enter the number of times you want to contact each RADIUS server. |
| **Address** | Enter the IP address of the RADIUS server. |

| Field | Description |
|---|---|
| **Accounting Port** | Enter the port used to connect to the server. |
| **Key** | Enter the password to access the RADIUS server. |
| **VPN ID** | Enter the VPN in which the RADIUS server. |
| **Priority** | Enter the server priority. |
| **Authentication Port** | Enter the port to connect to the RADIUS server. |
| **Secret Key** | Enter the AES encrypted key to access the RADIUS server. |
| **VPN IP Subnet** | Enter the VPN IP subnet (VxLAN tunnel VPN IP subnet) in which the RADIUS server is located. |

7. Click **Save** and **Add**.

## Configure TACACS

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **Remote AAA**.
3. Expand the **TACACS** tab to configure TACACS.
4. Enter the duration to wait for replies from the TACACS server in the **Timeout** field.
5. Choose the TACACS authentication type from the **Authentication** drop-down list.
6. Click **New TACACS Server** to add a new TACACS server.

| Field | Description |
|---|---|
| **Timeout** | Enter the duration to wait for replies from the TACACS server. |
| **Authentication Type** | Choose the TACACS authentication type. The options are:<br>• ASCII<br>• PAP |
| **Address** | Enter the IP address of the TACACS server. |
| **Key** | Enter the password to access the TACACS server. |
| **VPN ID** | Enter the VPN in which the TACACS server. |
| **Priority** | Enter the server priority. |
| **Authentication Port** | Enter the port to connect to a TACACS server. |
| **Secret Key** | Enter the AES encrypted key to access the TACACS server. |
| **VPN IP Subnet** | Enter the VPN IP subnet in which the TACACS server is located. |

7. Click **Add**.

# Verify RADIUS and TACACS Configuration for Multitenancy

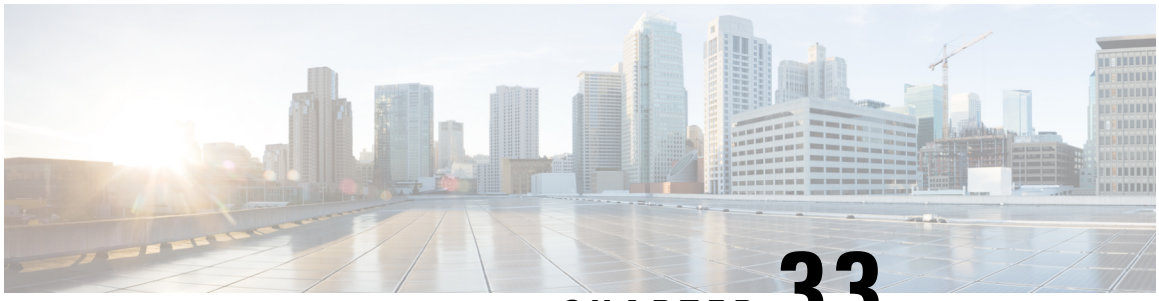
The following is a RADIUS and TACACS configuration example on Cisco IOS XE Catalyst SD-WAN devices through CLI:

```
Device# interface GigabitEthernet4

 description   VTEP Interface

 no shutdown

 arp timeout 1200

 ip address 172.1.1.101 255.255.255.0

 no ip redirects

 ip mtu    1500

 load-interval 30

 mtu           1500

 negotiation auto

exit
```

Use the **show ip interface brief** command to show the AAA configuration:

```
Device# show ip interface brief | i <VPN IP SUBNET of VxTunnel>

Where <VPN IP SUBNET of VXTunnel> is one that is configured under Tenant - > Administration
 -> Remote AAA
```

The output shows one tunnel per one node. If there are three nodes in a cluster, the output displays three tunnels in the subnet.



CHAPTER 33

# 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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 252: 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. |


- Information About Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers, on page 980
- Restrictions for Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers, on page 981
- Assign Cisco SD-WAN Controllers to Tenants During Onboarding, on page 981
- Update Cisco SD-WAN Controllers Placement For a Tenant, on page 986

# Information About Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers

### Automatic Tenant Placement by Cisco SD-WAN Manager

In Cisco vManage Release 20.8.x and earlier releases, when you onboard a tenant, Cisco SD-WAN Manager assigns a pair of multitenant Cisco SD-WAN Controllers to the tenant based on an internal algorithm that considers factors such as the following:

- number of tenant WAN edge devices that you forecast for the tenant
- number of tenants served by a pair of multitenant Cisco SD-WAN Controllers
- number of WAN edge devices connected to a pair of multitenant Cisco SD-WAN Controllers

After the tenant is onboarded, if the tenant needs to add more devices than you originally forecast, you can modify the forecast if the pair of multitenant Cisco SD-WAN Controllers serving the tenant can accommodate these additional WAN edge devices. If the Cisco SD-WAN Controllers cannot accommodate the additional WAN edge devices, you must delete the tenant and onboard the tenant again with the revised device forecast so that Cisco SD-WAN Manager assigns a suitable pair of Cisco SD-WAN Controllers. If none of the pairs of multitenant Cisco SD-WAN Controllers can accommodate the revised device forecast, add a new pair of Cisco SD-WAN Controllers and then onboard the tenant.

### Flexible Tenant Placement by Provide Admin User

From Cisco vManage Release 20.9.1, while onboarding a tenant, you have the flexibility to choose the pair of multitenant Cisco SD-WAN Controllers that are assigned to the tenant. Automatic tenant placement by Cisco SD-WAN Manager continues to be the default behavior with flexible tenant placement as an optional configuration.

To help you with flexible tenant placement, Cisco SD-WAN Manager lists available multitenant Cisco SD-WAN Controllers and provides the following details, as a percentage, for each controller:

- number of tenants assigned
- number of tenant WAN edge devices connected
- memory utilized
- CPU utilized

A multitenant Cisco SD-WAN Controller can serve a maximum of 24 tenants and 1000 tenant WAN edge devices across all the tenants. While onboarding a tenant, choose a pair of controllers that can be assigned one more tenant and can also connect to the number of WAN edge devices forecast for the tenant.

After the tenant is onboarded, if the tenant needs to add more devices than you originally forecast and the assigned pair of multitenant Cisco SD-WAN Controllers cannot connect to these additional WAN edge devices, you can migrate the tenant to another pair of Cisco SD-WAN Controllers that can serve one more tenant and accommodate the revised WAN edge device forecast for the tenant. If none of the multitenant Cisco SD-WAN Controllers pairs can accommodate the revised device forecast, you can migrate other tenants to alternative Cisco SD-WAN Controllers so that the controller utilization is efficient and the tenant assignment is optimal.

If the optimization doesn't create the capacity required to accommodate the revised device forecast for the tenant, add a new pair of Cisco SD-WAN Controllers and then migrate the tenant.

## Benefits of Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers

- Choose Cisco SD-WAN Controllers deployed in different failure zones to reduce the probability of both the controllers failing simultaneously. In a cloud environment, choose controllers deployed in different regions.
- Choose Cisco SD-WAN Controllers deployed in the same geographical region as the tenant WAN edge devices to reduce latency.
- Choose Cisco SD-WAN Controllers based on the CPU, DRAM, and hard disk resources allocated, and the utilization of these resources.
- Migrate a tenant to a different Cisco SD-WAN Controller to accommodate changes in the tenant device forecast.

# Restrictions for Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers

If you wish to migrate a tenant to different pair of Cisco SD-WAN Controllers, you must change the Cisco SD-WAN Controllers 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.

# 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 **Manager** 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 **Manager**.
- 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.<br>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.<br>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.<br>The organization name is case-sensitive. Each tenant or customer must have a unique organization name.<br>Enter the organization name in the following format:<br>`<SP Org Name>-<Tenant Org Name>`<br>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.<br>• 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.<br>**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**.<br>• 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.<br>• 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`.<br>**Note** If you fail to add the DNS A record, you will experience authentication errors when logging in to Cisco SD-WAN Manager.<br>Validate that the DNS is configured correctly by using the **nslookup** command. Example: `nslookup vmanage123.sdwan.cisco.com` .<br>• 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`.<br>Cluster ID is not required in the CNAME record.<br>Validate that the DNS is configured correctly by using the **nslookup** command. Example: `nslookup customer1.sdwan.cisco.com`.<br>• 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.<br><br>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 Controllers</td><td>• Automatic tenant placement: Ensure that the Select two Controllers field has the value Autoplacement. This is the default configuration.<br><br>• Flexible tenant placement:<br><br>a. Click the Select two Controllers drop-down list.<br><br>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:<br><br>
<table>
<tr><td>Tenant hosting capacity</td><td>Each Cisco SD-WAN Controller can serve a maximum of 24 tenants. Tenant hosting capaci represents the number of tenants to which the C SD-WAN Controller is assigned in the form of percentage. This value indicates whether you c 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. U device capacity represents the number of tenan WAN edge devices connected to the Cisco SD-W Controller in the form of a percentage of the maximum capacity (1000 WAN edge devices). 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 percentage.</td></tr>
<tr><td>CPU utilized</td><td>This value represents CPU usage as a percenta</td></tr>
</table>
<br>b. Select two Cisco SD-WAN Controllers to assign to the tenant based on the utilization details.<br><br>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.

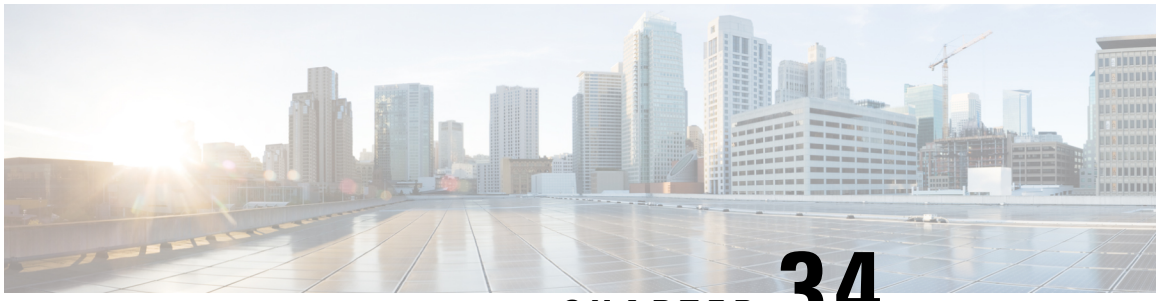
1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
3. For the tenant you wish to migrate to a different controller, click **…** adjacent to the tenant organization name.
4. Click **Update Controller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

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



CHAPTER 34

# Multitenant WAN Edge 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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 253: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Multitenant WAN Edge Devices | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a<br>Cisco vManage Release 20.7.1 | With this feature, a service provider can deploy, configure, and manage multitenant WAN edge devices in a multitenant Cisco Catalyst SD-WAN deployment. |
| Distribute Device Resources Among Tenants Using Tiers | Cisco IOS XE Catalyst SD-WAN Release 17.8.1a<br>Cisco vManage Release 20.8.1 | With this feature, you can define tiers and assign tenants to tiers. While defining a tier, you limit the amount of a multitenant WAN edge resource that is allocated to a tenant in the tier, when the tenant is onboarded to a multitenant WAN edge device.<br>From this release, you can specify how many tenant VPNs can be created for a tenant belonging to a tier. In subsequent releases, tiers will be enhanced to support limits on the usage of additional device resources such as firewall, NAT, and TLOCs. |

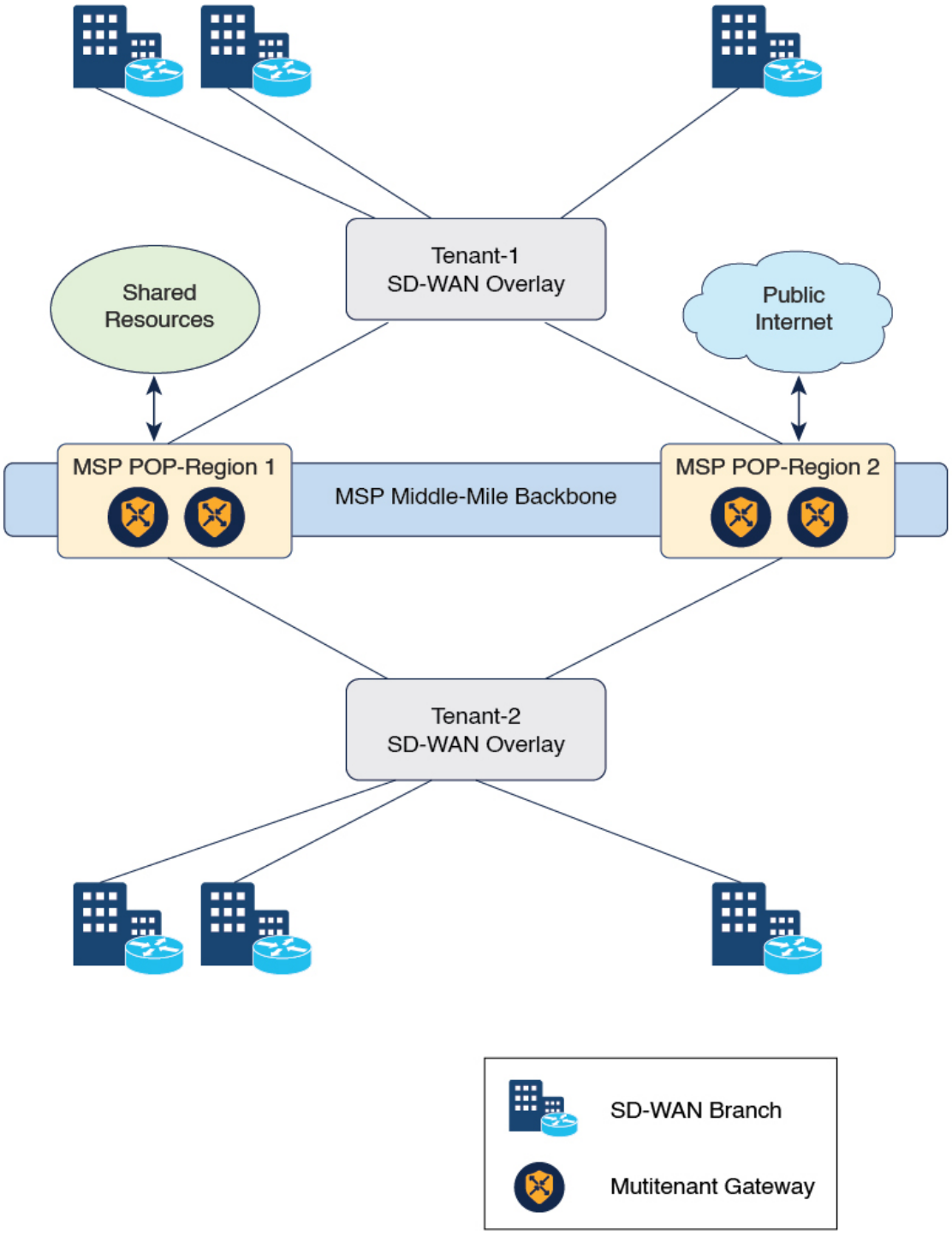
| Feature Name | Release Information | Description |
|---|---|---|
| Enhanced Multitenant Tier Definition to include Route and TLOC Resource-Usage Limits | Cisco IOS XE Catalyst SD-WAN Release 17.10.1a<br>Cisco vManage Release 20.10.1 | This feature is enhanced to support route and TLOC resource-usage limits. A service provider can assign a tier to limit the routes and TLOC resource-usage to the tenant based on the service agreement. |
| Enhanced Multitenant Tier Definition to include NAT Limits | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br>Cisco Catalyst SD-WAN Manager Release 20.12.1 | With this feature, you can configure maximum limit on NAT translations per tenant.<br>From this release **Tier** is called **Resource Profile** in Cisco SD-WAN Manager. |


- Information About Multitenant WAN Edge Devices, on page 990
- Supported Devices for Multitenant WAN Edge Devices, on page 993
- Prerequisites for Multitenant WAN Edge Devices, on page 994
- Restrictions for Multitenant WAN Edge Devices, on page 994
- Configure Multitenant WAN Edge Devices, on page 995
- Verify Configuration and Operation of Multitenant WAN Edge Devices, on page 1004
- Troubleshoot Multitenant WAN Edge Device Errors, on page 1017


# Information About Multitenant WAN Edge Devices

As a service provider managing a multitenant Cisco Catalyst SD-WAN deployment, you may wish to deploy a multitenant WAN edge device in the overlay network to serve as a shared gateway for traffic belonging to multiple tenants. For example, you can deploy such a shared gateway in each regional point of presence (PoP). You can carry inter-region traffic belonging to multiple tenants through these shared gateways and the transport backbone linking the PoPs.

*Figure 9: Multitenant WAN Edge Devices as Shared Gateways*




Multitenant WAN edge devices isolate traffic belonging to different tenants by mapping a tenant service VPN (referred to as tenant VPN) to a device VPN (also referred to as the device VRF). Cisco SD-WAN Manager performs the mapping between the tenant and device VPNs when you onboard a tenant on a multitenant WAN edge device.

Multitenant WAN edge devices establish control connections with the Cisco SD-WAN Validator nodes specified in the bootstrap configuration, and then connect to nodes in the Cisco SD-WAN Manager cluster. When you onboard a tenant to a multitenant WAN edge device, the device establishes control connections to the Cisco SD-WAN Controller assigned to the tenant.

The service provider must deploy, configure, and manage multitenant WAN edge devices. The devices and their states are displayed only in the Cisco SD-WAN Manager provider view. The provider, acting on behalf of the tenant, must deploy, configure, and manage single-tenant WAN edge devices owned by a tenant. The devices and their states are displayed in the tenant view or the provider-as-tenant view. When a tenant is onboarded to a multitenant WAN edge device, the multitenant WAN edge device can interoperate with single-tenant WAN edge devices owned by the tenant and other multitenant WAN edge devices to which the tenant is onboarded.

# Resource Profiles (Tiers)

When you onboard many tenants on a multitenant WAN edge device, you may need to distribute the limited device resources among the tenants to ensure fair usage of resources or to implement different service-level agreements (SLAs). A tier lets you define and limit how much of each device resource a tenant assigned to the tier can consume. After creating a tier, when you onboard a tenant, you assign a tenant to a particular tier to apply the resource-usage limits to the tenant.

### Usage Notes

- After you create a tier, you cannot modify the device-resource-usage limits specified in the tier. To apply a different set of limits to tenants, you must create a new tier and assign the relevant tenants to the new tier.
- You can delete a tier only when no tenants are assigned to it.

### Resource Usage Limits in Resource Profiles (Tiers)

*Table 254: Resource Usage Limits in Tiers*

| Resource Usage Limit | Description | Available From |
|---|---|---|
| Number of VPNs | Maximum number of tenant VPNs that can be created for a tenant belonging to the tier.<br>Cisco SD-WAN Manager enforces the limit when you create a new tenant VPN for a tenant.<br>• If you have already created the maximum number of tenant VPNs specified in the tier, Cisco SD-WAN Manager reports the error and doesn't apply the configuration. | Cisco IOS XE Release 17.8.1 and Cisco vManage Release 20.8.1 |

| Resource Usage Limit | Description | Available From |
|---|---|---|
| Route-limit | The number of IPv4 unicast and IPv6 unicast routes that can be created for a tenant belonging to the tier.<br>Route limit on a tenant is the sum of routes from all VRFs. | Cisco IOS XE Catalyst SD-WAN Release 17.10.1a<br>Cisco vManage Release 20.10.1 |
| TLOC | TLOC allows you to map transport interfaces to tenants. At least one TLOC needs to be selected per tier and you can include up to 16 TLOCs in a tier. | Cisco IOS XE Catalyst SD-WAN Release 17.10.1a<br>Cisco vManage Release 20.10.1 |
| NAT limit | The maximum limit on the number of NAT translations per tenant.<br>Once the maximum limit has reached for a tenant, the packets are dropped and further translations are not allowed. | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br>Cisco Catalyst SD-WAN Manager Release 20.12.1 |

## Benefits of Multitenant WAN Edge Devices

As a managed service provider, by deploying multitenant WAN edge devices, you can

- reuse the edge devices and the interconnecting transport backbone to serve multiple tenants
- lower capital and operational expenditure
- provide faster access to tenants to shared resources, SaaS, and IaaS through the shared transport backbone
- manage tenant association with the devices, tenant-specific policies, and QoS requirements with Cisco SD-WAN Manager as the unified management interface

# Supported Devices for Multitenant WAN Edge Devices

| Device Family | Device Model |
|---|---|
| Cisco ASR 1000 Series Aggregation Services Routers | ASR 1001-HX<br>ASR 1001-X<br>ASR 1002-HX<br>ASR 1002-X<br>**Note** Cisco IOS XE Catalyst SD-WAN Release 17.9.1a is the last supported release for ASR 1001-X and ASR 1002-X. |

| | |
|---|---|
| Cisco Catalyst 8000V Edge Software | Catalyst 8000V |
| Cisco Catalyst 8300 Series Edge Platforms | C8300-1N1S-4T2X<br>C8300-1N1S-6T<br>C8300-2N2S-4T2X<br>C8300-2N2S-6T |
| Cisco Catalyst 8500 Series Edge Platforms | C8500-12X<br>C8500-12X4QC<br>C8500L-8S4X |
| Cisco ISR 4000 Series Integrated Services Routers | ISR 4461 |

# Prerequisites for Multitenant WAN Edge Devices

- You must have completed the initial setup for a multitenant Cisco Catalyst SD-WAN deployment.
  - Multitenant Cisco SD-WAN Validator and Multitenant Cisco SD-WAN Controller must run Cisco SD-WAN Release 20.7.1 or a later release software.
  - Multitenant Cisco SD-WAN Manager must run Cisco vManage Release 20.7.1 or a later release software.
  - Cisco IOS XE Catalyst SD-WAN devices must run Cisco IOS XE Release 17.7.1 or a later release software.

