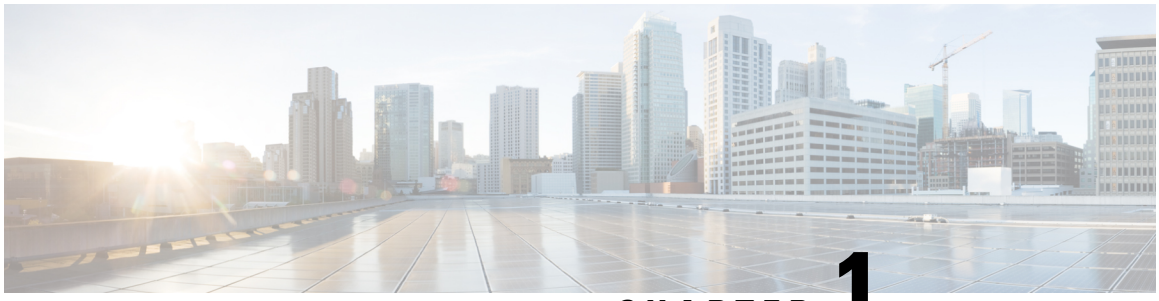
Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x

First Published: 2023-07-25

Last Modified: 2024-03-05

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

CONTENTS



CHAPTER 1

Introduction

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

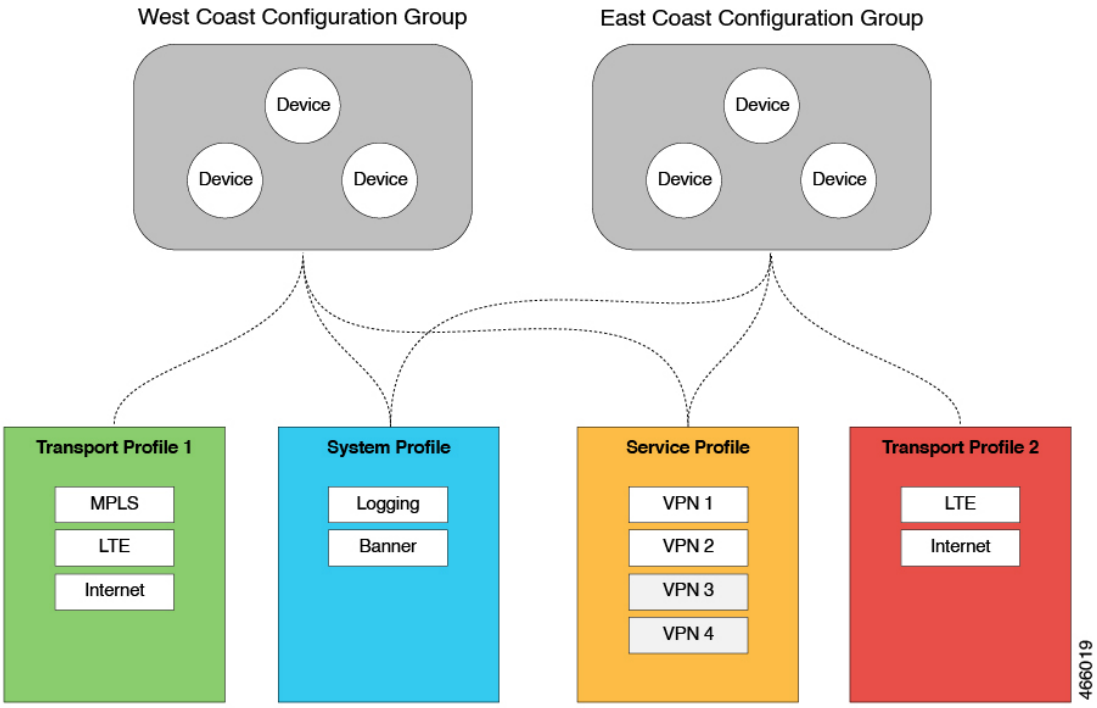
- You can associate a device to either a configuration group or a device template, but not both.
- You can add a device to only one configuration group.
- You can add only one tag rule to a configuration group.
- (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1) You can only 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



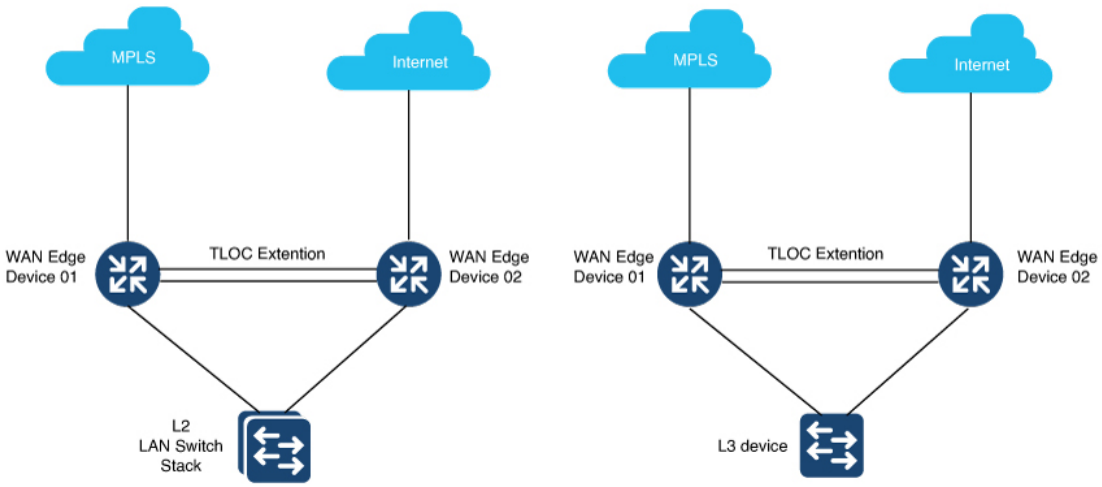
In this figure,

- 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

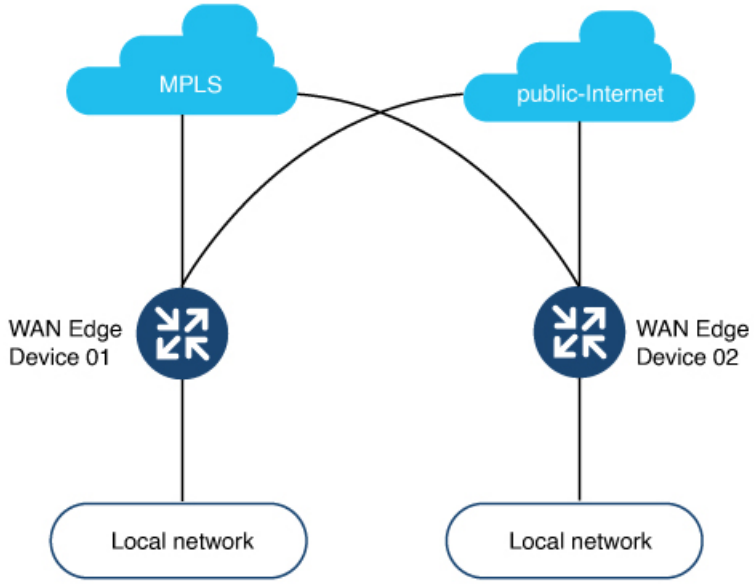
To deploy dual device site configuration, you can choose a TLOC extension or a full mesh topology in the dual router type configuration group workflow. Use of TLOC extensions is recommended for failure scenarios and redundancy.

Figure 2: TLOC Extension Topology

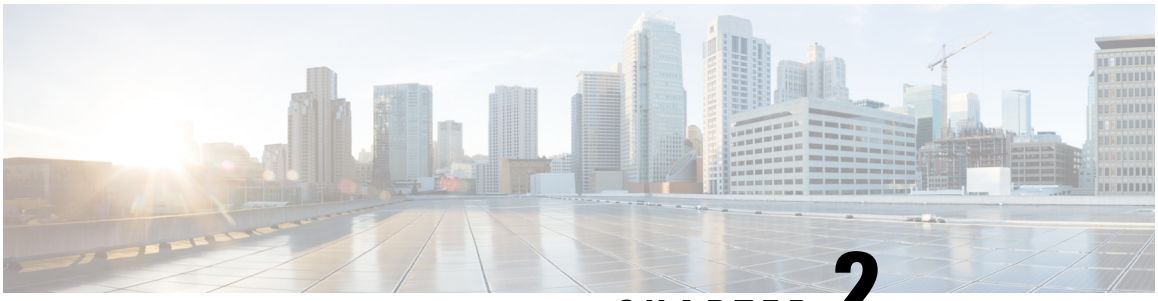


When you use a TLOC extension, there's a transport extension between the two devices. One end acts like a tunnel interface and the other end acts like a TLOC interface. By default, there's a single uplink to the public interface for each of the device. One device has an uplink to MPLS and the other device 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.