# Restrictions for Multitenant WAN Edge Devices

- The provider must own, deploy, and manage all multitenant WAN edge devices in the deployment. The provider must also deploy and manage any single-tenant device owned by a specific tenant.
- You must configure unique system IP address for each WAN edge device in the multitenant Cisco Catalyst SD-WAN deployment, irrespective of whether the device is a multitenant device owned and managed by the provider or a single-tenant device owned by a tenant and managed by the provider on behalf of the tenant.
- You can configure a maximum of 16 SLA classes. You can either assign specific SLA classes to tenants or share SLA classes among tenants.
- You cannot migrate a single-tenant WAN edge device from the tenant-level to serve as a multitenant WAN edge device at the provider-level. You must decommission the single-tenant device and delete it from Cisco SD-WAN Manager, perform a factory reset on the device to erase the existing configuration, and onboard the device at the provider-level.
- Multitenant WAN edge device do not support the following:
  - Cloud Express and Multicloud workflows

- Zone-Based Firewall (ZBFW) and advanced security features
- Per-tenant DPI statistics
- Dynamic on-demand tunnels
- SNMP
- Per-tenant management of NAT resources
- OMP IPv6 route filtering
- OMP notifications

- Tenant limits takes precedence when VRF limits are also configured.

# Configure Multitenant WAN Edge Devices

### Configuration Workflow

Perform the following configuration procedures as the Provider admin user.

1. Complete Initial Setup for Multitenancy.
   a. Add Tenants.
   b. (Optional) Onboard Tenant-Owned WAN Edge Devices.

**Note** As the provider admin, you must onboard the devices from the provider-as-tenant view. Configure unique system IP address for each WAN edge device in the deployment across all tenant overlay networks.

2. Enable Multitenant WAN Edge Deployment.
3. Onboard WAN Edge Devices at the Provider Level.

**Note**
- Importing WAN edge device details from the Plug and Play (PnP) portal to Cisco SD-WAN Manager using **Sync Smart Account** is not supported. Export the device serial file from the PnP portal and import the file to Cisco SD-WAN Manager.
- Configure unique system IP address for each WAN edge device in the deployment across all tenant overlay networks.

4. Enable Multitenancy on Provider-Managed WAN Edge Devices.
5. Create Tiers.
6. Onboard Tenants to a Multitenant WAN Edge Device.
7. Create Tenant VPN for Onboarded Tenants.

8. (Optional) Configure Required Policies.

# Enable Multitenant WAN Edge Deployment

### Before You Begin

Ensure that every WAN edge device in the deployment, across tenants, is configured with a unique system IP address.

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
3. Find **MT Edge Deployment Settings** and click **Edit**.
4. For **Enable MT Edge Deployment**, click **Enabled**.

   By default, **Enable MT Edge Deployment** is **Disabled**.
5. Click **Save**.

If two or more WAN edge devices in the deployment are configured with the same system IP address, Cisco SD-WAN Manager reports an error. Modify the configuration of the WAN edge devices and try to enable multitenant WAN edge deployment.

# Onboard WAN Edge Devices at the Provider Level

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. Upload the device serial number file to Cisco SD-WAN Manager. While uploading the file, choose the option to validate and send the device list to controllers.
3. Bootstrap the device using bootstrap configuration generated through Cisco SD-WAN Manager or manually create the initial configuration on the device.
4. If you are using Enterprise Certificates to authenticate the device, download the Certificate Signing Request (CSR) from Cisco SD-WAN Manager and get the CSR signed by the Enterprise CA. Install the certificate on Cisco SD-WAN Manager.
5. Create a configuration template for the device and attach the device to the template.

   While configuring the device, configure the service provider organization name as `sp-organization-name` and the tenant `organization-name`.

# Enable Multitenancy on Provider-Level WAN Edge Devices

You can enable multitenancy on a provider-level WAN edge using the Multi Tenant parameter in the System template.

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Click **Feature**.

4. Find the System template of the provider-level WAN edge device for which you wish to enable multitenancy.
5. For the System template, click **…** and click **Edit**.
6. In the Basic Configuration area, find the **Multi Tenant** parameter. Initially, the parameter has a default scope and the default value **Off**. For the **Multi Tenant** parameter,
   a. Click the scope drop-down list and choose **Global** scope.
   b. Click **On** to enable multitenancy.
7. Click **Update** to save and apply the modified configuration.

The provider-level WAN edge device can serve more than one tenant.

# Create a Resource Profile (Tier)

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 **Resource Profiles**.

   In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profiles** is called **Tiers**.

   Any existing tiers are displayed in a table.
4. Click **Add a Resource Profile**.

   In Cisco vManage Release 20.11.1 and earlier releases, **Add a Resource Profile** is called **Add Tier**.
5. In the **Add Tier** slide-in pane, do the following:
   a. Enter the following details:

| Field | Description |
|---|---|
| **Resource Profile Name**<br>In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profile Name** is called **Tier Name**. | Enter a unique name for the tier. |
| **Maximum VPN** | Enter the maximum number of VPNs that can be created on a multitenant WAN edge device for a tenant assigned to this tier.<br>Minimum value: 1<br>Maximum value: The maximum number of VPNs that you can specify for a tier depends on the device model. See Table 255: Maximum Number of VPNs Supported by Each Device Model, on page 999. |

| Field | Description |
|---|---|
| **NAT Limit (Optional)** | Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1<br><br>Enter the maximum number of NAT translations that are allowed on each tenant. |
| **Route Limit (Optional)** | Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1<br><br>(Optional) Specify IPv4 unicast or IPv6 unicast route limits. Route limit on a tenant is the sum of routes from all VRFs.<br><br>Default value is 0.<br><br>**Note** The value 0 means there is no route limit configured in the tier definition. |
| **Route Limit Type** | Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1<br><br>The following two route limit types can be configured for IPv4 or IPv6 routes on the device:<br><br>• **Warning-only**: This option allows to install new tenant IPv4 or IPv6 routes even after total exceeds their respective limit. A warning message is shown on device console when IPv4 route limit or IPv6 route limit is exceeded.<br><br>• **Warning with threshold**: This option allows to configure a warning threshold, which is the percentage of the route limit. A warning message is shown on device console when the threshold percentage of IPv4 route limit or IPv6 route limit is reached. When a tenant's total IPv4 or IPv6 routes exceed the configured IPv4 or IPv6 route limit, routes are rejected. |
| **Threshold** | Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1<br><br>Specify the route limit threshold value when you chose **Warning with threshold** option. When threshold percentage of IPv4 or IPv6 route limit is reached, a warning message is displayed on the device console.<br><br>Range: 1 to 100. |

| Field | Description |
|---|---|
| **Allowed Transport**<br>In Cisco vManage Release 20.11.1 and earlier releases, **Allowed Transport** is called **TLOC**. | Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1<br>Add TLOC details for the tier. For a tier, add at least one TLOC and up to 16 TLOCs. A TLOC definition includes the TLOC color and the encapsulation type.<br>Range: 1 to 16 |
| **Color** | Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1<br>Select the color from the drop-down list. The color attribute helps to identify an individual WAN transport tunnel. |
| **Encapsulation** | Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1<br>Select encapsulation type as either GRE or IPSec per TLOC configuration. |

***Table 255: Maximum Number of VPNs Supported by Each Device Model***

| Device Model | Maximum Number of VPNs |
|---|---|
| ASR1001-X | 80 |
| ASR1001-HX | 336 |
| ASR1002-X | 336 |
| ASR1002-HX | 336 |
| C8500-12X4QC | 336 |
| C8500-12X | 336 |
| C8500L-8S4X | 336 |
| C8300-1N1S-6T | 200 |
| C8300-1N1S-4T2X | 200 |
| C8300-2N2S-6T | 200 |
| C8300-2N2S-4T2X | 200 |
| Catalyst 8000V | 300 |
| ISR4461 | 80 |

**b.** To add the tier, click **Save**. To discard your entries and close the slide-in pane, click **Cancel**.

After you click **Save**, the slide-in pane is closed and the new tier is listed in the table along with any existing tiers.

# Onboard Tenants to a Multitenant WAN Edge Device

You can onboard tenants to a multitenant WAN edge device using the Tenant template. If you haven't onboarded a tenant to the device, create a tenant template, add tenants, and attach the tenant template to the device template. If you have onboarded tenants to the device, to onboard a new tenant, update the tenant template attached to the device.

When a new tenant is onboarded to the multitenant WAN edge device, the device establishes control connections to the Cisco SD-WAN Controllers assigned to the tenant.

### Before You Begin

Before onboarding the tenant to a multitenant WAN edge device, add the tenant to the multitenant deployment and create the tier with which you wish to associate the tenant.

### Create a Tenant Template

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Find the device template for the multitenant WAN edge device to which you wish to onboard tenants.
4. For the device template, click **…** and click **Edit**.

   The device template is displayed.
5. Click **Additional Templates**.
6. In the **Additional Templates** area, click the **Tenant** template drop-down list and then click **Create Template**.
7. In the Tenant template form, do as follows:
   a. Enter a unique **Template Name**. The template name can contain up to 128 alphanumeric characters.
   b. Enter a **Description** for the template. The description can contain up to 2048 alphanumeric characters.
   c. In the **Tenant** area, click **New Tenant**.
   d. From the **Tenant Name** drop-down list, choose the tenant organization name.

      In Cisco vManage Release 20.11.1 and earlier releases, **Tenant Name** is called **Org Name**.
   e. From the **Resource Profile Name** drop-down list, choose a tier for the tenant.

      In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profile Name** is called **Tier Name**.
   f. Click **Add**.
   g. Repeat **Step c** to **Step f** to add additional tenants.
8. Click **Save**.
9. For the device template, click **Update** to save and apply the modified configuration.
10. Select the target device in the left pane and click **Configure Devices**.

### Update a Tenant Template

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Click **Feature**.
4. For the tenant template attached to the device, click **…** and click **Edit**.

   The tenant template is displayed.
5. In the Tenant template form, do the following:
   a. In the **Tenant** area, click **New Tenant**.
   b. From the **Org Name** drop-down list, choose the tenant organization name.
   c. From the **Tier Name** drop-down list, choose a tier for the tenant.
   d. Click **Add**.
   e. Repeat **Step a** to **Step d** to add additional tenants.
6. Click **Update**.

# Create Tenant VPN for Onboarded Tenants

After onboarding a tenant to a multitenant WAN edge device, use the Cisco VPN template to create tenant VPNs. To isolate VPN traffic of one tenant from the VPN traffic of other tenants onboarded on the multitenant WAN edge device, Cisco SD-WAN Manager maps a tenant VPN ID to a device VPN ID while you create the tenant VPN.

### Create a Cisco VPN Template

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Find the Device template for the multitenant WAN edge device to which you wish to onboard tenants.
4. For the device template, click **…** and click **Edit**.

   The device template is displayed.
5. Click **Service VPN**.
6. In the **Service VPN** area, click **Add VPN**.
7. In the **Add VPN** slide-in pane, click **Create VPN Template**.
8. In the **Create VPN Template** slide-in pane, do the following:
   a. Enter a unique **Template Name**. The template name can contain up to 128 alphanumeric characters.
   b. Enter a **Description** for the template. The description can contain up to 2048 alphanumeric characters.
   c. In the **Basic Configuration** area, map the tenant VPN ID to a device VPN ID:
      1. From drop-down list corresponding to **Tenant VPN**, choose the tenant organization name.

2. In the text field corresponding to **Tenant VPN**, enter the tenant VPN ID.
3. Click **Generate VPN ID**.

   A read-only **VPN** field displays the device VPN ID for the tenant VPN ID. This mapping is performed by Cisco SD-WAN Manager. For a tenant, Cisco SD-WAN Manager maps a particular tenant VPN ID to the same device VPN ID on all the multitenant WAN edge devices.

**d.** Configure other properties of the tenant VPN in the template.

**e.** Click **Save**.

**9.** In the **Add VPN** slide-in pane, move the template created in **Step 8** from **Available VPN Templates** to **Selected VPN Templates**.

**10.** Click **Next**.

**11.** Add any additional Cisco VPN templates as needed.

**12.** Click **Add**.

**13.** For the device template, click **Update** to save and apply the modified configuration.

**14.** Select the target device in the left pane and click **Configure Devices**.

### Update a Cisco VPN Template

If you made a copy of an existing Cisco VPN template, you must modify the template for the new tenant VPN that you wish to create.

**1.** Log in to Cisco SD-WAN Manager as the Provider admin user.

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

**3.** Click **Feature**.

**4.** For the copied Cisco VPN template, click **…** and click **Edit**.

The Cisco VPN template is displayed.

**5.** In the Cisco VPN template form, do the following:

**a.** In the **Basic Configuration** area, map the tenant VPN ID to a device VPN ID:

1. From drop-down list corresponding to **Tenant VPN**, choose the tenant organization name.
2. In the text field corresponding to **Tenant VPN**, enter the tenant VPN ID.
3. Click **Update VPN ID**.

   A read-only **VPN** field displays the device VPN ID for the tenant VPN ID. This mapping is performed by Cisco SD-WAN Manager. For a tenant, Cisco SD-WAN Manager maps a particular tenant VPN ID to the same device VPN ID on all the multitenant WAN edge devices.

**b.** Configure other properties of the tenant VPN in the template.

**c.** Click **Update**.

**6.** Attach the Cisco VPN template to the device template of the target multitenant WAN edge device.

When you try to apply the tenant VPN configuration to the device, Cisco SD-WAN Manager checks the following:

1. The number of tenant VPNs that can be created for a tenant is restricted by the maximum number of the VPNs that is specified in the tier to which the tenant belongs. If the maximum number of tenant VPNs is already created for the tenant, Cisco SD-WAN Manager reports an error and does not apply the VPN configuration to the device.
2. Each device model supports a certain maximum number of device VPNs. On a multitenant WAN edge device, each tenant VPN is mapped to device VPN. If the maximum number of device VPNs supported by the device are already created and mapped to tenant VPNs, Cisco SD-WAN Manager reports an error and does not apply the configuration to the device.

# Remove Tenant from a Multitenant WAN Edge Device

To remove a tenant from a multitenant WAN Edge Device, you must detach the tenant service VPN template from the device template and delete the tenant from the Tenant template.

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. Remove the tenant service VPN template from the Device template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Find the device template for the multitenant WAN edge device to which you wish to onboard tenants.
   c. For the device template, click **…** and click **Edit**.

      The device template is displayed.
   d. Click **Service VPN**.
   e. In the **Service VPN** area, check the check box for the VPN template to be removed.
   f. Click **Remove VPN**.
   g. Click **Update** to save and apply the modified configuration.
3. Delete tenant from the Tenant template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature**.
   c. Find the Tenant template from which you should delete the tenant.
   d. For the Tenant template, click **…** and click **Edit**.
   e. In the Tenant section, find the organization name of the tenant you wish to delete.
   f. Click the Trash icon corresponding to the tenant organization name.
   g. Click **Update** to save and apply the modified configuration.

# Delete a Tier

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 **Tiers**.

   Existing tiers are displayed in a table.
4. For the desired tier, click **…** in the **Actions** column, and then, click **Delete**.
5. In the **Delete Tier** dialog box, confirm that you wish to delete the tier.

   The tier is deleted and is no longer listed in the table.

# Verify Configuration and Operation of Multitenant WAN Edge Devices

### View Tenants Onboarded to Multitenant WAN Edge Device

- The following is a sample output of the **show sdwan running-config tenant** command.

```
Device# show sdwan running-config tenant

tenant "multitenancy-Customer1"
 tier
  tier-name tier_tenant1
  max-vpn   10
 !
 tenant-vpn 1
  device-vpn 1
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
tenant "multitenancy-Customer2"
 tier
  tier-name tier_tenant2
  max-vpn   12
 !
 tenant-vpn 1
  device-vpn 2
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
tenant "multitenancy-Customer3"
 tier
  tier-name tier_tenant3
  max-vpn   10
 !
 tenant-vpn 1
```

```
  device-vpn 3
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
tenant "multitenancy-Customer4"
 tier
  tier-name tier_tenant4
  max-vpn   10
 !
 tenant-vpn 1
  device-vpn 4
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
```

- The following is a sample output of the **show sdwan tenant-summary** command.

```
Device# show sdwan tenant-summary
tenants-summary max-tenants 30
tenants-summary num-active-tenants 4
                                    GLOBAL
ORG NAME                  ID      UUID
-------------------------------------------------------------------------------
multitenancy-Customer1  16880   774cf81a-1d35-47f3-8c3f-ccb12506e09c
multitenancy-Customer2  23216   62c614be-fc18-4ed0-8f77-ddcd5196a412
multitenancy-Customer3  22400   48ba0449-f177-49c3-926c-a6d5077e34ae
multitenancy-Customer4  14624   61684731-4bda-40b9-9067-c2c9b846f8e8
```

- The following is a sample output of the **show tenant all** command.

```
Device# show tenant all

Tenant          ID         Tier            Tenant VPNs
-------------------------------------------------------------------------------
Tenant1        16880      tier_tenant1           1
Tenant2        23216      tier_tenant2           1
Tenant3        22400      tier_tenant3           1
Tenant4        14624      tier_tenant4           1
```

- The following is a sample output of the **show tenant mapping table** command.

```
Device# show tenant mapping table

Tenant       Tenant VPN        Device VPN         Active
-------------------------------------------------------------------------------
Tenant1          1                1                YES
Tenant2          1                2                YES
Tenant3          1                3                YES
Tenant4          1                4                YES
```

- The following is a sample output of the **show tenant Tenant1** command.

```
Device# show tenant Tenant1

Tenant Tenant1
```

```
  Tenant ID:     30176
  UUID:          5a8b858d-d090-4cc3-8321-a663b08043d3
  Flags:         0x0000
  Resource Limits (Tier "tier_tenant1"):
    Maximum IPv4 Routes           100 (warning-threshold:50)
    Maximum IPv6 Routes           100 (warning-only)
    Maximum NAT Sessions            3

  Mapping Entries:
    Tenant VPN       ->               Device VPN
    1                ->               1               (Active)
```

- The following is a sample output of the **show ip route tenant Tenant1** command.

```
Device# show ip route tenant Tenant1

Tenant name is Tenant1 (id:30176)
    route_limit: 100, warning_limit_percent: 50%
    route_count: 7, rejected_routes: 0

    vrf_name: 1, vrf_id: 4, tenant_vpn_id: 1 route_count: 7, rejected_routes: 0


Routing Table: 1
    Tenant Name: Tenant1, Tenant ID: 30176
    Rejected Routes in tenant: 0, Rejected Routes in this routing table: 0
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.11.0/24 is directly connected, GigabitEthernet4.101
L        172.16.11.2/32 is directly connected, GigabitEthernet4.101
m        172.16.21.0/24 [251/0] via 172.16.255.16, 2w4d, Sdwan-system-intf
m        172.16.31.0/24 [251/0] via 172.16.255.14, 2w4d, Sdwan-system-intf
S     192.168.11.0/24 [1/0] via 172.16.11.1
m     192.168.21.0/24 [251/0] via 172.16.255.16, 2w4d, Sdwan-system-intf
m     192.168.31.0/24 [251/0] via 172.16.255.14, 2w4d, Sdwan-system-intf
```

- The following is a sample output of the **show ipv6 route tenant Tenant1** command.

```
Device# show ipv6 route tenant Tenant1

Tenant name is Tenant1 (id:30176)
    route_limit: 100, warning_only: True
    route_count: 1, rejected_routes: 0

    vrf_name: 1, vrf_id: 4, tenant_vpn_id: 1 route_count: 1, rejected_routes: 0

IPv6 Routing Table - 1 - 1 entries
    Tenant Name: Tenant1, Tenant ID: 30176
```

```
    Rejected Routes in tenant: 0, Rejected Routes in this routing table: 0
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, ls - LISP destinations-summary, a - Application
       m - OMP
L   FF00::/8 [0/0]
     via Null0, receive
```

- The following is a sample output of the **Show run | sec tenant-definition** command.

```
Device# show run | sec tenant-definition

tenant-definition "Tenant1"
 global-tenant-id 45516
 universal-unique-id 696e6fa0-078c-47fb-81b1-40df3b04c8e1
 !
 tier tier_tenant6
  max nat-session 10
  max routes
   !
   address-family ipv4
    unicast-route-limit 15000 warning-threshold 80
   !
   address-family ipv6
    unicast-route-limit 15000 warning-threshold 80
 !
 tenant-vpn-id 1
  device-vpn 1
```

- The following is a sample output of the **show ip nat translations tenant Tenant1 total** command.

```
Device# show ip nat translations tenant Tenant1 total

Total number of translations: 2
```

- The following is a sample output of the **show logging | i TENANT** command.

```
Device# show logging | i TENANT

*Feb  4 21:10:33.625: %IOSXE-4-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00000004456610265827 %NAT-4-PER_TENANT_MAX_ENTRIES: per-tenant maximum limit of 10
reached for 26144.
```

- The following is a sample output IPv4 WARNING-ONLY Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/18 09:16:23.973714834 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:16:23.973: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant1, id:16880) ipv4
unicast route limit warning threshold: alarm_on
```

**Note** ROUTELIMITWARNING_ON: “alarm_on” means the route count has crossed the route limit.