CHAPTER 2

Using Configuration Groups

Use the Configuration Group Workflows

Before You Begin

Ensure that the IP address of the Cisco SD-WAN Validator is specified.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **vBond**.
2. Enter the IP address of the Cisco SD-WAN Validator.

Ensure that granular RBAC for each feature profile is specified by expanding it. With the set permissions to the usergroup, ensure that you are able to access required feature profiles from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.
2. Click **Add User Group**.
3. Enter **User Group Name**.
4. Select the **Read** or **Write** check box against feature that you want to assign to a user group.
5. Click **Save**.

Note To create Service, System and Tranport feature profiles using configuration groups, you need to provide read and write permissions on the following features to access each configuration group.

- **Feature Profile** > **System**
- **Feature Profile** > **System** > **AAA**
- **Feature Profile** > **System** > **BFD**
- **Feature Profile** > **System** > **Banner**
- **Feature Profile** > **System** > **Basic**
- **Feature Profile** > **System** > **Logging**
- **Feature Profile** > **System** > **NTP**
- **Feature Profile** > **System** > **OMP**
- **Feature Profile** > **System** > **SNMP**
- **Feature Profile** > **Service**
- **Feature Profile** > **Service** > **BFD**
- **Feature Profile** > **Service** > **LAN/VPN**
- **Feature Profile** > **Service** > **LAN/VPN/Interface/Ethernet**
- **Feature Profile** > **Service** > **Routing/BGP**
- **Feature Profile** > **Service** > **Routing/OSPF**
- **Feature Profile** > **Service** > **Routing/DHCP**
- **Feature Profile** > **Service** > **Routing/Multicast**
- **Feature Profile** > **Transport**
- **Feature Profile** > **Transport** > **Routing/BGP**
- **Feature Profile** > **Transport** > **WAN/VPN**
- **Feature Profile** > **Transport** > **WAN/VPN/Interface/Ethernet**

For more details on adding user groups, see Create User Groups.

Run the Create Configuration Group Workflow

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

From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create Configuration Group**. Alternatively, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. On the **Workflow Library** page, 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**.

The workflow creates a configuration group, which includes various feature profiles.

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 1: 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 Devices

Any field in a feature can be marked as device-specific which is referred as device variable. You can provide device variable values while adding devices for deploying them for any features.

Deploy Devices Manually

1. From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, choose **Configuration** > **Configuration Groups** in the Cisco SD-WAN Manager menu.

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**.
4. Choose one or more devices, and then click **Deploy**.

Deploy Devices Using the Deploy Configuration Group Workflow

Before You Begin

Ensure that one or more configuration groups are created so that you can choose a group from the list to deploy the associated devices.

Note In Cisco vManage Release 20.8.x, the Deploy Configuration Group workflow is called the Provision WAN Sites and Devices workflow.

Deploy Devices

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Deploy Configuration Group** workflow.
3. Follow the instructions provided in the workflow.

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.
- Remove a Cisco Catalyst 8000V device from a configuration group only after deploying the device. Manually issue the command **request platform software sdwan** *is-vmanaged disable* in the device CLI to completely dissociate the Cisco Catalyst 8000V device from a configuration group.

Features and Subfeatures

The following procedures relate to adding, editing, and removing features and subfeatures from a feature profile within a configuration group.

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 Run the Create Configuration Group Workflow, on page 8.

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. 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. 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. 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**.