```
Device# show ip route tenant "Tenant2"

2022/11/18 09:33:40.651174649 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:33:40.651: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant1, id:16880) ipv4
unicast route limit warning threshold:
alarm_off
```

**Note** ROUTELIMITWARNING_OFF: “alarm_off” means for the time being, route count is reduced and it has not crossed the warning/route limit.

- The following is a sample output of IPv6 WARNING-ONLY Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/18 09:11:23.589778787 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:11:23.589: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant1, id:16880) ipv6
unicast route limit warning threshold: alarm_on
```

**Note** ROUTELIMITWARNING_ON: "alarm_on" means the route count has crossed the route limit.

```
Device# show ip route tenant "Tenant2 Inc"

2022/11/18 09:33:40.661037261 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:33:40.661: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant1, id:16880) ipv6
unicast route limit warning threshold:
alarm_off
```

**Note** ROUTELIMITWARNING_OFF: “alarm_off” means for the time being, route count is reduced and it has not crossed the warning/route limit.

- The following is a sample output IPv4 Warning Threshold Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 19:07:04.330712142 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
19:07:04.330: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant2, id:23216) ipv4
unicast route limit warning threshold: alarm_on
```

**Note** ROUTELIMITWARNING_ON: “alarm_on” means the route count has crossed the warning threshold

```
Device# show ip route tenant "Tenant2"

2022/11/18 01:36:02.083288966 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
01:36:02.083: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant2, id:23216) ipv4
unicast route limit warning threshold: alarm_off
```

**Note** ROUTELIMITWARNING_OFF: “alarm_off” means means for the time being, route count is reduced and it has not crossed the warning threshold.

- The following is a sample output IPv4 Warning Threshold Route-Limit Exceeded Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/18 10:06:35.698972324 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
10:06:35.698: %RIBTENANT-3-ROUTELIMITEXCEEDED_ON: tenant(name:Tenant2, id:23216) ipv4
unicast route limit exceeded: alarm_on

2022/11/18 10:06:35.699002244 {iosrp_R0-0}{255}: [ribcmn] [16608]: (info): Failed to
add static route 192.168.202.0/24 to table(name:2, id:0x5) due to tenant(name:Tenant2,
 id:23216) route limit exceeded
```

**Note** ROUTELIMITEXCEEDED_ON: “alarm_on” means the route count has exceeded tenant route limit

```
Device# show logging process ios start last boot | i route limit

2022/11/17 20:12:02.090953653 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
20:12:02.090: %RIBTENANT-3-ROUTELIMITEXCEEDED_OFF: tenant(name:Tenant2, id:23216) ipv4
 unicast route limit exceeded: alarm_off
```

**Note** ROUTELIMITEXCEEDED_OFF: “alarm_off” means for the time being, route count is reduced and it has not exceeded the tenant route limit.

- The following is a sample output IPv6 Warning Threshold Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 19:41:31.886639286 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
19:41:31.886: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant2, id:23216) ipv6
unicast route limit warning threshold: alarm_on
```

**Note** ROUTELIMITWARNING_ON: “alarm_on” means the route count has crossed the warning threshold

```
Device# show logging process ios start last boot | i route limit

2022/11/17 19:49:06.553836193 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
19:49:06.553: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant2, id:23216) ipv6
unicast route limit warning threshold: alarm_off
```

**Note** ROUTELIMITWARNING_OFF: “alarm_off” means means for the time being, route count is reduced and it has not crossed the warning threshold.

- The following is a sample output IPv6 Warning Threshold Route-Limit Exceeded Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 05:07:19.326942097 {iosrp_R0-0}{255}: [iosrp] [17094]: (ERR): *Nov 17
05:07:19.326: %RIBTENANT-3-ROUTELIMITEXCEEDED_ON: tenant(name:Tenant2, id:7888) ipv6
unicast route limit exceeded: alarm_on

2022/11/17 05:07:19.327070153 {iosrp_R0-0}{255}: [ribcmn] [17094]: (info): Failed to
add static route 2001:C0A8:29C::/64 to table(name:2, id:0x1E000002) due to
tenant(name:Tenant2, id:7888) route limit exceeded
```

**Note** ROUTELIMITEXCEEDED_ON: “alarm_on” means the route count has exceeded tenant route limit.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 05:15:32.132557582 {iosrp_R0-0}{255}: [iosrp] [17094]: (ERR): *Nov 17
05:15:32.132: %RIBTENANT-3-ROUTELIMITEXCEEDED_OFF: tenant(name:Tenant2, id:7888) ipv6
unicast route limit exceeded: alarm_off
```

**Note** ROUTELIMITEXCEEDED_OFF: “alarm_off” means for the time being, route count is reduced and it has not exceeded the tenant route limit.

### View Tenant-Device Mapping on Cisco SD-WAN Validator

The following is a sample output of the **show support orchestrator tenant-uuid-map** command.

```
vBond# show support orchestrator tenant-uuid-map
-------------------------------------------------------------------------------------
|  Type  |             Chassis-num/uuid             | Tenant id list                 |
-------------------------------------------------------------------------------------
| vSmart | 0c90593a-0f40-4890-a980-5e14907482f7     | 18624,6672,27120               |
```

```
-------------------------------------------------------------------------------------
| vSmart | 8a083d5e-1350-4946-932e-237758bb2280     | 12448,6672,10384               |
-------------------------------------------------------------------------------------
| vSmart | c99c50da-3dff-4951-a598-b3cf71530e99     | 18624,12448,27120,10384        |
-------------------------------------------------------------------------------------
| vEdge  | c8k-24d9f68c-8c01-4e6c-813a-959752f30e73 | 18624,12448,6672,27120,10384   |
-------------------------------------------------------------------------------------
| vEdge  | c8k-fdd9c202-8756-4079-9a56-278e6635412b | 18624,12448,6672               |
```

You can view the tenant global ID on a multitenant WAN edge device using the **show sdwan tenant-summary** command. On a Cisco SD-WAN Controller, you can use the **show tenant-summary** command.

### View Tenant-Cisco SD-WAN Controller Mapping on Cisco SD-WAN Validator

The following is a sample output of the **show tenant-mapping** command.

```
vBond# show tenant-mapping
VSMART
SERIAL

NUM       TENANT NAMES                                                          TENANT COUNT
-------------------------------------------------------------------------------------------
12345990  [ "multitenancy-Customer6" "multitenancy-Customer4" "multitenancy-Customer3"
"multitenancy-Customer1" ]  4
12345992  -
                         0
12345994  [ "multitenancy-Customer6" "multitenancy-Customer5" "multitenancy-Customer3"
"multitenancy-Customer2" ]  4
12345997  -
                         0
12345998  -
                         0
12346001  [ "multitenancy-Customer5" "multitenancy-Customer4" "multitenancy-Customer2"
"multitenancy-Customer1" ]  4
```

### View Tenant-Mapping on Cisco SD-WAN Controller

The following is a sample output of the **show tenant-summary** command.

```
vSmart# show tenant-summary
tenant-summary max-tenants 24
tenant-summary num-active-tenants 4
                                    TENANT  TENANT
TENANT ORG NAME                     ID      VPN ID
-------------------------------------------------
multitenancy-Customer1              1       1003
multitenancy-Customer2              2       1004
multitenancy-Customer3              3       1005
multitenancy-Customer4              4       1006
```

### View Multitenant WAN Edge Device to Cisco SD-WAN Controller Connections

The following is a sample output of the **show sdwan control tenant-connections** command.

```
Device# show sdwan control tenant-connections

PEER LOCAL TENANT
SYSTEM IP COLOR NAME
-----------------------------------------------------------------------------------------------------
172.16.255.19 mpls multitenancy-Customer3
172.16.255.19 mpls multitenancy-Customer2
172.16.255.19 public-internet multitenancy-Customer3
172.16.255.19 public-internet multitenancy-Customer2
```

```
172.16.255.20 mpls multitenancy-Customer4
172.16.255.20 mpls multitenancy-Customer1 Inc
172.16.255.20 mpls multitenancy-Customer2 Inc
172.16.255.20 public-internet multitenancy-Customer4 Inc
172.16.255.20 public-internet multitenancy-Customer1 Inc
172.16.255.20 public-internet multitenancy-Customer2 Inc
172.16.255.24 mpls multitenancy-Customer4 Inc
172.16.255.24 mpls multitenancy-Customer1 Inc
172.16.255.24 mpls multitenancy-Customer3 Inc
172.16.255.24 public-internet multitenancy-Customer4 Inc
172.16.255.24 public-internet multitenancy-Customer1 Inc
172.16.255.24 public-internet multitenancy-Customer3 Inc
```

The PEER SYSTEM IP column shows the IP address of the Cisco SD-WAN Controller the multitenant WAN edge device is connected to. The TENANT NAME entry for a PEER SYSTEM IP shows the name of the tenant organization for which the connection to the Cisco SD-WAN Controller is established.

### View OMP Information on a Multitenant WAN Edge Device

- The following is a sample output of the **show sdwan tenant** *tenant-name* **omp peers** command.

```
Device# show sdwan tenant multitenancy-Customer1 omp peers
R -> routes received
I -> routes installed
S -> routes sent

TENANT DOMAIN OVERLAY SITE REGION
ID PEER TYPE ID ID ID ID STATE UPTIME R/I/S
-----------------------------------------------------------------------------------------------------------
23216 172.16.255.19 vsmart 1 1 101 None up 1:13:42:12 24/24/22
23216 172.16.255.20 vsmart 1 1 102 None up 1:13:42:12 24/0/22
```

  The output shows the Cisco SD-WAN Controllers to which the multitenant WAN edge device is connected for the particular tenant and summarizes the OMP exchanges between the Cisco SD-WAN Controllers and the device.

- The following is a sample output of the **show sdwan tenant** *tenant-name* **omp routes** command.

```
Device# show sdwan tenant multitenancy-Customer1 omp routes

Code:

C   -> chosen

I   -> installed

Red -> redistributed

Rej -> rejected

L   -> looped

R   -> resolved

S   -> stale

Ext -> extranet

Inv -> invalid

Stg -> staged

IA  -> On-demand inactive
```

```
U   -> TLOC unresolved

Reo -> reoriginated

                                                    PATH                    ATTRIBUTE


TENANT    VPN    PREFIX              FROM PEER        ID     LABEL    STATUS    TYPE
     TLOC IP          COLOR            ENCAP  PREFERENCE  REGION ID   REGION PATH

-----------------------------------------------------------------------------------------------

23184     1      172.16.11.0/24      0.0.0.0          66     1003     C,Red,R   installed
  172.16.255.15    mpls              ipsec  -           None        65534


                                    0.0.0.0          69     1003     C,Red,R   installed
  172.16.255.15    public-internet   ipsec  -           None        65534


23184     1      172.16.31.0/24      172.16.255.19    5      1003     C,I,R     installed
  172.16.255.14    mpls              ipsec  -           None        65534


                                    172.16.255.19    6      1003     C,I,R     installed
  172.16.255.14    public-internet   ipsec  -           None        65534


23184     1      192.168.11.0/24     0.0.0.0          66     1003     C,Red,R   installed
  172.16.255.15    mpls              ipsec  -           None        65534


                                    0.0.0.0          69     1003     C,Red,R   installed
  172.16.255.15    public-internet   ipsec  -           None        65534


23184     1      192.168.31.0/24     172.16.255.19    7      1003     C,I,R     installed
  172.16.255.14    mpls              ipsec  -           None        65534


                                    172.16.255.19    8      1003     C,I,R     installed
  172.16.255.14    public-internet   ipsec  -           None        65534
```

- The following is a sample output of the **show sdwan tenant** *tenant-name* **omp services** command.

```
Device# show sdwan tenant multitenancy-Customer1 omp services

C   -> chosen

I   -> installed

Red -> redistributed

Rej -> rejected

L   -> looped

R   -> resolved

S   -> stale
```

```
Ext -> extranet

Stg -> staged

IA  -> On-demand inactive

Inv -> invalid

Reo -> reoriginated


ADDRESS                                                                 PATH    REGION

FAMILY   TENANT    VPN    SERVICE  ORIGINATOR     FROM PEER        ID      ID
LABEL    STATUS    VRF
-------------------------------------------------------------------------------------------

ipv4     23184     1      VPN      172.16.255.15  0.0.0.0          66      NA
1003     C,Red,R   1
                                                  0.0.0.0          69      NA
1003     C,Red,R   1
ipv6     23184     1      VPN      172.16.255.15  0.0.0.0          66      NA
1003     C,Red,R   1
                                                  0.0.0.0          69      NA
1003     C,Red,R   1
```

Related per-Tenant OMP commands:

- **show sdwan tenant** *tenant-name* **omp tlocs**
- **show sdwan tenant** *tenant-name* **omp multicast-routes**
- **show sdwan tenant** *tenant-name* **omp ipv6-routes**

Related global OMP commands:

- **show sdwan omp tloc-paths**
- **show sdwan omp summary**

### View OMP Information on a Cisco SD-WAN Controller

- The following is a sample output of the **show tenant** *tenant-name* **omp peers** command.

```
vSmart# show tenant multitenancy-Customer1 omp peers
R -> routes received

I -> routes installed

S -> routes sent


                        DOMAIN    OVERLAY   SITE

PEER             TYPE   ID        ID        ID        STATE    UPTIME           R/I/S

-------------------------------------------------------------------------------------

172.16.255.14    vedge  1         1         400       up       23:09:40:04      4/0/0

172.16.255.15    vedge  1         1         500       up       0:14:33:55       0/0/0
```

```
172.16.255.24    vsmart  1         1         103       up        44:06:36:31      4/0/4
```

The output shows the other Cisco SD-WAN Controller serving the tenant and the multitenant or tenant-managed WAN edge devices connected to the Cisco SD-WAN Controller.

- The following is a sample output of the **show tenant** *tenant-name* **omp routes** command.

```
vSmart# show tenant multitenancy-Customer1 omp routes


--------------------------------------------------

omp route entries for vpn 1 route 172.16.33.0/24

--------------------------------------------------

            RECEIVED FROM:

peer            172.16.255.14

path-id         66

label           1005

status          C,R

loss-reason     not set

lost-to-peer    not set

lost-to-path-id not set

    Attributes:

     originator       172.16.255.14

     type             installed

     tloc             172.16.255.14, mpls, ipsec

     ultimate-tloc    not set

     domain-id        not set

     overlay-id       1

     site-id          400

     region-id        None

     region-path      65534

     preference       not set

     tag              not set

     origin-proto     connected

     origin-metric    0

     as-path          not set
```

```
     community        not set

     unknown-attr-len not set

.
.
.

------------------------------------------------

omp route entries for vpn 1 route 192.168.33.0/24

------------------------------------------------

            RECEIVED FROM:

peer            172.16.255.14

path-id         66

label           1005
status          C,R

loss-reason     not set

lost-to-peer    not set

lost-to-path-id not set

    Attributes:

     originator       172.16.255.14

     type             installed

     tloc             172.16.255.14, mpls, ipsec

     ultimate-tloc    not set

     domain-id        not set

     overlay-id       1

     site-id          400

     region-id        None

     region-path      65534

     preference       not set

     tag              not set

     origin-proto     static

     origin-metric    0

     as-path          not set

     community        not set

     unknown-attr-len not set
```

The command output shows the routes advertised by multitenant and tenant-managed WAN edge devices for the tenant VPNs.

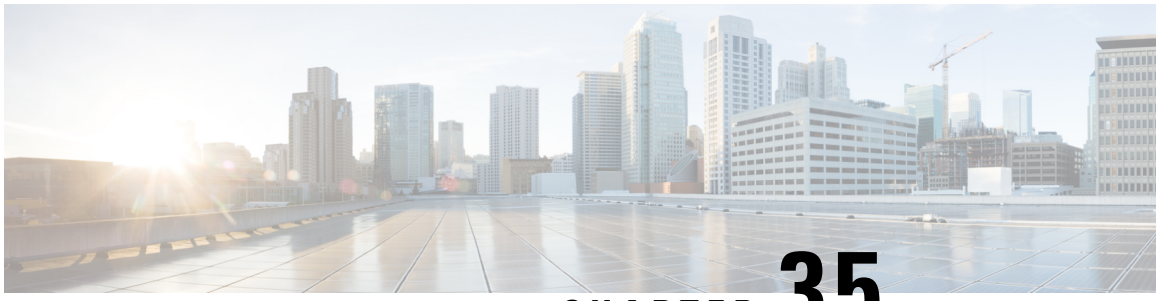
### View Per Tenant Policy Configuration on a Multitenant WAN Edge Device

To view per tenant policy configuration, use the following commands:

- **show sdwan tenant** *tenant-name* **policy from-vsmart**
- **show sdwan tenant** *tenant-name* **policy data-policy-filter**
- **show sdwan tenant** *tenant-name* **policy app-route-policy-filter**
- **show sdwan tenant** *tenant-name* **policy from-vsmart policy data-policy**
- **show sdwan tenant** *tenant-name* **policy from-vsmart policy app-route-policy**

# Troubleshoot Multitenant WAN Edge Device Errors

| Error Scenario | Log File |
|---|---|
| Device Onboarding | Cisco SD-WAN Manager: `/var/log/nms/vmanage-server.log` |
| Device Configuration Pull | Cisco SD-WAN Manager: `/var/log/nms/vmanage-server-deviceconfig-template.log`<br>WAN edge device: `/bootflash/sdwan/cfgloader.log` |



CHAPTER 35

# Cisco Catalyst SD-WAN Multitenancy (Cisco IOS XE Releases 17.4.x and 17.5.x)

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 256: Feature History*

| Feature Name | Release Information | Feature Description |
|---|---|---|
| Cisco Catalyst SD-WAN Multitenancy | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a<br>Cisco vManage Release 20.4.1 | With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. In a multitenant Cisco Catalyst SD-WAN deployment, tenants share Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Validators and Cisco Catalyst SD-WAN Controllers. Tenant data is logically isolated on these shared resources. |


- Overview of Cisco Catalyst SD-WAN Multitenancy, on page 1020
- User Roles in Multitenant Environment, on page 1022
- Hardware Supported and Specifications, on page 1024
- Initial Setup for Multitenancy, on page 1025
- Manage Tenants, on page 1028
- Cisco SD-WAN Manager Dashboard for Multitenancy, on page 1032
- Manage Tenant WAN Edge Devices, on page 1036
- Tenant-Specific Policies on Cisco Catalyst SD-WAN Controllers, on page 1037
- Manage Tenant Data, on page 1037
- View OMP Statistics per Tenant on a Cisco SD-WAN Controller, on page 1041

- View Tenants Associated with a Cisco SD-WAN Controller, on page 1042
- Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment, on page 1042

# Overview of Cisco Catalyst SD-WAN Multitenancy

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. The tenants share Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Validators, and Cisco Catalyst SD-WAN Controllers. The domain name of the service provider has subdomains for each tenant. For example, the `multitenancy.com` service provider can manage the tenants Customer1 (`Customer1.multitenancy.com`) and Customer2 (`Customer2.multitenancy.com`).

Following are the key features of Cisco Catalyst SD-WAN multitenancy:

- Full enterprise multitenancy: Cisco Catalyst SD-WAN supports multitenancy and offers enterprises the flexibility of segregated roles such as service provider and tenants. Service providers can use multitenancy to provide Cisco Catalyst SD-WAN service offerings to their customers.
- Multi-tenant Cisco SD-WAN Manager:
  - Cisco SD-WAN Manager is deployed and configured by the service provider. The provider enables multitenancy and creates a Cisco SD-WAN Manager cluster to serve tenants. Only the provider can access a Cisco SD-WAN Manager instance through the SSH terminal.

**Note** To connect to a device through SSH, use the IP address of the `vmanage_system` interface; this IP address is assigned by Cisco SD-WAN Manager. Do not use a user-configured system IP address to connect to a device through SSH.

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

  - Cisco SD-WAN Manager offers service providers an overall view of the SD-WAN multi-tenant deployment and allows a provider to manage the shared Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller devices. Cisco SD-WAN Manager also allows service providers to monitor and manage the deployments of each tenant.
  - Cisco SD-WAN Manager allows tenants to monitor and manage their deployment. Through Cisco SD-WAN Manager, tenants can deploy and configure WAN edge devices. Tenants can also configure custom policies on assigned Cisco Catalyst SD-WAN Controllers.
- Multi-tenant Cisco Catalyst SD-WAN Validators:
  - Cisco Catalyst SD-WAN Validators are deployed and configured by the service provider. Only the provider can access a Cisco Catalyst SD-WAN Validator through the SSH terminal.

**Note** To connect to a device through SSH, use the IP address of the `vmanage_system` interface; this IP address is assigned by Cisco SD-WAN Manager. Do not use a user-configured system IP address to connect to a device through SSH.

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

- Cisco Catalyst SD-WAN Validators serve WAN edge devices of multiple tenants as the devices are added to the overlay network.

- Multi-tenant Cisco Catalyst SD-WAN Controllers:
  - Cisco Catalyst SD-WAN Controllers are deployed by the service provider. Only the provider can create and attach device and feature templates to Cisco Catalyst SD-WAN Controllers, and can access a Cisco Catalyst SD-WAN Controller through the SSH terminal.

**Note** To connect to a device through SSH, use the IP address of the `vmanage_system` interface; this IP address is assigned by Cisco SD-WAN Manager. Do not use a user-configured system IP address to connect to a device through SSH.

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

  - When a tenant is created, Cisco SD-WAN Manager assigns two Cisco Catalyst SD-WAN Controllers for the tenant. The Cisco Catalyst SD-WAN Controllers form an active-active cluster.

    Each tenant is assigned only two Cisco Catalyst SD-WAN Controllers. Before a tenant is created, two Cisco Catalyst SD-WAN Controllers must be available to serve the tenant.
  - Each pair of Cisco Catalyst SD-WAN Controllers can serve a maximum of 24 tenants.
  - Tenants can configure custom policies on the Cisco Catalyst SD-WAN Controllers assigned to them. Cisco SD-WAN Manager notifies the Cisco Catalyst SD-WAN Controllers to pull the policy templates. Cisco Catalyst SD-WAN Controllers pull the templates and deploy the policy configuration for the specific tenant.
  - Only the provider can view events, audit logs, and OMP alarms for a Cisco Catalyst SD-WAN Controller on Cisco SD-WAN Manager.

- WAN Edge Devices:
  - A tenant or the provider acting on behalf of a tenant can add WAN edge devices to the tenant network, configure the devices, and remove the devices from the tenant network, or access the device through the SSH terminal.

**Note** To connect to a device through SSH, use the IP address of the `vmanage_system` interface; this IP address is assigned by Cisco SD-WAN Manager. Do not use a user-configured system IP address to connect to a device through SSH.

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

- A provider can manage the WAN edge devices only from provider-as-tenant view. In the provider view, Cisco SD-WAN Manager does not present any WAN edge device information.
- Cisco SD-WAN Manager reports WAN edge device events, logs, and alarms only in the Tenant Role and the provider-as-tenant views.

- Overlapping VPN numbers: A particular VPN or a set of common VPNs is assigned to a specific tenant, with their own configurations and monitoring dashboard environment. These VPN numbers can overlap where they are used by other tenants.
- On-prem and cloud deployment models: Cisco Catalyst SD-WAN controllers can be deployed in an organization data center on servers running the VMware vSphere ESXi or the Kernel-based Virtual Machine (KVM) hypervisor. Cisco Catalyst SD-WAN controllers can also be deployed in the cloud on Amazon Web Services (AWS) servers.

# User Roles in Multitenant Environment

A multi-tenant environment includes the service provider and tenant roles. Each role has distinct privileges, views, and functions.

### Provider Role

The provider role entitles system-wide administrative privileges. A user with the provider role has the default username **admin**. The provider user can access Cisco SD-WAN Manager using the domain name of the service provider or by using the Cisco SD-WAN Manager IP address. When using a domain name, the domain name has the format `https://multitenancy.com`.

The **admin** user is part of the user group **netadmin**. Users in this group are permitted to perform all operations on the controllers and the Cisco Catalyst SD-WAN devices of the tenants. You can add additional users to the **netadmin** group.

You cannot modify the privileges of the **netadmin** group. On Cisco SD-WAN Manager, you can view the privileges of the user group from the **Administration** > **Manage Users** > **User Groups** page.

**Note** When you create a new provider user in Cisco SD-WAN Manager, including a **netadmin** user, by default, the user is not allowed SSH access to the Cisco SD-WAN Manager VM. To enable SSH access, configure SSH authentication using a AAA template and push the template to Cisco SD-WAN Manager. For more information on enabling SSH authentication, see SSH Authentication using Cisco SD-WAN Manager on Cisco IOS XE Catalyst SD-WAN Devices.

For more information about configuring users and user groups, see Configure User Access and Authentication.

Cisco SD-WAN Manager offers two views to a provider:

- **Provider View**

  When a provider user logs in to multi-tenant Cisco SD-WAN Manager as **admin** or another **netadmin** user, Cisco SD-WAN Manager presents the provider view and displays the provider dashboard.

  You can perform the following functions from the provider view:

  - Provision and manage Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Validators and Cisco Catalyst SD-WAN Controllers.
  - Add, modify, or delete tenants.
  - Monitor the overlay network.

- **Provider-as-Tenant View**

  When a provider user selects a specific tenant from the **Select Tenant** drop-down list at the top of the provider dashboard, Cisco SD-WAN Manager presents the provider-as-tenant view and displays the tenant dashboard for the selected tenant. The provider user has the same view of Cisco SD-WAN Manager as a tenant user would when logged in as **tenantadmin**. From this view, the provider can manage the tenant deployment on behalf of the tenant.

  In the provider dashboard, a table of tenants presents a status summary for each tenant. A provider user can also launch the provider-as-tenant view by clicking on a tenant name in this table.

### Tenant Role

The tenant role entitles tenant administrative privileges. A user with the tenant role has the default username **tenantadmin**. The default password is **Cisco#123@Viptela**. We recommend that you change the default password on first login. For information on changing the default password, see Hardware and Software Installation.

The **tenantadmin** user is part of the user group **tenantadmin**. Users in this group are permitted to perform all operations on the WAN edge devices of the tenants. You can add additional users to the **tenantadmin** group.

You cannot modify the privileges of the **tenantadmin** group. On Cisco SD-WAN Manager, you can view the privileges of the user group from the **Administration** > **Manage Users** > **User Groups** page.

For more information about configuring users and user groups, see Configure User Access and Authentication.

A tenant user can log in to Cisco SD-WAN Manager using a dedicated URL and the default username **tenantadmin**. For example, the dedicated URL of a tenant could be `https://Customer1.multitenancy.com` for a provider using the domain name

`https://multitenancy.com`. When the user logs in, Cisco SD-WAN Manager presents the tenant view and displays the tenant dashboard.

A tenant user with administrative privileges can perform the following functions:

- Provision and manage tenant routers
- Monitor overlay network of the tenant
- Create custom policies on the assigned Cisco Catalyst SD-WAN Controllers
- Upgrade the software on the tenant routers.

# Hardware Supported and Specifications

The following platforms support multitenancy.

***Table 257: Router Models***

| Platform | Router Models |
|---|---|
| Cisco IOS XE Catalyst SD-WAN device | • Cisco ASR 1000 Series Aggregation Services Routers<br>• Cisco ISR 1000 Series Integrated Services Routers<br>• Cisco ISR 4000 Series Integrated Services Routers<br>• Cisco Catalyst 8300 Series Edge Platforms<br>• Cisco Catalyst 8500 Series Edge Platforms<br>• Cisco Catalyst 8000V Edge Software |

The following hypervisors and deployment model are supported for multitenancy.

***Table 258: Deployment Model***

| Specification | Description |
|---|---|
| Supported hypervisors | VMware, KVM, AWS (cloud-hosted by Cisco) |
| Cisco SD-WAN Manager Deployment Model | Cluster, 3 Cisco SD-WAN Manager instances with each instance running all Cisco SD-WAN Manager services. |

The supported hardware specifications for the Cisco Catalyst SD-WAN Validator, Cisco SD-WAN Manager, and the Cisco Catalyst SD-WAN Controllerare as follows:

*Table 259: On-prem Deployment*

| **Server** | Cisco SD-WAN Manager | Cisco Catalyst SD-WAN Validator | Cisco Catalyst SD-WAN Controller |
|---|---|---|---|
| **Deployment Model** | Cluster | N/A | Non-containerized |
| **Number of Instances** | 3 | 2 | 2 per 24 tenants |
| **CPU**<br>**DRAM**<br>**Hard Disk** | 32 vCPU<br>72 GB<br>1 TB | 4 vCPU<br>4 GB<br>10 GB | 8 vCPU<br>16 GB<br>16 GB |
| **NMS Service Distribution** | Some services run on all three Cisco SD-WAN Manager instances in the cluster, while some services run on only one of the three instances in the cluster. Therefore, the CPU load may vary among the instances. | N/A | N/A |

**Note** If DPI is enabled, we recommend that the aggregated DPI data across all Cisco SD-WAN Managere instances not exceed 350 GB per day.

# Initial Setup for Multitenancy

### Prerequisites

- Download and install software versions as recommended in the following table:

*Table 260: Software Prerequisites for Cisco Catalyst SD-WAN Multitenancy*

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.4.1 |
| Cisco Catalyst SD-WAN Validator | Cisco SD-WAN Release 20.4.1 |
| Cisco Catalyst SD-WAN Controller | Cisco SD-WAN Release 20.4.1 |
| Cisco IOS XE Catalyst SD-WAN device | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a |

A configuration in which one or more controllers, or WAN edge devices, are running software versions earlier than those mentioned in the table above is not supported.

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

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

- Log in to Cisco SD-WAN Manager as the provider **admin** user.

1. Create three Cisco SD-WAN Manager instances and associated configuration templates. See Deploy Cisco SD-WAN Manager.
   a. While configuring Cisco SD-WAN Manager instances, configure the service provider organization name (`sp-organization-name`) and the organization name (`organization-name`).

      **Example:**

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

2. Configure one of the Cisco SD-WAN Manager instances to support multitenancy. See Enable Multitenancy on Cisco SD-WAN Manager, on page 1027
3. Create a Cisco SD-WAN Manager cluster consisting of three Cisco SD-WAN Manager instances. See Cluster Management.
   - The Cisco SD-WAN Manager cluster must have three Cisco SD-WAN Manager instances. A cluster with more than three instances or fewer than three instances is not a supported configuration for Cisco Catalyst SD-WAN multitenancy.
   - While creating the Cisco SD-WAN Manager cluster, add the Cisco SD-WAN Manager instance configured to support multitenancy before adding the other two Cisco SD-WAN Manager instances.
4. Certify all instances of Cisco SD-WAN Manager. See Generate Cisco SD-WAN Manager Certificate.
5. Create and configure Cisco SD-WAN Validatorinstances. See Deploy Cisco SD-WAN Validator.

   While configuring Cisco SD-WAN Validator instances, configure the service provider organization name (`sp-organization-name`) and the organization name (`organization-name`). See Configure Organization Name in Cisco SD-WAN Validator.

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

6. Create Cisco SD-WAN Controller instances. See Deploy the Cisco SD-WAN Controllers.

   To support 50 tenants and 1000 devices across all tenants, deploy 6 Cisco SD-WAN Controller instances. To support 100 tenants and 5000 devices across all tenants, deploy 12 Cisco SD-WAN Controllers.

   a. Add Cisco SD-WAN Controller to the overlay network.

7. Onboard new tenants. See Add a New Tenant.

# Enable Multitenancy on Cisco SD-WAN Manager

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** > **Tenancy Mode**.If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.
3. In the **Tenancy** field, click **Multitenant**.
4. In the **Domain** field, enter the domain name of the service provider (for example, multitenancy.com).
5. Enter a **Cluster Id** (for example, cluster-1 or 123456).
6. Click **Save**. If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, 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.

# Add 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 **Configuration** > **Devices**.
3. Click **Controllers**.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

4. Click **Add Controller**.
5. In the **Add Controller** dialog box, do the following:
   a. In the **Controller 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 **Validator 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 **Manager** 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 **Manager**. The new Cisco SD-WAN Controller is ready to be used in your mutitenant deployment.

# Manage Tenants

## Add a New Tenant

### Prerequisites

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

A Cisco SD-WAN Controller enters the `Manager` 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. 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 `Manager`.
- 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 261: 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. |
| **Organization Name** | Enter the tenant organization name in the format `<SP Org Name>-<Tenant Org Name>`.<br>**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 `multitenancy.com` service provider, a valid domain name can be `Customer1.multitenancy.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 the Cisco SD-WAN Manager **Administration** > **Settings** > **Tenancy Mode** GUI navigation path.

- 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.

  When creating fully qualified domain names (FQDN) the following DNS entries are required:

  - **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.** 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 Validators.

**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, modify the tenant name, description, or domain name.
   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, on page 1037.

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**.

# Cisco SD-WAN Manager Dashboard for Multitenancy

After enabling Cisco SD-WAN Manager for multitenancy, you can view the multitenant dashboard when you log in to Cisco SD-WAN Manager. Cisco SD-WAN Manager multitenant dashboard is a portal where the provider or tenant can view and provision the underlying system.

The bar at the top of every Cisco SD-WAN Manager multitenant screen includes icons that allow smooth navigation.

## View Tenant Activity, Device, and Network Information

When you log in to a multitenant Cisco SD-WAN Manager as an administrator, the provider dashboard displays the following components. To return to the provider dashboard from other Cisco SD-WAN Manager screens, click **Dashboard** at the left bar.

- Device pane — runs across the top of the multitenant dashboard screen. The device pane displays the number of active Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and Cisco SD-WAN Manager instances, the connectivity status of devices, and information on certificates that have expired or about to expire.
- Tenants pane — displays the total number of tenants and a summary of the control status, site health, router health, and Cisco Catalyst SD-WAN Controller status of all tenants.
- Table of tenants in the overlay network — List of individual tenants, with separate information about the control status, site health, WAN edge device health, and Cisco Catalyst SD-WAN Controller status for each tenant.

  To display tenant-specific status summary information,

  1. Click a tenant name from the tenant list.

     A dialog box opens on the right side of the screen that provides additional information about the status of the tenant.

  2. To access the tenant dashboard for the selected tenant, click **<Tenant name> Dashboard**.

     Cisco SD-WAN Manager presents the provider-as-tenant view and displays the tenant dashboard. To return to the provider view, click **Provider** at the top of page.

  3. To close the dialog box, click the tenant name from the tenant list.

## View Detailed Information of a Tenant Setup

Cisco SD-WAN Manager displays the tenant dashboard, which provides information about a tenant deployment when

- a provider **admin** user selects a specific tenant from the **Select Tenant** drop-down list in the provider dashboard. This view is called the provider-as-tenant view.

- a **tenantadmin** user logs in to Cisco SD-WAN Manager. This view is called the tenant view.

### View All Network Connections in the Tenant Overlay Network

The **Device** pane runs across the top of the tenant dashboard and displays the number of control connections from Cisco SD-WAN Manager to the Cisco SD-WAN Controllers and routers in the overlay network of a tenant. For each WAN edge device, the Device pane shows

- Total number of control connections between Cisco SD-WAN Controllers and WAN edge devices
- Number of valid control connections between Cisco SD-WAN Controllers and WAN edge devices
- Number of invalid control connections between Cisco SD-WAN Controllers and WAN edge devices

Click a connection number, or the **Up** or **Down** arrow, to display a table with detailed information about each connection. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen, or access the **Tools** > **SSH Terminal** Screen.

**Note** In Cisco vManage Release 20.6.x and earlier releases, **Real Time** view is part of the **Monitor** > **Network** screen.

### View Information About Device Reboots

The **Reboot** pane displays the total number of reboots in the last 24 hours for all devices in the network. It includes soft and cold reboots and reboots that occurred as a result of power-cycling a device. For each reboot, the following information is listed:

- System IP and hostname of the device that rebooted.
- Time when the device was rebooted.
- Reason for the device reboot

If the same device reboots more than once, each reboot option is reported separately.

Click the **Reboot** pane to open the **Reboot** dialog box. In the **Reboot** dialog box, click **Crashes**. For all device crashes, the following information is listed:

- System IP and hostname of the device on which the crash occurred.
- Crash index of the device
- Core time when the device crashed.
- File name of the device crash log

### View Network Connections

The **Control Status** pane displays whether Cisco SD-WAN Controller and WAN edge devices are connected. Each Cisco SD-WAN Controller must connect to all other Cisco SD-WAN Controllers in the network. Each WAN edge device must connect to the maximum number of configured Cisco SD-WAN Controllers. The **Control Status** pane displays three network connection counts:

- Control Up — total number of devices with the required number of operational control plane connections to a Cisco SD-WAN Controller
- Partial — total number of devices with some, but not all, operational control plane connection to Cisco SD-WAN Controllers.
- Control Down — total number of devices with no control plane connection to a Cisco SD-WAN Controller

To display a table with device details, click a row from the **Control Status** dialog box. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen.

**Note** In Cisco vManage Release 20.6.x and earlier releases, **Real Time** view is part of the **Monitor** > **Network** screen.

### View State of Data Connections for a Site

The **Site Health** pane displays the state of data connections for a site. When a site has multiple WAN edge devices, this pane displays the state for the entire site and not for individual devices. The Site Health pane displays three connectivity states:

- Full WAN Connectivity — total number of sites where all BFD sessions on all routers are in the up state.
- Partial WAN Connectivity — total number of sites where tunnel and all BFD sessions on all routers are in the down state. These sites still have limited data plane connectivity.
- No WAN Connectivity — total number of sites where all BFD sessions on all routers are in the down state. These sites have no data plane connectivity.

To display a table with detailed information about each site, node, or tunnel, click a row from the **Site Health** dialog box. Click the **More Actions** icon at the right of each row in the table to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen, or access the **Tools** > **SSH Terminal** screen.

**Note** In Cisco vManage Release 20.6.x and earlier releases, **Real Time** view is part of the **Monitor** > **Network** screen.

### View Interface Usage for WAN Edge Interfaces

The **Transport Interface Distribution** pane displays interface usage in the last 24 hours for all WAN edge interfaces in VPN 0. It includes all TLOC interfaces. Click the pane to view details of interface usage in the **Transport Interface Distribution** dialog box.

### View WAN Edge Device Counts

The **WAN Edge Inventory** pane provides four WAN edge device counts:

- Total — total number of authorized serial numbers for WAN edge devices that have been uploaded on Cisco SD-WAN Manager. The serial number is uploaded on the **Configuration** > **Devices** screen.

- Authorized — total number of authorized WAN edge devices in the overlay network These WAN edge devices are marked as **Valid** in the **Configuration** > **Certificates** > **WAN Edge List** screen.
- Deployed — total number of deployed WAN edge devices. These are WAN edge devices that are marked as Valid and are now operational in the network.
- Staging — total number of WAN edge devices you configure at a staging site before they are made a part of the overlay network. These routers do not take part in any routing decisions and do not affect network monitoring through Cisco SD-WAN Manager.

  Click the pane to view hostname, system IP, site ID, and other details of each router from the **WAN Edge Inventory** dialog box.

### View Aggregated State of WAN Edge Devices

The **WAN Edge Health** pane offers an aggregated view of the state of WAN edge devices by providing a count of the number of devices in each state, therefore describing the health of the hardware nodes. The three WAN edge device states are:

- Normal — number of WAN edge devices with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as, normal.
- Warning — number of WAN edge devices with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as, warning
- Error — number of WAN edge devices with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as, error.

  Click a number or the WAN edge device state to display a table with the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the **More Actions** icon at the right of each row in the table to access the following:

  - **Hardware Environment**
  - **Real Time** view from the **Monitor** > **Devices** screen

    Cisco vManage Release 20.6.x and earlier: **Real Time** view from the **Monitor** > **Network** screen
  - **Tools** > **SSH Terminal** screen.

### View WAN Edge Device Loss, Latency, Jitter

The **Transport Health** pane displays the aggregated average loss, latency, and jitters for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

From the **Type** drop-down arrow, choose loss, latency, or jitter.

Click the icon to select a time period for which to display the transport health.

Click the icon to open the **Transport Health** dialog box. This dialog box displays a more detailed view. To display information in a tabular format, click **Details**. You can choose to change the displayed health type and time period.

### View DPI Flow Information of WAN Edge Devices

The **Top Applications pane** displays DPI flow information for traffic transiting routers in the overlay network.

**Note** DPI flow information is shown only for the last 24 hours. To view DPI flow information for a time before the last 24 hours, you must check the information for the specific device.

Click the icon to select a time period for which to display data. From the **VPN** drop-down list, select a VPN to display DPI information for all flows in that VPN.

Click the icon to open the **Top Applications** dialog box. This dialog box displays a more detailed view of the same information. You can change the VPN and time period.

### View Tunnels Data

The **Application-Aware Routing** pane allows you to choose the following tunnel criteria from the **Type** drop-down arrow:

- Loss
- Latency
- Jitter

Based on the tunnel criteria, the pane displays the 10 worst tunnels. For example, if you choose loss, the pane shows 10 tunnels with the greatest average loss over the last 24 hours.

Click the icon against a row to display a graphical representation of the data. Select a time period for which to display data or click **Custom** to display a drop-down arrow for specifying a custom time period.

Click the icon to open the **Application-Aware Routing** dialog box. This dialog box displays the 25 worst tunnels based on criteria you choose from the **Type** drop-down arrow, the criteria being loss, latency, and jitter.

# Manage Tenant WAN Edge Devices

## Add a WAN Edge Device to 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. 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.

# Tenant-Specific Policies on Cisco Catalyst SD-WAN Controllers

A provider **admin** user (from the Cisco SD-WAN Manager provider-as-tenant view) or a **tenantadmin** user (from the Cisco SD-WAN Manager tenant view) can create and deploy tenant-specific policies on the Cisco Catalyst SD-WAN Controllers serving the tenant. The user can configure a CLI policy or create the policy using the UI policy configuration wizard.

When you activate or deactivate a policy,

1. Cisco SD-WAN Manager identifies the Cisco Catalyst SD-WAN Controllers serving the tenant.
2. Cisco SD-WAN Manager notifies the Cisco Catalyst SD-WAN Controllers to pull the policy configuration.
3. Cisco Catalyst SD-WAN Controllers pull and deploy the policy configuration.
4. Cisco SD-WAN Manager reports the status of the policy pull by the Cisco Catalyst SD-WAN Controllers.

# Manage Tenant Data

## Back Up Tenant Data

The tenant data backup solution of Cisco SD-WAN Manager multitenancy provides the following functionalities:

- Create, Extract, and List Configuration Data Backup File.

- Back up configuration database of a specific tenant with an option to restore it later. See Restore and Delete Tenant Data Backup File.
- Delete back up files of a tenant stored in Cisco SD-WAN Manager. For deleting tenant data backup files, see Restore and Delete Tenant Data Backup File.

The following factors are applicable when using data backup solution:

- The tenant data backup solution operations can be performed by a tenant administrator over tenant view and as a provider. To know how to access tenant dashboard through different views, see User Roles in Multitenant Environment, on page 1022.
- A tenant is allowed to perform the following backup operations at a particular time and must complete an operation before starting a new operation:
  - Back up a single configuration database
  - Download the backup file.
  - Restore or import backup files
  - Delete backup files.
  - List backup files
- A tenant backup file format is as follows:

  `Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz`
- The tenant data backup operation is a readonly operation on the configuration database. However, to ensure data consistency and prevent data loss, do not perform any major changes on the network.
- When a backup or restore operation for a specific tenant is in-progress, other tenants are allowed to perform the backup and restore operations smoothly.
- A tenant is not allowed to perform other backup operations when the restore operation of the tenant database is in-progress. So, a tenant can perform a single backup operation and when this operation is in-progress, all new backup operation requests are rejected.

  The remaining tenants can continue with their backup operations.
- A tenant must use the same Cisco SD-WAN Manager version for backup generation and restore operation.
- A tenant can store a maximum of three backup files in Cisco SD-WAN Manager and can download to store them outside Cisco SD-WAN Manager repository. If the tenant already has three backup files, a subsequent backup operation results in the earliest backup file being deleted and a new backup file being generated.
- Ensure that the following parameter values match in both the backup file and the setup where tenant has requested for a restore operation:
  - Tenant Id
  - Organization Name
  - SP Organization Name
- The tenant data backup solution creates a task in the tenant view of Cisco SD-WAN Manager. Therefore, the tenant can monitor the progress of the operation from the task view of the tenant dashboard.

- A provider cannot back up provider data using this solution. Therefore, the provider can back up all tenants information at once by backing up all tenants configuration database using CLI.

# Create, Extract, and List Configuration Data Backup File

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. In the address bar, modify the URL path with `dataservice` for the REST API connection.

   **Example:** `https://<tenant_URL>/dataservice`

3. Create a configuration backup file by using the following API:
   `https://<tenant_URL>/dataservice/tenantbackup/export`.

4. If the configuration backup file has been created successfully, Cisco SD-WAN Manager task view indicates that the backup file has been generated. You can view the process identifier of the created process or task.

   **Example:**

   ```
   {
      "processId": "72d69805-b987-436f-9b7a-afef2f3f9061",
   "status": "in-progress"
   }
   ```

5. Verify the task status using the obtained process identifier.

   **Example:**
   `https://<tenant_URL>/dataservice/device/action/status/72d69805-b987-436f-9b7a-afef2f3f9061`

   The verification generates the details of the task in the JSON file format.

6. After the task is completed, extract or download the backed-up file available under the **data** section of the JSON task file.

   **Example:** To extract or download the backup file, use the following API:
   `https://<tenannt_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz`

7. List backup files stored in Cisco SD-WAN Manager using the following API.

   **Example:** `https://<tenant_URL>//dataservice/tenantbackup/list`

# Restore and Delete Tenant Data Backup File

**Before you begin:**

To run the restore and delete tenant data backup files API, you can download and install Postman tool or any other alternative tool for testing http applications and services. In this document, the procedure to restore and delete tenant data backup files has been explained using the Postman tool. Postman is a software tool used as an API development environment. You can download the tool from the Postman website.

1. Open Google Chrome, or another browser, and enable developer mode on it.
2. 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**.

3. To get header information of the restore API, do as follows:
   a. On the right side of the screen, click the **Network** tab to get the network capture view.
   b. In the network capture view, click the **Name** column to sort the listed items.
   c. Search and click **index.html**.
   d. Click the **Headers** tab and expand **Request Headers**.
   e. Choose all text under **Request Headers** and copy it to the clipboard.
4. Import backup files through the Postman UI:
   a. Open the Postman UI.
   b. To disable SSL certificate verification, click **Postman** > **Preferences** > **General** > **Request**. Turn off **SSL Certificate Verification**.
   c. In the Postman UI, create a new tab.
   d. Click **Headers** and then click **Bulk Edit**.
   e. Paste the text that was copied in step 3 from the **Request Headers** block into an editable form.
   f. From the **GET** method drop-down list, choose **POST**.
   g. In the **Paste request URL** field, paste the dedicated URL of the tenant and include `dataservice/tenantbackup/import`.

      **Example:** `https://Customer1.multitenancy.com/dataservice/tenantbackup/import`
   h. Click the **Body** tab and select **form-data**.
   i. Under **KEY** column, enter *bakup.tar.gz*
   j. Under **VALUE** column, click **Select Files** and select a backup file to be imported.
   k. To run the API, click **Send**.

      In the **Response** section of the Postman UI, you can view the JSON information that indicates the file that was restored.
5. Monitor the restoration of backup files in either of the following ways:
   a. Use Cisco SD-WAN Manager task view that indicates if backup file has been imported successfully. You can view the process identifier of the created process or task.

      **Example:**

      ```
      {"processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
          "status": "Import Successfully Submitted for tenant 1579026919487"
      }
      ```
   b. Use the following URL to get the status,
      `https://<tenant_URL>/dataservice/device/action/status/<processId>`

**Example:**