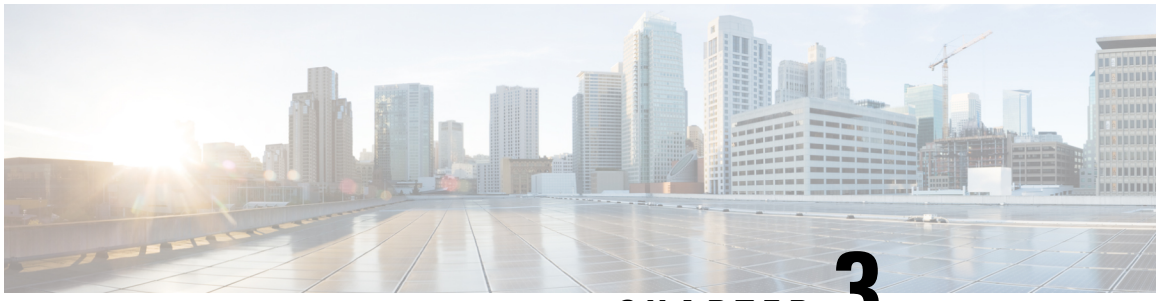
Delete a Feature

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**.

PART I

Part Cisco IOS XE Devices (SD-WAN)



CHAPTER 3

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	

Field	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. 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. Each username must have a password. Users are allowed to change their own passwords. 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.
Privilege	Select between privilege level 1 or 15. • Level 1: User EXEC mode. Read-only, and access to limited commands, such as the ping command. • 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. Range: 0 through 65535. Default: 1813

Field	Description
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. Default: 1812
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 seconds
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS 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 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. Default: 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.

Accounting

Field	Description
Add Accounting Rule	
Rule Id*	Enter the accounting rule ID.

Field	Description
Method*	Specifies the accounting method list. Choose one of the following: • **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level. • **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**: Runs accounting for all network-related service requests. • **system**: Performs accounting for all system-level events not associated with users, such as reloads. **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.
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.

Field	Description
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. Range: 1 through 4,294,967,296 (2^{32} – 1) milliseconds 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. Range: 1 through 6 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. Range: 0-63 Default: 48

Color

Field	Description
Add Color	

Field	Description
Color*	Choose the color of the transport tunnel for data traffic moving between the devices. The color identifies a specific WAN transport provider. Values: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver 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. Range: 100 through 300000 milliseconds 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. Range: 1 through 60 Default: 7
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. 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. Range: 0-63 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.

Field	Description
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.
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. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps). Default: 9600
Overlay ID	Specifies the overlay ID of a device in the Cisco Catalyst SD-WAN overlay network. Range: 0 - 4294967295 ($2^{32} – 1$) 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. 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. 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. Default: Enabled
Track Interface Tag	Set the tag string to include in routes associated with a network that is connected to a non-operational interface. 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. 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. Values: 0 through 19
On Demand Tunnel	Enable dynamic on-demand tunnels between any two Cisco Catalyst SD-WAN spoke devices.

Field	Description
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. Range: 1 to 65535 minutes Default: 10 minutes
Control Session PPS	Enter a maximum rate of DTLS control session traffic to police the flow of control traffic. Range: 1 through 65535 pps 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. 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. Range: 10 through 1209600 seconds (14 days) 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. This option is turned off by default. Click **On** to enable it. Enabling the feature displays the **Extended Anti-Replay Window** field. Range: 10 ms to 2048 ms Default: 256 ms

Field	Description
Replay Window	Specify the size of the sliding replay window. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets. 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: • **esp**: Enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header. • **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. • **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. • **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.

Field	Description
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). A MAC is computed for a TCP segment using a configured MAC algorithm, relevant traffic keys, and the TCP segment data prefixed with a pseudoheader. When options are included, the content of all options is included in the MAC with TCP-AO's **MAC** field is filled with zeroes. 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. 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. Range: 0 through 255.
Send ID*	Specify the send identifier for the key. Range: 0 through 255.
TCP	Specify the algorithm to compute MACs for TCP segments. You can choose one of the following: • **aes-128-cmac** • **hmac-sha-1** • **hmac-sha-256**
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: • **Accept Local**: This option is disabled by default. Click **On** to enable it. • **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. • **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).

Field	Description
Send Lifetime	The following fields appear when you click this field: • **Send Local**: This option is disabled by default. Click **On** to enable it. • **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. • **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).

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. 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. 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. 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 Settings

Parameter Name	Description
Port Type	Choose from one of the following port combinations: • **12 ports of 1/10GE + 3 ports of 40GE** • **8 ports of 1/10GE + 4 ports of 40GE** • **2 ports of 100GE** • **12 ports of 1/10GE + 1 port of 100GE** • **8 ports of 1/10GE + 1 port of 40GE + 1 port of 100GE** • **3 ports of 40GE + 1 port of 100GE** Default is 12 ports of 1/10GE + 3 ports of 40GE.