```
https://Customer1.multitenancy.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d
```

6. Delete tenant data backup file through Postman UI.
   a. In the Postman UI, create a new tab.
   b. Click **Headers** and then click **Bulk Edit**.
   c. Paste the text that was copied in step 3 from the **Request Headers** block into an editable form.
   d. From the **GET** method drop-down list, choose **DELETE**.
   e. In the **Paste request URL** field, paste the dedicated URL of the tenant and include `dataservice/tenantbackup/delete?fileName='filename'`. The filename can either be name of the backup file or all.

      **Example:**

      ```
      https://Customer1.multitenancy.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz
      ```

      **Example:**

      ```
      https://Customer1.multitenancy.com/dataservice/tenantbackup/delete?fileName=all
      ```

   f. To run the API, click **Send**.

   In the **Response** section of the Postman UI, you can view the JSON information that indicates the files that were deleted.

   **Example:**

```
{
    "Deleted": [
        "bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz"
    ]
}
```

# 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 **Controller** 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.

# Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment

*Table 262: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>Cisco vManage Release 20.5.1 | This feature enables you to migrate a single-tenant Cisco Catalyst SD-WAN overlay to a multitenant deployment using a sequence of Cisco SD-WAN Manager API calls. |

### Before You Begin

- Before you begin the migration,
  - Ensure that the edge devices in the single-tenant deployment can reach the Cisco SD-WAN Validator in the multitenant deployment
  - Ensure that the template, routing, and policy configuration on the edge devices is synchronized with the current configuration on Cisco SD-WAN Manager
  - Ensure that the Certificate Authority (CA) on both single-tenant and multitenant Cisco SD-WAN Managers are same.
  - Configure a maintenance window for the single-tenant overlay before performing this procedure. See Configure or Cancel Cisco SD-WAN Manager Server Maintenance Window.
- Minimum software requirements for the single-tenant overlay to be migrated:

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.5.1 |
| Cisco SD-WAN Validator | Cisco SD-WAN Release 20.5.1 |

| Device | Software Version |
|---|---|
| Cisco SD-WAN Controller | Cisco SD-WAN Release 20.5.1 |
| Cisco IOS XE Catalyst SD-WAN device | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a |

- Minimum software requirements for the multitenant deployment to which the single-tenant overlay must be migrated:

| Device | Software Version |
|---|---|
| Cisco SD-WAN Manager | Cisco vManage Release 20.5.1 |
| Cisco SD-WAN Validator | Cisco SD-WAN Release 20.5.1 |
| Cisco SD-WAN Controller | Cisco SD-WAN Release 20.5.1 |
| Cisco IOS XE Catalyst SD-WAN device | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a |

- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.

### Migration Procedure

1. Export the single-tenant deployment and configuration data from a Cisco SD-WAN Manager instance controlling the overlay.

| | |
|---|---|
| Method | `POST` |
| URL | `https://`*`ST-vManage-IP-address`* |
| Endpoint | `/dataservice/tenantmigration/export` |
| Authorization | Admin user credentials. |

| | |
|---|---|
| Body | Required<br>Format: Raw JSON<br>`{ "desc": <tenant_description>, "name": <tenant_name>, "subdomain": <tenant_name>.<domain>, "orgName": <tenant_orgname > }`<br>Field Description:<br>• `desc`: A description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters.<br>• `name`: Unique name for the tenant in the multitenant deployment.<br>• `subdomain`: Fully qualified sub-domain name of the tenant. The sub-domain name must include the domain name of the service provider. For example, if `multitenancy.com` is the domain name of service provider, and the tenant name is `Customer1`, the tenant sub-domain name would be `Customer1.multitenancy.com`.<br>• `orgName`: Name of the tenant organization. The organization name is case-sensitive. |
| Response | Format: JSON<br>`{ "processId": <vManage_process_ID>, }` |

While exporting the data, Cisco SD-WAN Manager attempts to detach any CLI templates from the edge devices in preparation for the migration to the multitenant deployment. If prompted by Cisco SD-WAN Manager, detach CLI templates from the edge devices and execute the export API call again.

2. Check the status of the data export task in Cisco SD-WAN Manager. When the task succeeds, download the data using the URL
`https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz`

3. On a multitenant Cisco SD-WAN Manager instance, import the data exported from the single-tenant overlay.

| | |
|---|---|
| Method | `POST` |
| URL | `https://MT-vManage-IP-address` |
| Endpoint | `/dataservice/tenantmigration/import` |
| Authorization | Provider Admin user credentials. |
| Body | Required<br>Format: form-data<br>Key Type: File<br>Value: `default.tar.gz` |

| | |
|---|---|
| Response | Format: JSON<br>{<br>"processId": <vManage_process_ID>,<br>"migrationTokenURL": <token_URL>,<br>} |

When the task succeeds, on the multitenant Cisco SD-WAN Manager, you can view the devices, templates, and policies imported from the single-tenant overlay.

4. Obtain the migration token using the token URL obtained in response to the API call in **Step 3**.

| | |
|---|---|
| Method | GET |
| URL | https://*MT-vManage-IP-address* |
| Endpoint | migrationTokenURL obtained in **Step 3**. |
| Authorization | Provider Admin user credentials. |
| Response | The migration token as a large blob of encoded text. |

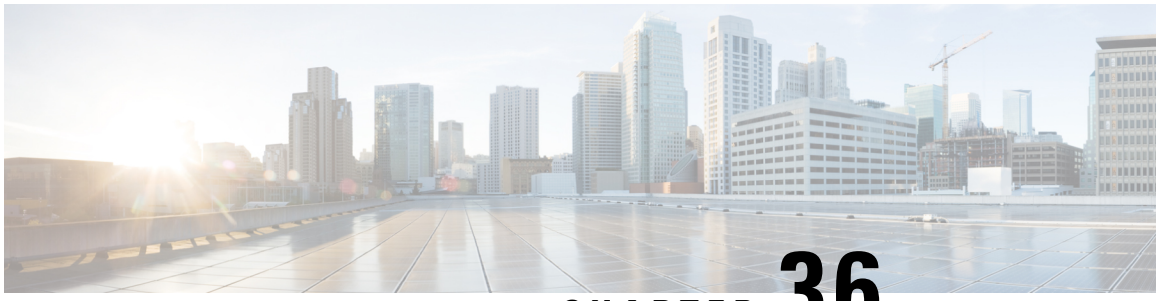
5. On the single-tenant Cisco SD-WAN Manager instance, initiate the migration of the overlay to the multitenant deployment.

| | |
|---|---|
| Method | POST |
| URL | https://*ST-vManage-IP-address* |
| Endpoint | dataservice/tenantmigration/networkMigration |
| Authorization | Admin user credentials. |
| Body | Required<br>Format: Raw text<br>Content: Migration token obtained in **Step 4**. |
| Response | Format: JSON<br>{<br>"processId": <vManage_process_ID>,<br>} |

In Cisco SD-WAN Manager, check the status of the migration task. As part of the migration task, the address of the multitenant Cisco SD-WAN Validator, and the service provider and tenant organization names are pushed to the WAN edge devices of the single-tenant overlay. If the task succeeds, WAN edge devices form control connections to controllers in the multitenant deployment; the WAN edge devices are no longer connected to the controllers of the single-tenant overlay.

Attach any CLI templates detached from the edge devices (in Step 1) after migration to the multitenant deployment. Before you attach the templates, update the Cisco SD-WAN Validator IP address and the Organization name to match the configuration of the multitenant deployment.

**Note** In the single-tenant deployment, if Cisco SD-WAN Manager-signed certificates are installed on cloud-based WAN edge devices, the certificates are cleared when the devices are migrated to the multitenant deployment. You must re-certify the devices on the multitenant Cisco SD-WAN Manager. If enterprise certificates are installed on the cloud-based WAN edge devices, the certificates are not affected by the migration. For more information, see Enterprise Certificates.



CHAPTER 36

# Cisco Catalyst SD-WAN Carrier Supporting Carrier

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 263: 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<br>Cisco vManage Release 20.6.1 | The feature adds support for carrier supporting carrier (CSC) connectivity on Cisco IOS XE Catalyst SD-WAN devices.<br>CSC enables you to interconnect IP or multiprotocol label switching (MPLS) networks operating at different sites over an MPLS backbone network. Using CSC requires an edge router that supports CSC functionality, called a carrier edge (CE) device, at each site. This feature enables a Cisco IOS XE Catalyst SD-WAN device to serve as a CE device, making it unnecessary to have a separate dedicated CE device at each site managed by Cisco Catalyst SD-WAN. |


- Prerequisites for Cisco Catalyst SD-WAN Carrier Supporting Carrier, on page 1048
- Restrictions for Cisco Catalyst SD-WAN Carrier Supporting Carrier, on page 1048
- Information About Cisco Catalyst SD-WAN Carrier Supporting Carrier, on page 1048
- Benefits of Cisco Catalyst SD-WAN Carrier Supporting Carrier, on page 1050
- Use Cases for Cisco Catalyst SD-WAN Carrier Supporting Carrier, on page 1050
- Configure Carrier Supporting Carrier, on page 1050
- Verify That a Device is Configured for Carrier Supporting Carrier, on page 1054

# Prerequisites for Cisco Catalyst SD-WAN Carrier Supporting Carrier

A Cisco IOS XE Catalyst SD-WAN device that functions as a CSC customer edge (CSC-CE) device must have an external border gateway protocol (eBGP) peer connection with the CSC provider edge (CSC-PE) router.

# Restrictions for Cisco Catalyst SD-WAN Carrier Supporting Carrier

- IPv6 addressing is not supported.
- Network address translation (NAT) for the MPLS link is not supported.
- Firewall services on the MPLS link are not supported.
- Cloud OnRamp for SaaS is not supported.
- VPN route leak is not supported.

# Information About Cisco Catalyst SD-WAN Carrier Supporting Carrier

### Carrier Supporting Carrier

Carrier supporting carrier (CSC) is a hierarchical VPN model that allows organizations to interconnect their IP or MPLS networks located at different sites over an MPLS backbone network. This eliminates the need for the organizations to build and maintain their own MPLS backbone.

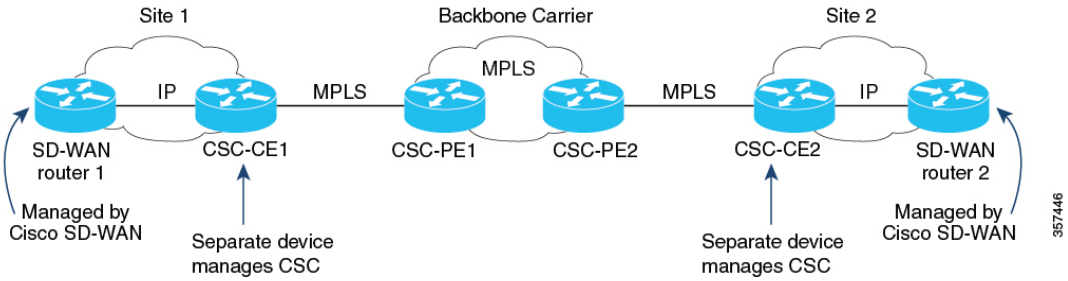
The following are components of CSC:

- Backbone carrier: The service provider that provides the backbone network. Typically, the backbone carrier network employs multiple segments to segregate the traffic of different customer carriers that share the backbone carrier network. The backbone carrier may be managed by the same organization or by a different organization as the customer carriers.
- Customer carrier: An organization that uses the backbone network to route traffic from one site to another. The customer carrier may be part of the organization that operates the backbone network, or may be independent.
- CSC-CE: Customer edge (CE) device. This device operates within a local site network and connects the site to the backbone carrier, using an MPLS connection. It utilizes the backbone carrier to connect to other sites.
- CSC-PE: Provider edge (PE) device. This device operates within the backbone carrier network and connects to CSC-CE devices at customer sites, using an MPLS connection.

### Cisco Catalyst SD-WAN Carrier Supporting Carrier

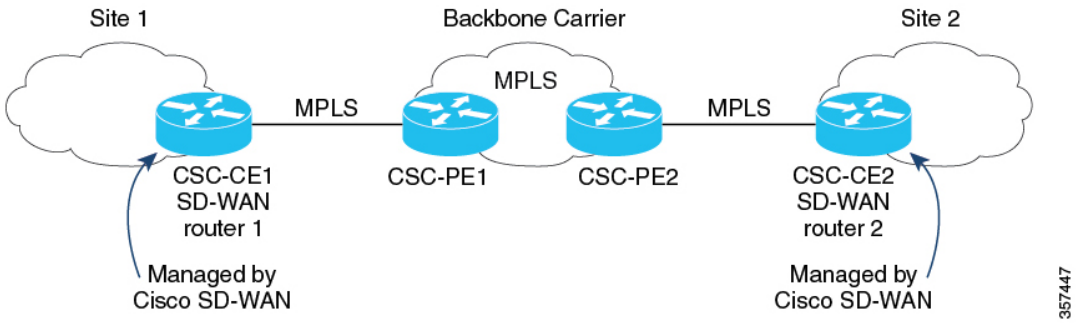
The following illustration shows a CSC network topology with a Cisco IOS XE Catalyst SD-WAN device at each site, using a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. Because the Cisco IOS XE Catalyst SD-WAN devices cannot function as a CSC-CE when using these releases, the topology requries two separate devices at each site: an edge device managed by Cisco Catalyst SD-WAN and a separate CSC-CE device.

***Figure 10: Carrier Supporting Carrier with Cisco Catalyst SD-WAN, Before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a***




From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, a Cisco IOS XE Catalyst SD-WAN device can serve as a CSC-CE device, making it unnecessary to have a separate dedicated CSC-CE device. As compared with the previous illustration, the following illustration shows a simpler CSC network topology, with Cisco IOS XE Catalyst SD-WAN devices providing CSC-CE functionality.

***Figure 11: Carrier Supporting Carrier with Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Later***




### Traffic Flow

If a CSC-CE device only has an MPLS connection to the neighbor CSC-PE device, then all traffic from the CSC-CE device uses the MPLS connection, including the following traffic types:

- Service VPN traffic
- Control traffic
- Cisco Catalyst SD-WAN bidirectional forwarding detection (BFD) probe traffic

If a CSC-CE device has an MPLS connection to the neighbor CSC-PE device and also has a separate connection to the internet, then the traffic from the CSC-CE device may use different connections, as follows:

- Based on the configured traffic policy, control traffic and BFD probe traffic can use the internet and MPLS connections.

- Service VPN traffic uses only the MPLS connection.

### Label Switching

For traffic that uses an MPLS connection between a CSC device and the backbone carrier, the backbone carrier manages the traffic using label-switched paths, and has no information about the customer carrier routes.

# Benefits of Cisco Catalyst SD-WAN Carrier Supporting Carrier

Cisco Catalyst SD-WAN support for CSC enables a Cisco IOS XE Catalyst SD-WAN device to serve as an edge device at a site where CSC is required. With the Cisco IOS XE Catalyst SD-WAN device providing CSC-CE functionality, it is not necessary to have a separate router serving the CE role.

# Use Cases for Cisco Catalyst SD-WAN Carrier Supporting Carrier

Cisco Catalyst SD-WAN support for CSC is useful for global organizations that use CSC with a backbone carrier to support multiple, separate divisions of the organization. Each division's traffic is private but shares a common backbone carrier.

Service providers that use a CSC topology may benefit from Cisco Catalyst SD-WAN support for CSC. Carrier edge devices managed by Cisco Catalyst SD-WAN can support CSC, making it unnecessary to have a separate device to manage CSC functionality.

# Configure Carrier Supporting Carrier

You can configure the CE devices for CSC in the following ways:

- (Recommended) In Cisco SD-WAN Manager, use a BGP feature template.
- In Cisco SD-WAN Manager, use a CLI template to configure CSC by CLI.

## Configure Carrier Supporting Carrier

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 Carrier Supporting Carrier Using the CLI

We recommend that you use the BGP feature template in Cisco SD-WAN Manager to configure Cisco IOS XE Catalyst SD-WAN devices for use with CSC. If it is necessary to configure a device by CLI, use a CLI template in Cisco SD-WAN Manager.

### Before You Begin

Before you configure a Cisco IOS XE Catalyst SD-WAN device to provide CSC-CE functionality, apply a BGP configuration to the device. The following steps add CSC functionality.

### Configure Carrier Supporting Carrier the CLI

1. Configure the following on CSC-CE1:

   a. Configure the device to map MPLS labels to VRFs. For incoming traffic, the router checks the MPLS label of the traffic and uses the IP loookup table of the VRF mapped to that label. For example, if MPLS label 10 is mapped to VRF 1, then for incoming traffic with the MPLS label 10, the router uses the IP lookup table of VRF 1. For information about mmapping MPLS labels to VRFs, see the Cisco documentation for MPLS forwarding commands.

   ```
   Device# config-transaction
   Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
   Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
   Device(config)# mpls label range min-label max-label static min-static-label
   max-static-label
   ```

   b. Enable multiprotocol label switching (MPLS) on the interface.

   ```
   Device(config)# interfaceinterface
   Device(config-if)# mpls bgp forwarding
   ```

   c. Enter router configuration mode and configure the router to run a BGP process.

   ```
   Device(config-if)# router bgp bgp-number
   ```

   d. Configure a CSC-PE device as the neighbor, where *neighbor-ip* is the address of the neighbor CSC-PE device.

   ```
   Device(config-router)# neighbor neighbor-ip allowas-in
   ```

   e. If the device uses a loopback WAN interface, advertise the ability of the router to send MPLS labels with BGP routes. The **explicit-null** keyword enables a CSC-CE router to send labels with a value of 0 to its neighbor.

**Note** If you include the **neighbor** *neighbor-ip* **send-label explicit-null** command on a device that does not use a loopback WAN interface, it does not adversely impact performance.