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. Range: 1 to 536870 (seconds) Default: 300 seconds (5 minutes)
TCP Timeout	Specify the NAT64 translation timeout for TCP. Range: 1 to 536870 (seconds) Default: 3600 seconds (1 hour)

Authentication

Field	Description
HTTP Authentication	Choose the HTTP authentication mode. Accepted values: Local, AAA Default: Local

SSH Version

Field	Description
SSH Version	Choose the SSH version. 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.

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.

Field	Description
Action Type	Choose one of the following actions for the ACL policy: • **Accept** • **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. • **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12. • **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535. • **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: • **Accept** • **Drop**
Default Action	The **Default Action** in the left pane is to drop the packets. Change the default action by clicking the ellipsis (**...**) icon.

Field	Description
Condition	• **Device Access Protocol (required)**: Choose a carrier from the drop-down list. For example, SNMP, SSH. • **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12. • **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535. • **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.

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. Range: 1 to 20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the oldest files. Range: 1 to 10 Default: 10

TLS Profile

Field	Description
Add TLS Profile	
TLS Profile Name*	Enter the name of the TLS profile.

Field	Description
TLS Version	Choose a TLS version: • **TLSv1.1** • **TLSv1.2**
Authentication Type*	Choose **Server**.
Cipher Suite List	Choose groups of cipher suites (encryption algorithm) based on the TLS version. The following is the list of cipher suites. • **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 • **dhe-aes-cbc-sha2**: Encryption type tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **dhe-aes-gcm-sha2**: Encryption type tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 and above) • **ecdhe-ecdsa-aes-gcm-sha2**: Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 and above) SuiteB • **ecdhe-rsa-aes-cbc-sha2**: Encryption type tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 and above) • **ecdhe-rsa-aes-gcm-sha2**: Encryption type tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 and above) • **rsa-aes-cbc-sha2**: Encryption type tls_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **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. 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. 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: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **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: **TLS Properties Custom Profile**: Enable this option to choose a TLS profile. When you enable this option, the following field appears: **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. 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. 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.

Field	Description
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: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **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 ability 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 (called access regions) and connect to each other. Each border router serves a single access region. Configure each border router with the "border-router" role and with the number of the access region that the border router serves.
- One or more regional overlay networks, called access regions: Each access region 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. Configure each edge router with the "edge-router" role and an access region number.

Basic Settings

Parameter Name	Description
Region	Beginning with Cisco Catalyst SD-WAN Manager Release 20.13.1, this field has been removed. Set the region in the deployment phase. • Border routers: Configure the access region for the border router to serve. • Edge routers: Configure the access region for the edge router. Range: 1 to 63
Role	• Border routers: Use **border-router**. • Edge routers: Use **edge-router**.
Secondary Region ID	Secondary regions provide another layer to the Multi-Region Fabric architecture. A secondary region contains only edge routers and enables 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. Range: 1 to 63
Enable Migration Mode to Multi-Region Fabric	Beginning with Cisco Catalyst SD-WAN Manager Release 20.13.1, this field has moved to the **Advanced** tab. Use this parameter when migrating devices from a non-Multi-Region Fabric architecture to Multi-Region Fabric. To prepare for migration, do the following: • Use the **enabled** option for devices that will function as edge routers after migration. • Use the **enabled-from-bgp-core** option for Cisco Catalyst SD-WAN gateway routers that will function as border routers after migration.

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.

Field	Description
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. Range: 0 to 65530
Set authentication key for the server	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. 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. Range: 1 to 4 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. 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. When you enable this option, the following field appears: **Stratum**: Enter the stratum value for the primary NTP router. The stratum value defines the hierarchical distance of the router from its reference clock. 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. 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 advertises routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistribute the learned routes, advertising each route-TLOC tuple. A 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 s, 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. Range: 1 through 16 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 installs a maximum of four unique OMP paths into its route table. Range: 1 through 16 Default: 4

Field	Description
Advertisement Interval (In Second)	Specify the time between OMP update packets. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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. Range: 1 through 3600 seconds (1 hour) 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.
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.