```
Device(config-router)# neighbor neighbor-ip send-label explicit-null
```

2. Configure the following on CSC-CE2:

   a. Configure the device to map MPLS labels to VRFs. For incoming traffic, the router checks the MPLS label of the traffic and uses the IP loookup table of the VRF mapped to that label. For example, if MPLS label 10 is mapped to VRF 1, then for incoming traffic with the MPLS label 10, the router uses

the IP lookup table of VRF 1. For information about mmapping MPLS labels to VRFs, see the Cisco documentation for MPLS forwarding commands.

```
Device# config-transaction
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
Device(config)# mpls label range min-label max-label static min-static-label
max-static-label
```

**b.** Enable multiprotocol label switching (MPLS) on the interface.

```
Device(config)# interfaceinterface
Device(config-if)# mpls bgp forwarding
```

**c.** Enter router configuration mode and configure the router to run a BGP process.

```
Device(config-if)# router bgp bgp-number
```

**d.** Configure a CSC-PE device as the neighbor, where *neighbor-ip* is the address of the neighbor CSC-PE device.

```
Device(config-router)# neighbor neighbor-ip as-override
```

**e.** If the device uses a loopback WAN interface, advertise the ability of the router to send MPLS labels with BGP routes.

```
Device(config-router)# neighbor neighbor-ip send-label explicit-null
```

### Example

The following examples show a complete BGP configuration, including CSC functionality, for two devices: CSC-CE1 and CSC-CE2.

- CSC-CE1 has the address 10.1.1.10.
- CSC-CE2 has the address 10.1.1.20.
- CSC-PE1 (the neighbor of CSC-CE1) has the address 10.2.2.10.
- CSC-PE2 (the neighbor of CSC-CE2) has the address 10.2.2.20.

The following is the configuration for CSC-CE1:

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99
interface GigabitEthernet2
 no shutdown
 mpls bgp forwarding
 ip address 10.1.1.15 255.255.255.0

router bgp 10
 bgp log-neighbor-changes
 bgp router-id 172.16.255.15
 neighbor 10.1.1.20 remote-as 100
 neighbor 10.1.1.20 fall-over bfd
address-family ipv4 unicast
  maximum-paths 4
  neighbor 10.1.1.20 activate
  neighbor 10.1.1.20 advertisement-interval 30
  neighbor 10.2.2.10 allowas-in
  neighbor 10.2.2.10 send-label explicit-null
```

```
  neighbor 10.1.1.20 send-community both
  exit-address-family
 !
 timers bgp 60 180
```

The following is the configuration for CSC-CE2:

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99
interface GigabitEthernet5
 ip address 10.0.6.11 255.255.255.0
 negotiation auto
 mpls bgp forwarding

router bgp 10
 bgp log-neighbor-changes
 bgp router-id 172.16.255.11
 neighbor 10.1.1.10 remote-as 200
 address-family ipv4 unicast
  neighbor 10.1.1.10 activate
  neighbor 10.1.1.10 advertisement-interval 30
    neighbor 10.2.2.20 as-override
    neighbor 10.2.2.20 send-label explicit-null
  network 10.0.7.0 mask 255.255.255.0
  redistribute connected
  redistribute static
  exit-address-family
```

# Verify That a Device is Configured for Carrier Supporting Carrier

To verify that a device is configured correctly to reach a remote CSC-CE device, execute the **show ip route** *remote-csc-ce-device-address* command on the device. Verify that the command output shows the following:

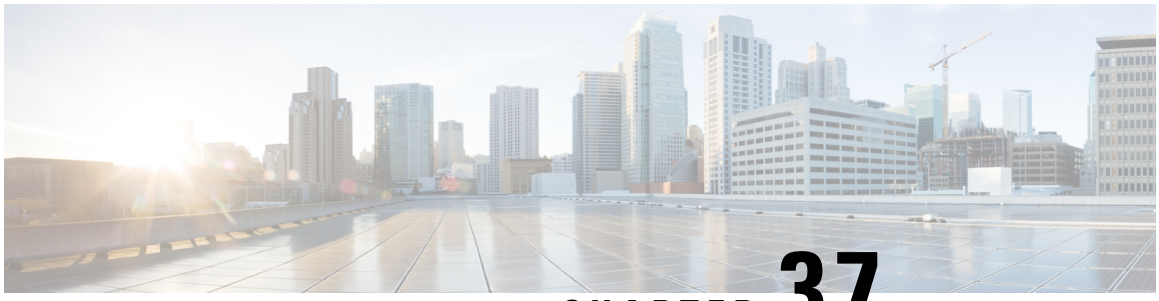
- A routing entry for the remote site IP address.
- One or more routing descriptor blocks describing the next-hop addresses for the path to the remote CSC-CE device. Verify that each descriptor block includes an MPLS label.

### Example

```
Device# show ip route 10.0.1.100
Routing entry for 10.0.1.0/24
...
Routing Descriptor Blocks:
* 10.1.1.100, from 10.1.1.100, 00:00:50 ago
...
MPLS label: 26
…
```

If the device is not configured correctly, the output displays the following:

```
% Subnet not in table
```



CHAPTER 37

# Wireless Management on Cisco 1000 Series Integrated Services Routers

**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**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

*Table 264: 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<br>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.<br>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. |

| Feature Name | Release Information | Description |
|---|---|---|
| Wireless Management on Cisco ISR 1000 Series Routers (supporting WiFi 6 WLAN module) | Cisco IOS XE Catalyst SD-WAN Release 17.9.1a<br>Cisco vManage Release 20.9.1 | This feature enables you to configure wireless LAN settings on WiFi 6-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager.<br>The Embedded Wireless Controller on Cisco 1000 Series Integrated Services Routers helps you provide wireless connectivity without the need for another external controller to configure and manage the wireless settings on the routers. |


- Supported Devices for Wireless Management on Cisco ISR 1000 Series Routers, on page 1056
- Prerequisites for Wireless Management on Cisco ISR 1000 Series Routers, on page 1057
- Restrictions for Wireless Management on Cisco ISR 1000 Series Routers, on page 1058
- Information About Wireless Management on Cisco ISR 1000 Series Routers, on page 1058
- Configure Wireless Management on Cisco ISR 1000 Series Routers, on page 1058
- Configure Wireless Management on Cisco ISR 1000 Series Routers Using a CLI Template, on page 1061
- Monitor Wireless Configuration on Cisco ISR 1000 Series Routers, on page 1062
- Configuration Example for Wireless Configuration on Cisco ISR 1000 Series Routers, on page 1063
- Troubleshooting Wireless Configuration on Cisco ISR 1000 Series Routers, on page 1064


# Supported Devices for Wireless Management on Cisco ISR 1000 Series Routers

The following table displays a list of Cisco ISR 1000 Series routers that include the WLAN module and supporting WiFi 5.

*Table 265: Cisco ISR 1000 Series Routers*

| Device Family | Device Name | Release Version |
|---|---|---|
| Cisco ISR 1000 Series Routers with WLAN module supporting WiFi 5 | • C1101-4PLTEPW<br>• C1109-4PLTE2PW<br>• C1111-4PW<br>• C1111-8PLTEEAW<br>• C1111-8PW<br>• C1112-8PLTEEAW<br>• C1112-8PW<br>• C1113-8PLTEEAW<br>• C1113-8PMW<br>• C1113-8PW<br>• C1116-4PLTEEAW<br>• C1116-4PW<br>• C1117-4PLTEEAW<br>• C1117-4PLTELAW<br>• C1117-4PMLTEEAW<br>• C1117-4PMW<br>• C1117-4PW<br>• C1121-8PLTEPW<br>• C1121X-8PLTEPW | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1 |
| Cisco ISR 1000 Series Routers with WLAN module supporting WiFi 6 | • C1131X-8PLTEPW<br>• C1131-8PLTEPW<br>• C1131X-8PW<br>• C1131-8PW | Cisco IOS XE Catalyst SD-WAN Release 17.9.1a<br>Cisco vManage Release 20.9.1 |

# Prerequisites for Wireless Management on Cisco ISR 1000 Series Routers

- Add the management interface of the Wireless LAN (WLAN) module to a specific VLAN in order to access servers such as DHCP and RADIUS.

- Configure a DHCP server to assign the IP address for the access point.
- Configure a switch virtual interface (SVI) on the Cisco ISR 1000 Services Router for virtual WLAN controller management.

# Restrictions for Wireless Management on Cisco ISR 1000 Series Routers

- You can configure only one access point on the LAN side of the router that is configured with Cisco Mobility Express. However, you can connect other external access points to the router that are not configured with Cisco Mobility Express.
- Ensure that there are no other accessible wireless controllers on the LAN side.

# Information About Wireless Management on Cisco ISR 1000 Series Routers

A WLAN module supporting WiFi 5 is provisioned on a Cisco ISR 1000 Series Routers for wireless connectivity. Cisco Mobility Express, a virtual wireless LAN controller, is installed in the WLAN module to provide wireless LAN access. The wireless settings for wireless LAN access are available on Cisco Mobility Express, and these settings can be configured and managed using Cisco SD-WAN Manager

C1131 Cisco IOS XE Catalyst SD-WAN devices includes an Embedded Wireless Controller (EWC) that supports WiFi 6. The EWC also serves as a virtual wireless controller that is installed on the WLAN module. The wireless settings for wireless LAN access are available on the EWC; these settings can be configured and managed using Cisco SD-WAN Manager.

# Configure Wireless Management on Cisco ISR 1000 Series 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.<br>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:<br>• **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server.<br>• **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase.<br>• **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:<br>• **2.4GHz**<br>• **5GHz**<br>• **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.<br>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.**<br>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 Wireless Management on Cisco ISR 1000 Series Routers Using a CLI Template

This section provides sample CLI configurations to configure and manage wireless settings on Cisco ISR 1000 Series Routers using the CLI templates.

### Configure Radio Profile Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

```
radio-profile 24ghz
shutdown
exit
radio-profile 5ghz
no shutdown
```

### Configure WLAN Profile Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

```
wlan-profile wlan-profile-sample-1
vlan-id 100
ssid sample-ssid-1
data-security personal
passphrase 0 Pass-Phrase-Sample123#
qos-type silver
wlan-profile wlan-profile-sample-2
vlan-id 200
ssid sample-ssid-2
data-security enterprise
aaa radius-server 10.2.3.4 auth-port 1812 shared-secret 0 EsrdT_23sss

qos-type gold
nobroadcast-ssid
```

### Configure General WLAN Settings Using a CLI Template

For more informationabout using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** By default, CLI templates execute commands in global config mode.

```
wireless-lan country US
wireless-lan mgmt ip address10.16.1.100 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 0 sRe32dfst#asd
```

Here is the complete configuration example that shows that show how to configure and manage wireless settings on Cisco ISR 1000 Series Routers.

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

# Monitor Wireless Configuration on Cisco ISR 1000 Series Routers

To monitor the wireless settings that are configured on Cisco ISR 1000 Series Routers using Cisco SD-WAN Manager, perform this procedure :

1. From the Cisco SD-WAN Manager menu, navigate to **Monitor** > **Network**.
2. Choose a router from the list of the routers.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following options:

| Device Option | Description |
|---|---|
| **Wireless Radio** | Displays the radio parameters of the wireless LAN. |
| **Wireless SSID** | Displays information about the wireless SSID. |
| **Wireless Clients** | Displays information about the wireless clients in the wireless LAN. |

# Configuration Example for Wireless Configuration on Cisco ISR 1000 Series Routers

The following is an example of wireless configuration of a Cisco ISR 1000 Series Routers:

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

# Troubleshooting Wireless Configuration on Cisco ISR 1000 Series Routers

## Access Point Cannot Connect to Cisco Mobility Express or EWC

### Problem

An access point is not able to connect to the Cisco Mobility Express or EWC.

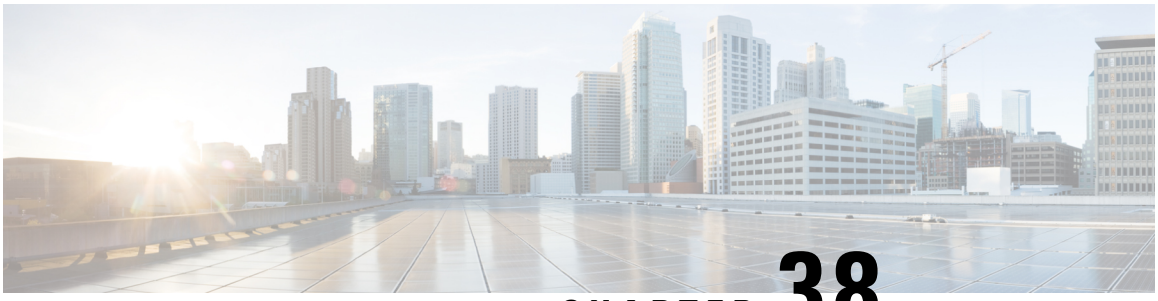
### Possible Causes

This problem is most likely to occur when there is no DCHP server in the management VLAN (the native VLAN of interface Wlan-GigabitEthernet).

### Solution

Add the management interface of the WLAN module to a specific VLAN in order to access servers like DHCP and RADIUS. See Prerequisites for Wireless Management on Cisco ISR 1000 Series Routers, on page 1057

A DHCP server is required in the native VLAN of the WiFi module to assign IP address for the access point. Without IP address, the access point will not able to connect to Cisco Mobility Express or EWC.



CHAPTER 38

# Extended Visibility with Cisco SD-WAN and Cisco ThousandEyes

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


- Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes, on page 1065


# Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes

***Table 266: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes | Cisco IOS XE Release 17.6.1a<br><br>Cisco vManage Release 20.6.1 | You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on supported Cisco IOS XE Catalyst SD-WAN devices to integrate Cisco Catalyst SD-WAN with Cisco ThousandEyes. You can install and activate the Cisco ThousandEyes Enterprise agent through Cisco SD-WAN Manager.<br><br>By integrating Cisco Catalyst SD-WAN with Cisco ThousandEyes, you can gain granular insights into network and application performance with full hop-by-hop path analysis across the Internet, and isolate fault domains for expedited troubleshooting and resolution. |

| 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<br>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<br>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. |

# Information About for Extending Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes

Cisco ThousandEyes is a SaaS application that provides you an end-to-end view across networks and services that impact your business. It monitors the network traffic paths across internal, external, and carrier networks and the Internet in realtime to provide network performance data. Cisco ThousandEyes provides intelligent insights into your WAN and the cloud and helps you optimize application delivery and end-user experience.

### Deploy and Configure the ThousandEyes Agent

From Cisco IOS XE Release 17.6.1, you can deploy and configure the Cisco ThousandEyes Enterprise agent on Cisco IOS XE Catalyst SD-WAN devices to enable extensive monitoring of the WAN traffic for enhanced visibility within and beyond the Cisco Catalyst SD-WAN fabric. The Cisco ThousandEyes Enterprise agent is an embedded Docker-based application that runs on Cisco IOS XE Catalyst SD-WAN devices as a docker-type container application using the IOX Docker application-hosting capability.

### Services in the Cisco Networking Cloud

From Cisco Catalyst SD-WAN Manager Release 20.14.1, you can navigate to Cisco services hosted in the Cisco Networking Cloud, such as Cisco ThousandEyes. Enable the cross platform navigator in **Administration** > **Settings** > **Cross Platform Navigator**.

### More Information

For more information on Cisco ThousandEyes and on configuring tests and viewing results in the Cisco ThousandEyes portal, see the Cisco ThousandEyes *Getting Started* documentation.

# Supported Devices for Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes

| Release | Platform | Device Model | Minimum Supported ThousandEyes Enterprise Agent Version |
|---|---|---|---|
| Cisco IOS XE Release 17.6.1a and later | Cisco Catalyst 8300 Series Edge Platforms | C8300-1N1S-6T | 4.0.2 |
| | | C8300-1N1S-4T2X | |
| | | C8300-2N2S-6T | |
| | | C8300-2N2S-4T2X | |
| | Cisco Catalyst 8200 Series Edge Platforms | C8200-1N-4T | 4.0.2 |
| | | C8200L-1N-4T | |
| | Cisco 4000 Series Integrated Services Routers | ISR4461 | 4.0.2 |
| | | ISR4451 | |
| | | ISR4431 | |
| | | ISR4351 | |
| | | ISR4331 | |
| | | ISR4321 | |
| | | ISR4221X | |
| Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and later | Cisco 1000 Series Integrated Services Routers | ISR1100X-6G | 4.1.0 |
| Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and later | Cisco Catalyst 8500 Series Edge Platforms | C8500-12X | 4.2.0 |
| | | C8500-12X4QC | |
| | | C8500L-8S4X | |
| | Cisco ASR 1000 Series Aggregation Services Routers | ASR 1001-HX | 4.2.0 |
| | | ASR 1001-X | |
| | | ASR 1002-HX | |
| | | ASR 1002-X | |
| | | ASR 1006-X (RP3) | |

### Storage and DRAM Requirements

- **External Storage**: On devices that are equipped with external storage (SSD M.2 NVMe), the Cisco ThousandEyes Enterprise agent is installed in the external storage. The minimum external storage capacity

that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If the device does not have sufficient external storage capacity, upgrade the storage capacity to meet the minimum requirement.

Although the minimum external storage capacity that is required is 8 GB, we recommend that you provision the device with an external storage capacity of 16 GB or more. With the minimum external storage capacity, you may need to manually clean up files while upgrading the software image on the device.

- **Bootflash**: On devices that are not equipped with external storage, the Cisco ThousandEyes Enterprise agent is installed on the bootflash. The minimum bootflash capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If the device does not have sufficient bootflash capacity, upgrade the storage capacity to meet the minimum requirement.

**Important** On the ISR1100X-6G, the Cisco ThousandEyes Enterprise agent is installed on the bootflash. For this particular device model, the minimum bootflash capacity that is required to install the agent is 16 GB.

Although the minimum bootflash capacity that is required is 8 GB, we recommend that you provision the device with an bootflash capacity of 16 GB or more. With the minimum bootflash capacity, you may need to manually clean up files while upgrading the software image on the device.

- **DRAM**: The minimum DRAM capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If a device does not have the minimum DRAM capacity that is required to install the Cisco ThousandEyes Enterprise agent, upgrade the DRAM to meet the minimum requirement.
- Cisco ThousandEyes Enterprise agent can be deployed with other applications if the device has the resources (CPU, memory, and storage) to run the other applications. If the available resources are not sufficient to run the other applications, IOX generates an error message and does not run the other applications.

  To host the Cisco ThousandEyes Enterprise agent, a Cisco IOS XE Catalyst SD-WAN device must have a minimum of 8 GB DRAM. If you wish host additional applications such as UTD and DRE on the same device, we recommend that you provision the device with at least a 16 GB DRAM.

# Prerequisites for Extending Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes

- Before deploying the Cisco ThousandEyes Enterprise agent, you must create an account on the Cisco ThousandEyes portal and obtain an account group token. The agent uses the token to authenticate itself with Cisco ThousandEyes and check-in to the right Cisco ThousandEyes account.

  For information on obtaining the account group token, see *Where Can I Get the Account Group Token?* on Cisco ThousandEyes Documentation portal.

- The Cisco ThousandEyes Enterprise agent requires DNS name resolution and HTTP/HTTPS connectivity to discover and register with the Cisco ThousandEyes portal. Ensure that this connectivity exists before deploying the agent by configuring the appropriate firewall rules, NAT settings, upstream routing, and other related settings.

  For more information on the required firewall configuration, see *Firewall Configuration for Enterprise Agents* on Cisco ThousandEyes Documentation portal.

# Restrictions for Extending Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes

- Cisco ThousandEyes Enterprise agent probes are sourced from Virtual Port-Group interfaces and are not affected by AppRoute data policies.
- The Cisco ThousandEyes Enterprise agent, hosted natively as a container application on Cisco IOS XE Catalyst SD-WAN devices, does not support browser-based application tests, such as page load test and transaction test.
- For every changes to the thousandeye instance to reflect the changes done you need uninstall or deactivate and reintsall and reactivate it.

  For Cisco IOS XE Catalyst SD-WAN devices prior to Cisco IOS XE Release 17.6.1, the Docker image can be installed either directly from the ThousandEyes download servers, or by downloading the container image to a local machine and uploading it to the router via SCP, FTP, TFTP, or USB storage, depending on whether the router has direct internet access or not.

  For Cisco IOS XE Catalyst SD-WAN devices after Cisco IOS XE Release 17.6.1, in addition to the previous methods, you can install the Enterprise Agent via bootflash.
- The provision for Cisco ThousandEyes enterprise agent in transport VPN (VPN 0) is not supported.

# Configure Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN Devices

## 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 **Manager**.
5. In the **Upload VNF's Package to Manager** 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 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.<br>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.<br>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)<br>Enter the IP address of your preferred DNS server.<br>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:<br>• **Static**<br>• **PAC**<br>Static proxy settings:<br>• **Proxy Host**: Set the configuration as a **Global** setting and enter the hostname of the proxy server.<br>• **Proxy Port**: Set the configuration as a **Global** setting and enter the port number of the proxy server.<br>PAC settings:<br>• **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.

## Provision Cisco ThousandEyes Enterprise Agent in a Service VPN Using CLI

This section provides example command sequences to provision the Cisco ThousandEyes Enterprise agent on Cisco IOS XE Catalyst SD-WAN devices using a device CLI template or an add-on CLI template.

### 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 Managersoftware repository, while provisioning the agent, Cisco SD-WAN Manager installs and activates the latest version of the agent software.

This section provides example CLI configurations to provision the Cisco ThousandEyes Enterprise agent in a service VPN.

1. Enable IOX on the device.