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. Range: 0 through 604800 seconds (168 hours, or 7 days) 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.

Field	Description
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.

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. 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. Click the toggle button to enable the continuous monitoring option in UMTS.
Monitoring Interval (Minutes)	In the **Monitoring Interval (Minutes)** field, choose a time. 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: • **SLA Change**: Change in the service-level agreement (SLA) parameter for the tunnel. • **PMTU Change**: Change in the Path MTU (PMTU) parameter for the tunnel.

To save the configuration, click **Save**.

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.

Field	Description
Connection Type	Choose the connection type from the following: • **IPsec** • **SSL-VPN** 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. 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. Click **Add Radius Group** to add a RADIUS server and group to the AAA feature profile in the System Profile.

Field	Description
Pre-Shared Key (PSK) Authentication	Enable Pre-Shared Key (PSK) authentication. • **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. • **Groups PSK**: Choose this option to configure a common pre-shared key for all remote access clients connecting to a device. **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. 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. **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. 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. 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. 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. **Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN.

Field	Description
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. **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: • IPv4 Address or IPv6 Address • Email • FQDN • 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. 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.
Anti-DOS Threshold	Enter the Anti-DOS threshold value. Range: 10 to 1000. Default: 100.

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.

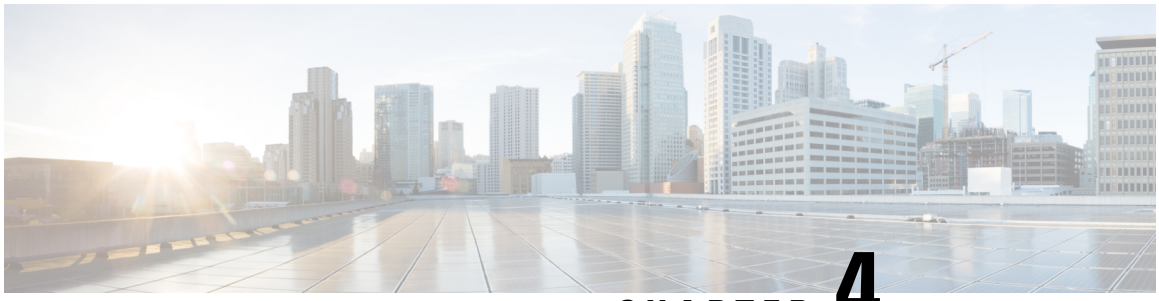
SNMP Version

Field	Description
SNMP Version	Choose one of the following SNMP versions: • **SNMP v2** • **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: • **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. • **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. 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. Range: 1 though 65535
Community Name*	Choose the name of a community that was configured under **Add Community**. 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: • **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. • **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. • **no-auth-no-priv**: Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials. **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. **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: • **md5** • **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. • **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. • **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. 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. 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.



CHAPTER 4

Transport and Management

ACL IPv4

1. In the **Add Feature** window, 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** window 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 rule's name 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 describe the options for configuring the ACL IPv4 feature.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Condition	Specifies the ACL condition. The options are: • DSCP • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Peer
Action Type	Specifies the action type. The options are: Accept or Reject.

Field	Description
Accept Condition	Specifies the accept condition type. The options are: • Counter • DSCP • Log • Next Hop • Mirror List • Class • Policer

You can select the specific ACL sequence in the ACL Policy window to edit, delete or add.

Note You can also configure **ACL Policy** features from Transport and Service Profile configuration groups.

ACL IPv6

1. In the **Add Feature** window, 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** window 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 rule's name 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 describe the options for configuring the ACL IPv6 feature.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Condition	Specifies the ACL condition. The options are: • Next Header • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Traffic Class
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • Counter • Log • Next Hop • Traffic Class • Mirror List • Class • Policer

You can select the specific ACL sequence in the ACL Policy window to edit, delete or add.

Note You can also configure **ACL Policy** features from Transport and Service Profile configuration groups.

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.
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. Range: 1 through 255 Default: 20
Internal Routes Distance	Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another. Range: 1 through 255 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. Range: 1 through 255 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. 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	

Field	Description
Protocol*	Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, **eigrp**, and **nat**. 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. 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. 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 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. 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. 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. Range: 0 to 32

Field	Description
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**. 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. 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. 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. 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. 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.
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. Range: 1 to 255 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.