```
iox
```

2. Configure virtual port group. The virtual port group acts as the gateway for the Cisco ThousandEyes Enterprise agent.

```
interface VirtualPortGroup4
 vrf forwarding 100
  ip address 192.168.61.1 255.255.255.252
```

3. Configure app-hosting paramters for the Cisco ThousandEyes Enterprise agent.

```
app-hosting appid te
app-vnic gateway0 virtualportgroup 4 guest-interface 0
 guest-ipaddress 192.168.61.2 netmask 255.255.255.252
app-default-gateway 192.168.61.1 guest-interface 0
app-resource docker
 prepend-pkg-opts
 run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=z0kemf"
 run-opts 2 "--hostname ISR4461TE"
 run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e TEAGENT_PROXY_LOCATION=proxy-exmaple.com:80"
name-server0  192.168.168.183
start
```

**Note**

- You can use the proxy configuration only if the Cisco ThousandEyes agent does not have an Internet access without a proxy. Also, the hostname is optional and if you do not provide the hostname during the installation, the device hostname will be used as the Cisco ThousandEyes agent hostname. The device hostname will be displayed on the Cisco ThousandEyes portal. From Cisco IOS XE Release 17.7.1a, the DNS name server information is optional.
- If the Cisco ThousandEyes agent uses a private IP address, establish a connection to the device through NAT.

## 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.

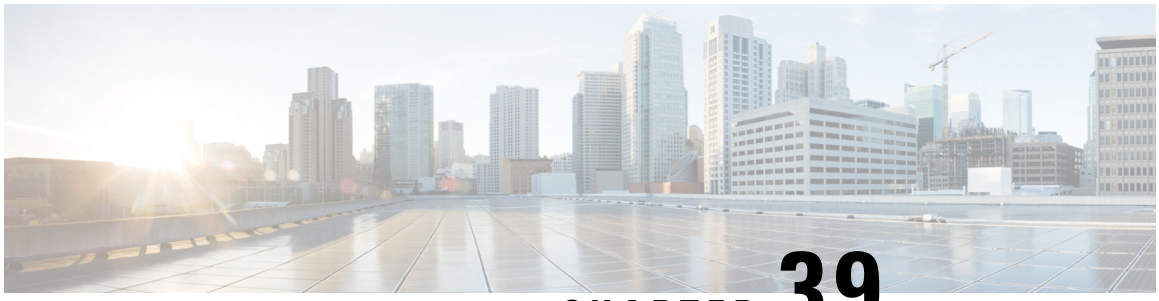
4. For this template, click **…** and then click **Edit**.
5. Click **Additional Templates**.
6. In the **Additional Templates** section, for **ThousandEyes Agent** choose **None** from the drop-down list.
7. Click **Update**.
8. Update necessary variables, if any, and click **Next**.
9. Review the configuration and click **Configure Devices**.

# Troubleshoot Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN Devices

1. Connect to Cisco ThousandEyes Enterprise agent.

   ```
   Device#app-hosting connect appid Appid session /bin/bash
   ```

2. To verify the agent configuration, check the following CFG file: `/etc/te-agent.cfg`
3. To view the agent logs, check the following file: `var/log/agent/te-agent.log`



CHAPTER 39

# Layer 2 VPN


- Layer 2 VPN, on page 1075
- Information About Layer 2 VPN Support within the Cisco Catalyst SD-WAN Overlay Network, on page 1076
- Supported Platforms for Layer 2 VPN, on page 1077
- Restrictions for Layer 2 VPN, on page 1077
- Configure an L2VPN on a Cisco IOS XE Catalyst SD-WAN Device Using CLI Template or CLI Add-On Feature Template, on page 1077
- Configure Point-to-Point Layer 2 VPN Using CLI Template or CLI Add-On Feature Template, on page 1078
- Configure Point-to-Multipoint Layer 2 VPN Using CLI Template or CLI Add-On Feature Template, on page 1080
- Configure Layer 2 VPN Switchport, on page 1083
- Advanced Layer 2 Configuration, on page 1085
- Verify a Layer 2 VPN Using CLI , on page 1085
- Monitor Configured Layer 2 VPN Using CLI, on page 1090


# Layer 2 VPN

*Table 267: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Layer 2 (L2) VPN | Cisco IOS XE Catalyst SD-WAN Release 17.14.1a<br><br>Cisco Catalyst SD-WAN Control Components Release 20.14.x | The feature adds Layer 2 VPN support on the Cisco Catalyst SD-WAN overlay network.<br><br>It allows you to configure Layer 2 point-to-point and point-to-multipoint connections within the Cisco Catalyst SD-WAN fabric. |

# Information About Layer 2 VPN Support within the Cisco Catalyst SD-WAN Overlay Network

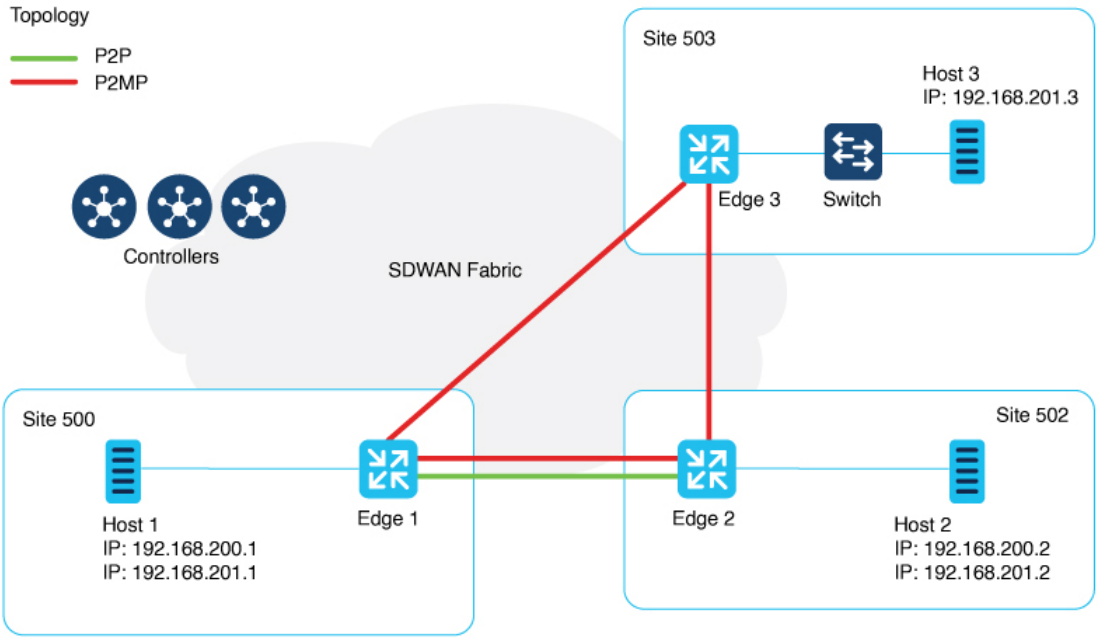
The Cisco Catalyst SD-WAN solution provides Layer 3 services with security, segmentation, and scalability across the overlay network. Considering the importance of Layer 2 (L2) connectivity, particularly for legacy systems and non-IP applications, Layer 2 services are supported within the Cisco Catalyst SD-WAN overlay network. L2VPN support enables using legacy applications that require Layer 2 connectivity in the Cisco Catalyst SD-WAN fabric.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the following L2VPN features are supported:

- Point-to-point L2VPN Service (P2P)
- Point-to-Multipoint L2VPN Service (P2MP)
- Single homing
- Flood and Learn in WAN and LAN
- Ingress replication for Broadcast, Unknown-unicast and Multicast (BUM)
- Full mesh topology only

### Network Topology for Layer 2 Connections

***Figure 12: Topology***




This illustration shows three sites and shows P2P (green line) and P2MP (red lines) connections between edge routers at the sites.

- Point-to-Point (P2P): Connects sites 500 and 502 with a dedicated Layer 2 VPN. The L2VPN between the two sites allow Host 1 and Host 2 to interact.
- Point-to-Multipoint (P2MP): Connects sites 500, 502, and 503 with Layer 2 VPN. Host 1 communicates with both Host 2 and Host 3 across a Layer 2 multipoint network.

The L2VPN connections use existing Cisco Catalyst SD-WAN tunnels.

# Supported Platforms for Layer 2 VPN

Minimum software releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

All Cisco IOS XE Catalyst SD-WAN devices.

# Restrictions for Layer 2 VPN

Minimum software releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Control Components Release 20.14.1

Hub-and-spoke topology is currently not supported for L2VPN.

# Configure an L2VPN on a Cisco IOS XE Catalyst SD-WAN Device Using CLI Template or CLI Add-On Feature Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Control Components Release 20.14.1

This section provides CLI configurations to configure L2VPN on a Cisco IOS XE Catalyst SD-WAN device.

### Before You Begin

When configuring a device to support L2VPN services, we recommend using a single CLI add-on template for all the required configuration commands. The tasks are described separately, but you can combine the configuration commands into one template.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

**Note** In Cisco SD-WAN Manager, use a CLI add-on template to configure the L2VPN instance on participating devices.

To configure L2VPN on an edge device, configure an instance, a bridge-domain, and an interface. Add the configuration pieces, as shown in the following configuration, into your CLI add-on feature template or CLI template.

### Configure an L2VPN Instance, Bridge-Domain, and Interfaces

1. Configure an L2VPN instance for P2P and P2MP connections.

```
l2vpn sdwan instance instance-id point-to-point
l2vpn sdwan instance instance-id multipoint
```

The instance ID is a unique identifier for each L2VPN connection, and must not overlap or be shared with any L3 VRFs in the Cisco Catalyst SD-WAN fabric. For example, you cannot use L2VPN instance 10 and vrf definition 10.

2. Configure a bridge-domain.

```
bridge-domain bridge-id
```

3. Configure a Layer 2 interface on a Cisco IOS XE Catalyst SD-WAN device.

```
interface vlan-id
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
  no shutdown
```

If you have not configured rewrite under service instance, dot1q must be the same at all sites participating in the Layer 2 network. For more information on configuring rewrite, see Advanced Layer 2 Configuration, on page 1085.

### Example

```
l2vpn sdwan instance 100 point-to-point
l2vpn sdwan instance 200 multipoint

bridge-domain 12
bridge-domain 13

interface Vlan2001
 service instance 200 ethernet
  encapsulation dot1q 2001
  no shutdown
```

For more information about the preceding commands, see Cisco IOS XE SD-WAN Qualified Command Reference.

# Configure Point-to-Point Layer 2 VPN Using CLI Template or CLI Add-On Feature Template

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1, Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

### Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

  By default, CLI templates execute commands in global config mode.

- You can use one L2VPN instance ID for one or more bridge domains. To identify a particular bridge-domain, use Virtual Circuit (VC) ID. This ID is the identifier of the virtual circuit between the Cisco IOS XE Catalyst SD-WAN devices. It must be the same at both ends of the circuit.

- To create a P2P pseudowire, L2VPN instance ID, and VC ID must be the same on different Cisco IOS XE Catalyst SD-WAN devices.
- Remote-site-id is only supported for P2P configuration.

The difference between P2P and P2MP is that, in P2MP there are no target sites.

This section provides the CLI configuration to configure P2P L2VPN services between two sites (sites A and B) on the Cisco Catalyst SD-WAN overlay network.

### Configure an Edge Router at Site A

Site A uses an edge router and connects the Ethernet interface to the L2 network that bridges to Site B.

1. Define the L2VPN instance for point-to-point service:

```
l2vpn sdwan instance instance-id point-to-point
```

2. Configure the Ethernet interface:

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
```

3. Define the bridge domain and associate it with the interface and L2VPN instance:

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id
 single homing
```

### Configure an Edge Router at Site B

Site B uses an edge router and Switchport Ethernet interface.

1. Define the L2VPN instance for point-to-point service:

```
l2vpn sdwan instance instance-id point-to-point
```

2. Define the VLAN for the L2VPN:

```
vlan vlan-id
 name L2vpn
```

3. Configure the VLAN interface:

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
  no shutdown
```

4. Configure the Ethernet interface as an access port for VLAN:

```
interface interface-name
 switchport access vlan vlan-id
```

5. Define the bridge-domain for Site B and associate it with the VLAN and L2VPN instance:

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id
 single homing
```

### Example

Site 500 is using a Cisco Catalyst 8000V Edge Software, where GigabitEthernet5 is connected to the Layer 2 network that bridges to Site 502.

```
l2vpn sdwan instance 100 point-to-point

interface GigabitEthernet5
 service instance 100 ethernet
  encapsulation dot1q 2002
  !
bridge-domain 100
 member GigabitEthernet5 service-instance 100
 member sdwan-instance 100 remote-site 502 vc-id 100 single-homing
```

Use Switchport GigabitEthernet 0/1/7 at Site 502 with a Cisco ISR1100-8P.

```
l2vpn sdwan instance 100 point-to-point
vlan 2002
 name L2vpn
interface Vlan2002
 service instance 100 ethernet
  encapsulation dot1q 2002
  no shutdown
  !
interface GigabitEthernet 0/1/7
 switchport access vlan 2002
bridge-domain 100
 member Vlan2002 service-instance 100
 member sdwan-instance 100 remote-site 500 vc-id 100 single-homing
```

After configuring the point-to-point L2VPN service on both sites, you can integrate these configuration blocks into your CLI Template or CLI Add-On Feature Template. This template can then be used to deploy the configuration across the relevant devices in the Cisco Catalyst SD-WAN fabric. Verify the connectivity and functionality of the L2VPN service following the deployment to confirm that the bridge between Site 500 and Site 502 is operational.

# Configure Point-to-Multipoint Layer 2 VPN Using CLI Template or CLI Add-On Feature Template

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1, Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

### Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

  By default, CLI templates execute commands in global config mode.

- One L2VPN instance ID can be used by one or more bridge domains. VC ID is used to identify a particular bridge-domain.
- L2VPN instance ID and VC ID must be the same on different edge devices.

This following section provides steps for configuring P2MP L2VPN over Cisco Catalyst SD-WAN overlay, connecting a local Layer 2 network at site A to multiple remote sites (B and C). Site A uses Gigabit Ethernet interface to connect to the Layer 2 network for bridging.

### Configuration an Edge Router at Sites A, B, and C

Site A is using an edge router, where an Ethernet interface is connected to the Layer 2 network that bridges to Site B and Site C.

1. Define the L2VPN instance for the multipoint service on the data center router:

```
l2vpn sdwan instance instance-id multipoint
```

2. Configure the Ethernet interface on the data center router:

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
```

3. Define the bridge-domain on the data center router and associate it with the interface and L2VPN instance:

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id
 single homing
```

### Configuration for an Edge Router at Site B

1. Define the L2VPN instance for multipoint service on the branch router:

```
l2vpn sdwan instance instance-id multipoint
```

2. Define the VLAN for the L2VPN on the branch router:

```
vlan vlan-id
 name L2vpn
```

3. Configure the VLAN interface on the branch router:

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
  no shutdown
```

4. Configure the Ethernet interface on the branch router as an access port for VLAN:

```
interface interface-name
 switchport access vlan vlan-id
```

5. Define the bridge-domain on the branch router and associate it with the VLAN and L2VPN instance:

```
bridge-domain bridge-id
 member vlan-nameservice-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id
 single homing
```

### Configuration for an Edge Router at Branch Router C

Repeat the same steps as for branch router B, substituting the specific interface used on router C. In this example, we have used the Ethernet interface.

1. Define the L2VPN instance for multipoint service on the branch router:

```
l2vpn sdwan instance instance-id multipoint
```

2. Define the VLAN for the L2VPN on the branch router:

```
vlan vlan-id
 name L2vpn
```

3. Configure the VLAN interface on the branch router:

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
  no shutdown
```

4. Configure the Ethernet interface on the branch router as an access port for VLAN:

```
interface interface-name
 switchport access vlan vlan-id
```

5. Define the bridge-domain on the branch router and associate it with the VLAN and L2VPN instance:

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id
 single homing
```

### Example

This section provides an example configuration for P2MP L2VPN service within the Cisco Catalyst SD-WAN overlay network, connecting a local Layer 2 network at site 500 to multiple remote sites (502 and 503). Site 500 uses GigabitEthernet6 interface to connect to the L2 network for bridging.

Verify the connectivity and functionality of the P2MP L2VPN service and ensure that all sites are correctly bridged.

Site 500 is using a Cisco Catalyst 8000V edge router, where GigabitEthernet6 is connected to the Layer 2 network that bridges to site 502 and site 503.

```
l2vpn sdwan instance 200 multipoint

interface GigabitEthernet6
 service instance 200 ethernet
  encapsulation dot1q 2001
```

```
  !
bridge-domain 200
 member GigabitEthernet6 service-instance 200
 member sdwan-instance 200 vc-id 200 single-homing
```

Configuration for the branch router 502:

```
l2vpn sdwan instance 200 multipoint

vlan 2001
 name L2MPvpn

interface Vlan2001
 service instance 200 ethernet
  encapsulation dot1q 2001
  no shutdown
  !
interface GigabitEthernet 0/1/6
 switchport access vlan 2001

bridge-domain 200
 member Vlan2001 service-instance 200
 member sdwan-instance 200 vc-id 200 single-homing
```

Configure Branch Router 503:

Repeat the same steps as for branch router 502, substituting the specific interface used on router 503. In this example, we have used the GigabitEthernet 0/1/6 interface.

```
l2vpn sdwan instance 200 multipoint

vlan 2001
 name L2MPvpn

interface Vlan2001
 service instance 200 ethernet
  encapsulation dot1q 2001
  no shutdown
  !
bridge-domain 200
 member Vlan2001 service-instance 200
 member sdwan-instance 200 vc-id 200 single-homing
```

# Configure Layer 2 VPN Switchport

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Control Components Release 20.14.1

If your device has embedded switchports such as Cisco ISR1121-8P or similar and you want to use one of them for the L2VPN services, then you need to configure a VLAN interface first and then assign that VLAN to your switchport as described in this section.

To support a Layer 2 switchport, configure a service instance in the VLAN interface. In the VLAN interface, a packet always has the dot1q tag even when the Layer 2 switchport is configured with switchport mode access. Therefore, the dot1q tag is mandatory in the service instance of the VLAN interface.

This following section provides steps to configure a Layer 2 switchport for P2MP (applicable for devices with embedded switchports). You can also configure a Layer 2 switchport for P2P by updating the L2VPN instance command.

### Configure an Edge Router at Sites A, B, and C

Site A is using an edge router, where the Ethernet interface is connected to the Layer 2 network that bridges to Site B and Site C.

1. Define the L2VPN instance for multipoint service on the branch routers:

```
l2vpn sdwan instance instance-id multipoint
```

2. Define the VLAN for the L2VPN on the branch routers:

```
vlan vlan-id
 name L2vpn
```

3. Configure the Ethernet interface on the routers:

```
interface interface-name
```

4. Set the switch port access VLAN and switchport mode to access to accept traffic only from the specified VLAN:

```
switchport access Vlan  vlan-id
switchport mode access
```

5. Configure the VLAN interface on the router and disable the IP address assignment:

```
interface interface-name
 no ip address
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
```

6. Define the bridge-domain on the data center router and associate it with the interface and L2VPN instance:

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id
 single homing
```

### Example

```
l2vpn sdwan instance 200 multipoint

interface GigabitEthernet0/1/2
 switchport access Vlan 201
 switchport mode access

interface Vlan201
 no ip address
 service instance 200 ethernet
  encapsulation dot1q 201
  !
```

```
bridge-domain 201
 member Vlan201 service-instance 200
 member sdwan-instance 200 vc-id 201 single-homing
```

# Advanced Layer 2 Configuration

Minimum software releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

For advanced Layer 2 configuration options such as 802.1Q tunneling (Q-in-Q), or rewrite, you need to configure Ethernet Virtual Connections (EVCs) on edge routers (Cisco ASR 1000 Series). EVC is a Layer 2 platform-independent bridging architecture that supports Ethernet services. For more information about configuring an EVC, see Configuring Ethernet Virtual Connections on a Cisco Router.

# Verify a Layer 2 VPN Using CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Control Components Release 20.14.1

### Show L2VPN Status

The following command shows the details of a specific local instance.

```
show l2vpn sdwan [instance instance-id] [vc-id vc-id]
```

The following command shows the remote peer information, system ip, color, status, and so on.

```
show l2vpn sdwan instance [instance  instance-id] [vc-id vc-id] peers
```

The following is a sample output from the **show l2vpn sdwan** command displaying information about the L2VPN connection.

```
Device#show l2vpn sdwan instance 13 vc-id 13
VC_ID: 13 Bridge-domain: 13
Local l2vpn status: UP
Local Pseudoports: GigabitEthernet7 service instance 13
```

### Show L2VPN Information in OMP on a Cisco IOS XE Catalyst SD-WAN Device

The following command shows Layer 2 routes learned through OMP from all VPNs across the Cisco Catalyst SD-WAN fabric.

```
show sdwan omp l2-routes
```

The following command shows specific L2-routes learned in that VPN ID tied to the L2 instance on the Cisco IOS XE Catalyst SD-WAN devices.

```
show sdwan omp l2-routes [vpn vpn-id]
```

The following command shows the specific L2-route or path learned in the specific VPN and virtual circuit.

```
show sdwan omp l2-routes [vpn vpn-id] [vc-id vc-id]
```

The following is a sample output from the **show omp l2-routes** command displaying Layer 2 routes learned through OMP from all VPNs across the Cisco Catalyst SD-WAN fabric.

```
Device#show sdwan omp l2-routes
Code:
vm5#show sdwan omp l2-routes
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                        REMOTE
                                    ROUTE                   IP                   SITE
               PATH                     SITE
VPN    VC ID        ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
-----------------------------------------------------------------------------------------
12     12           172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
0.0.0.0          66     1004     C,Red,R   501

0.0.0.0          69     1004     C,Red,R   501
12     12           172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.19    2      1014     C,I,R     500

172.16.255.20    1      1014     C,R       500
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
0.0.0.0          66     1006     C,Red,R   -

0.0.0.0          69     1006     C,Red,R   -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.19    2      1016     C,I,R     -

172.16.255.20    1      1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.19    1      1007     C,I,R     -

172.16.255.20    1      1007     C,R       -
15     1            172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
0.0.0.0          66     1020     C,Red,R   501

0.0.0.0          69     1020     C,Red,R   501
15     1            172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.19    2      1020     C,I,R     500

172.16.255.20    1      1020     C,R       500
```

### Show L2VPN Information in OMP on a Cisco Catalyst SD-WAN Controller

The following command shows Layer 2 routes learned through OMP from all VPNs across the Cisco Catalyst SD-WAN fabric.

```
show sdwan omp l2-routes
```

The following command shows specific L2-routes learned in that VPN ID tied to the L2 instance on the Cisco SD-WAN Controllers.

```
show sdwan omp l2-routes [vpn vpn-id]
```

The following command shows the specific L2-route or path learned in the specific VPN and virtual circuit.

```
show sdwan omp l2-routes [vpn vpn-id] [vc-id vc-id]
```

The following is a sample output from the **show omp l2-routes** command displaying Layer 2 routes learned through OMP for Cisco Catalyst SD-WAN Controllers.

```
Device#show omp l2-routes | tab
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
```

| VPN FROM PEER | VC ID | PATH ID | ORIGINATOR LABEL | ROUTE STATUS | REMOTE SITE MAC ADDRESS ID | IP ADDRESS | VPN TYPE | SITE ID |
|---|---|---|---|---|---|---|---|---|
| 12 | 12 | | 172.16.255.15 | vpn | 0000.0000.0000 | :: | p2p | 500 |
| 172.16.255.15 | | 66 | 1004 | C,R | 501 | | | |
| 172.16.255.15 | | 69 | 1004 | C,R | 501 | | | |
| 172.16.255.20 | | 1 | 1004 | C,R | 501 | | | |
| 172.16.255.20 | | 2 | 1004 | C,R | 501 | | | |
| 12 | 12 | | 172.16.255.27 | vpn | 0000.0000.0000 | :: | p2p | 501 |
| 172.16.255.20 | | 1 | 1014 | C,R | 500 | | | |
| 172.16.255.27 | | 70 | 1014 | C,R | 500 | | | |
| 13 | 13 | | 172.16.255.15 | vpn | 0000.0000.0000 | :: | multipoint | 500 |
| 172.16.255.15 | | 66 | 1006 | C,R | - | | | |
| 172.16.255.15 | | 69 | 1006 | C,R | - | | | |
| 172.16.255.20 | | 1 | 1006 | C,R | - | | | |
| 172.16.255.20 | | 2 | 1006 | C,R | - | | | |
| 13 | 13 | | 172.16.255.27 | vpn | 0000.0000.0000 | :: | multipoint | 501 |
| 172.16.255.20 | | 1 | 1016 | C,R | - | | | |
| 172.16.255.27 | | 70 | 1016 | C,R | - | | | |
| 13 | 13 | | 172.16.255.32 | vpn | 0000.0000.0000 | :: | multipoint | 503 |
| 172.16.255.20 | | 1 | 1007 | C,R | - | | | |
| 172.16.255.32 | | 71 | 1007 | C,R | - | | | |

```
14     1            172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1018     C,R       -

172.16.255.27    70     1018     C,R       -
15     1            172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1020     C,R       501

172.16.255.15    69     1020     C,R       501

172.16.255.20    1      1020     C,R       501

172.16.255.20    2      1020     C,R       501
15     1            172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1020     C,R       500

172.16.255.27    70     1020     C,R       500
```

### Show Bridge-Domain Information

The following is a sample output from the **show platform software sdwan ftmd bridge-domain** command that displays information related to bridge domains within the context of Forwarding Table Management Daemon (FTMD).

```
Device#show platform software sdwan ftmd bridge-domain
L2vpn Bridge-domain 12 Table:
  sdwan efp dpidx: 4210708(0x404014)
  Label: 1004 lbl-nhop-id: 196611 (binosId=0xf830003f)
  Bum Label: 1005 bum-lbl-nhop-id: 196612 (binosId=0xf830004f)
  Remote Site Table(1 entries in total):
    remote-site-id: 501 sla-nhop-id: 29 (binosId=0xf80001df)

L2vpn Bridge-domain 13 Table:
  sdwan efp dpidx: 4210709(0x404015)
  Label: 1006 lbl-nhop-id: 196613 (binosId=0xf830005f)
  Bum Label: 1007 bum-lbl-nhop-id: 196614 (binosId=0xf830006f)
  Remote Site Table(2 entries in total):
    remote-site-id: 501 sla-nhop-id: 30 (binosId=0xf80001ef)
remote-site-id: 503 sla-nhop-id: 33 (binosId=0xf800021f)
```

### Show Cisco Catalyst SD-WAN Flood List Information and Packet Counters in Data Plane

The following is a sample output from the **show platform hardware qfp active feature bridge-domain datapath** *bridge-domain-id* **sdwan-flood-list** command that displays the Cisco Catalyst SD-WAN flood list information.

```
Device#show platform hardware qfp active feature bridge-domain datapath 13 sdwan-flood-list

l2vpn:13 sdwan-olist:0xe0d36d80

Flood List for Bridge Domain 13:
 SDWAN oce_base:0xe1961a40 intf:SFI13.13.4210709 flags:
 SDWAN oce_base:0xe1961680 intf:SFI13.13.4210709 flags:
```

### Show Packet Counters in Data Plane

The following is a sample output from the **show platform hardware qfp active feature bridge-domain datapath** *bridge-id* command to display a QFP hardware module packet counters for a specific bridge domain within the data path.

```
Device#show platform hardware qfp active feature bridge-domain datapath 200
QFP L2BD Bridge Domain information
```

```
BD id                  : 200

State enabled          : Yes

Aging timeout (sec)    : 300

Aging active entry     : Yes

Max mac limit          : 65536

Unkwn mac limit flood  : Yes

mac_learn_enabled      : Yes

mac_learn_controled    : No

Unknown unicast olist  : Yes

otv_aed_enabled : No

otv_enabled : No

mcast_snooping_enabled : No

Feature : sdwan

SISF snoop protocols   : None

Sdwan instance id      : 200

Mac learned            : 0

BDI outer vtag         : 00000000

BDI inner vtag         : 00000000


Replication tree info:

  Global replication    : depth encode 0X1000001, (head 0XE4E90000)

  Split-horizon-group 0 : depth encode 00000000, (head 00000000)

  Split-horizon-group 1 : depth encode 00000000, (head 00000000)
Bridge Domain statistics


Total bridged               pkts : 0          bytes: 0

Total unknown unicast       pkts : 0          bytes: 0

Total broadcasted           pkts : 0          bytes: 0

Total to BDI                pkts : 0          bytes: 0

Total injected              pkts : 0          bytes: 0

Total mac-sec violation drop pkts : 0         bytes: 0
```

```
Total mac-sec move drop      pkts : 0          bytes: 0

Total mac-sec unknown drop   pkts : 0          bytes: 0

Total source filter drop     pkts : 0          bytes: 0

Total bfib policy drop       pkts : 0          bytes: 0

Total replication start drop pkts : 0          bytes: 0

Total recycle tail drop      pkts : 0          bytes: 0

Total static MAC move drop   pkts : 0          bytes: 0

Total BD disabled drop       pkts : 0          bytes: 0

Total STP state drop         pkts : 0          bytes: 0

Total UUF suppression drop   pkts : 0          bytes: 0

Total sisf ctrl punt         pkts : 0          bytes: 0

Total sisf ctrl drop         pkts : 0          bytes: 0

Total p2p lan to wan         pkts : 0          bytes: 0

Total p2p wan to lan         pkts : 0          bytes: 0
```

# Monitor Configured Layer 2 VPN Using CLI

The following is a sample output from the **show l2vpn sdwan all** command. The following examples show the configuration and status information for L2VPN instances within a Cisco Catalyst SD-WAN overlay network. The output includes details for both point-to-point (P2P) and point-to-multipoint (P2MP) topologies.

Example 1

```
Device#show l2vpn sdwan all
L2VPN sdwan Instance : 100
VPN Type : point-to-point
  VC_ID: 100 Bridge-domain: 100 UP
    Local l2vpn status: UP
    Local Pseudoports: GigabitEthernet5 service instance 100
    Remote Site: 53
      System IP          status       up/down    color           encap    label  DF
      10.100.31.53       DOWN         00:15:04   public-internet ipsec    1023   N/A
```

Example 2

```
Device#show l2vpn sdwan all
L2VPN sdwan Instance : 200
VPN Type : multipoint
IP Local-learning    : Disabled
Flooding Suppression : Disabled
  VC_ID: 200 Bridge-domain: 200 UP
    Local l2vpn status: UP
    Local Pseudoports: GigabitEthernet5 service instance 200
    Remote Site: 50
      System IP          status       up/down    color           encap    label  DF
      10.100.31.50       UP           00:04:14   public-internet ipsec    1008   N/A
```

```
    Remote Site: 53
      System IP          status       up/down    color           encap    label  DF
      10.100.31.53       UP           00:15:00   public-internet ipsec    1025   N/A
```

The following is a sample output from the **show l2vpn sdwan instance** *instance-id* **vc-id** *vc-id***peers** command. The following examples show information about a specific Cisco Catalyst SD-WAN L2VPN instance (instance 200) and its associated virtual circuit (vc-id 200), including details about its peer connections.

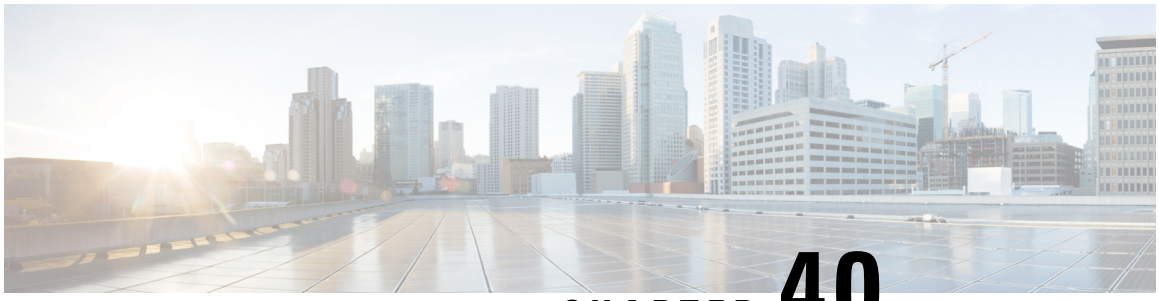
`show l2vpn sdwan` **`instance`** *`instance-id`* **`vc-id`** *`vc-id`* **`peers`**

Example 1

```
Device1#show l2vpn sdwan instance 200 vc-id 200 peers
    Remote Site: 50   MACs Learn: 0
      System IP          status       up/down    color           encap    label  DF
      10.100.31.50       UP           00:19:54   public-internet ipsec    1008   N/A

    Remote Site: 53   MACs Learn: 0
      System IP          status       up/down    color           encap    label  DF
      10.100.31.53       UP           00:30:40   public-internet ipsec    1025   N/A
```

Example 2

```
Device#show l2vpn sdwan instance 200 vc-id 200 peers
     Remote Site: 1   MACs Learn: 0
      System IP          status       up/down    color           encap    label  DF
      10.100.31.1        UP           00:30:13   public-internet ipsec    1014   N/A
```



CHAPTER 40

# Troubleshoot Cisco Catalyst SD-WAN Systems and Interfaces


- Overview, on page 1093
- Support Articles, on page 1093
- Feedback Request, on page 1095
- Disclaimer and Caution, on page 1095


## Overview

This chapter provides links to documents authored by Cisco subject matter experts (SMEs). They aim to help you resolve technical issues without requiring a support ticket. If these documents are unable to resolve your issue, we recommend visiting the applicable Cisco Community. There is a wealth of information and advice available from fellow Cisco customers who may have experienced this issue already and provided a solution. If you are not able to find a resolution on the Community, it may be best that you raise a support ticket at Cisco Support. In cases where a support ticket has to be raised, these documents provide guidance about the data that should be collected and added to the support ticket. Specify the support document you referred, and TAC can create an improvement request with the document owner.

## Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following are the support articles associated with this technology:

| Document | Description |
|---|---|
| Collect an Admin-Tech in SDWAN Environment and Upload to TAC Case | This document describes how to initiate an `admin-tech` in an SD-WAN environment. |

| Document | Description |
|---|---|
| Configure a Custom Cisco SD-WAN Manager Application Server Logo | This document describes the process to modify Cisco Catalyst SD-WAN Manager application server logo images. The change is made from the Cisco Catalyst SD-WAN Manager CLI. |
| Configure and Troubleshoot a DHCP Server on Cisco IOS XE SDWAN Router | This document describes how to configure and troubleshoot a DHCP Server on a Cisco SD-WAN IOS XE Router. |
| Configure and Verify SD-WAN On-demand Tunnels | This document describes configuration and verification steps to create SD-WAN On-demand Tunnels. |
| Configure Banner Feature Templates with Special Characters | This document describes the use of banner feature templates for the generation of banner and message of the day (MOTD) text blocks in Cisco IOS XE. |
| Configure Basic Parameters to Form Control Connections on cEdge | This document describes the basic configuration and correct commit order to onboard a Cisco IOS XE Catalyst SD-WAN device to a Cisco Catalyst SD-WAN overlay. |
| Configure IPsec and GRE in the Same Tunnel Interface on XE SD-WAN | This document describes the configuration to enable IPsec and GRE encapsulation for the same tunnel interface on a Cisco IOS XE SD-WAN Router. |
| Configure L3 TLOC Extension | This video describes how to configure L3 TLOC Extension on SD-WAN. |
| Configure Layer 3 TLOC Extension | This document describes how to configure TLOC-Extension Layer 3(L3) on Cisco SD-WAN. |
| Configure SD-WAN Edge Router for Inline Deployment | This document describes how to configure Cisco SD-WAN Edge with MPLS transport to access Cisco SD-WAN Controller on Internet via inline DC WAN Edge. |
| Configure ThousandEyes on SD-WAN Devices | This video provides the procedure to configure ThousandEyes on SD-WAN Devices. |
| Configure Thousand Eyes on SD-WAN Devices | This document describes how to integrate ThousandEyes Endpoint Agent on Cisco Catalyst SD-WAN. |
| Configure Host Entry for Cisco SD-WAN Validator | This document describes the procedure to configure host entry for Cisco Catalyst SD-WAN Validator. |
| Configure TLOC-Extension Using Cisco SD-WAN Manager Feature Template | This document describes how to configure TLOC-Extension using Cisco SD-WAN Manager feature template. |
| Create a Cisco SD-WAN Controller CLI Template to Push a Centralized Policy | This document describes an easy way to create a CLI Template for Cisco Catalyst SD-WAN Controlleras they are needed to push a Centralized Policy for the overlay. |
| Perform Password Recovery with a Template on SD-WAN | This document describes the steps for password recovery of a device with a template in Cisco Catalyst SD-WAN environment. |

| Document | Description |
|---|---|
| Quick Start Guide - Data Collection for Various SD-WAN Issues | This document describes several Cisco Catalyst SD-WAN issues along relevant data that must be collected in advance before you open a TAC case to improve the speed of troubleshooting and/or problem resolution. |
| Troubleshoot SD-WAN Control Connections | This document describes some of the probable causes that lead to a problem with Control Connections and how to troubleshoot them. |
| Troubleshoot SD-WAN Dynamic On-Demand Tunnels | This document describes troubleshoot commands that can be used when configuring or checking an issue related to SD-WAN dynamic on-demand tunnels. |
| Troubleshoot "Unable to Validate Proxy Server" Error in Cisco SD-WAN Manager | This document describes the "Failed to update setting Invalid request. unable to validate proxy server" error in Cisco SD-WAN Manager and how to resolve it. |
| Understand NTP Association Codes in SD-WAN Controllers | This document describes how to understand NTP association status codes on SD-WAN controllers. |
| Verify and Identify Packet Loss in the WAN for SD-WAN | This document describes how to identify and collect data when traffic has loss across the WAN but no drops are seen on the SD-WAN Edge. |

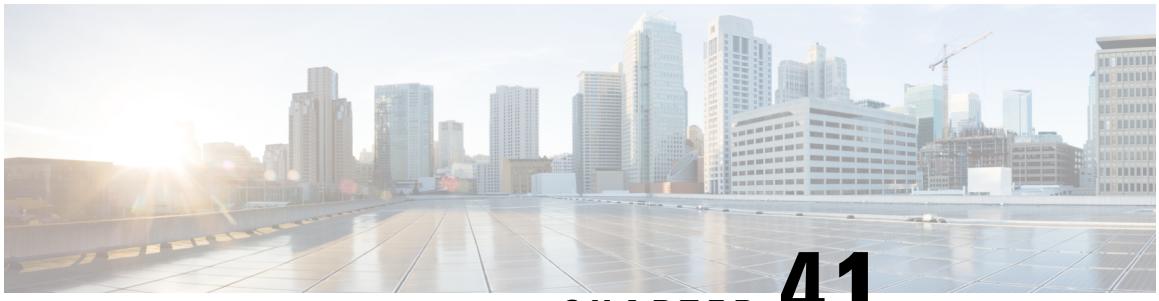
# Feedback Request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the **Feedback** button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

# Disclaimer and Caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



CHAPTER 41

# Appendix: Cisco SD-WAN Manager How-Tos


• How to Load a Custom Cisco SD-WAN Manager Application Server Logo, on page 1097


# How to Load a Custom Cisco SD-WAN Manager Application Server Logo

To change the Cisco SD-WAN Manager web application server logo and load a new custom logo, use the **request nms application-server update-logo** command.

The logo image is located in the upper left corner of all Cisco SD-WAN Manager web application server screens. You can load two files, a larger version, which is displayed on wider browser screens, and a smaller version, which is displayed when the screen size narrows. Both files must be PNG files located on the local device, and both must be 1 MB or smaller in size. For best resolution, it is recommended that the image for the large logo be 180 x 33 pixels, and for the small logo 30 x 33 pixels.