Field	Description
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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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. 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. Route policy is not supported in Cisco vManage Release 20.9.1.

Field	Description
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **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. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **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. • **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. Range: 1 to 255 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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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. 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. Route policy is not supported in Cisco vManage Release 20.9.1.

Field	Description
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **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. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **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. • **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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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.

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.
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. Range: 0 through 65535 Default: 10

Field	Description
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. Range: 3 to 7 minutes 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. Range: 1 through 15
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.

Field	Description
No Overwrite	Enable this option to overwrite the profile on the cellular modem. By default, this option is disabled.

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: • **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. • **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.

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 2: 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: • **ipv6-interface** **Note** This tracker type is available only in Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier. • **http** • **icmp** This tracker type is available from Cisco Catalyst SD-WAN Manager Release 20.13.1.
Endpoint	Choose an endpoint type: • **Endpoint DNS Name**: When you choose this option, the following field appears: **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. • **Endpoint IP**: When you choose this option, the following field appears: **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. • **Endpoint API URL**: When you choose this option, the following field appears: **API url of endpoint**: API URL of the endpoint. The API URL can be a valid URL as described by RFC 3986.

Field	Description
Interval	Time interval between probes to determine the status of the configured endpoint. 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. Range: 20 to 600 seconds Default: 60 seconds (1 minute) 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. Range: 1 to 10 Default: 3
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds

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 3: 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.

Field	Description
Tracker Boolean	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**. **OR** is the default boolean operation. An **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the interface is active. If you select the **AND** operation, the transport-interface status is reported as active if both the associated trackers of the tracker group, report that the interface is active.

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.
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	

Field	Description
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:
	• **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **Address***: Enter the next-hop IPv4 address.
	  • **Administrative distance***: Enter the administrative distance for the route.
	• **dhcp**
	• **null0**: When you choose this option, the following field appears:
	  • **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: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **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. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT**: Choose NAT64 or NAT66.

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. 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. 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. 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.

Field	Description
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. Default: <Device specific IPv4 system_ip >
Distance for External Routes	Specify the OSPF route administration distance for routes learned from other domains. Range: 1 through 255 Default: 110
Distance for Inter-Area Routes	Specify the OSPF route administration distance for routes coming from one area into another. Range: 1 through 255 Default: 110
Distance for Intra-Area Routes	Specify the OSPF route administration distance for routes within an area. Range: 0 through 255 Default: 110

Redistribute

Field	Description
Add Redistribute	
Protocol	Choose the protocol from which to redistribute routes into OSPF. • **Static** • **Connected** • **BGP** • **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	
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. Choose a type: • **administrative**: Force the maximum metric to take effect immediately, through operator intervention. • **on-startup**: Advertise the maximum metric for the specified time. **Note** You can configure a maximum of one router LSA.

Area

Field	Description
Add Area	
Area Number*	Enter the number of the OSPF area. Allowed value: Any 32-bit integer
Set the area type	Choose the type of OSPF area: • **Stub** • **NSSA** **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. Range: 1 through 65535 seconds 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. Range: 1 through 65535 seconds 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. Range: 1 through 65535 seconds Default: 5 seconds
Interface Cost	Specify the cost of the OSPF interface. 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. Range: 0 through 255 Default: 1
OSPF Network Type	Choose the OSPF network type to which the interface is to connect: • **Broadcast network** • **Point-to-point network** • **Non-broadcast network** • **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. Default: Disabled
Authentication Type	Specify the key ID and authentication key if you use message digest (MD5): • **Message Digest Key ID**: Enter the key ID for message digest (MD5 authentication). The input value must be an integer. Range: 1 through 255 • **Message Digest Key**: Enter the MD5 authentication key. 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. 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. Range: 1 through 4294967 Mbps 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: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **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. Range: 1 through 600000 ms (600 seconds) Default: 200 ms
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 10000 ms (10 seconds)
Select Route Policy	Enter the name of a localized control policy to apply to routes coming from OSPF neighbors.

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. • **Connected** • **Static** • **Nat-route** • **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. Allowed value: Any 32-bit integer
Area Type	Choose the type of OSPFv3 area: • **Stub** - no external routes • **NSSA**: not-so-stubby area, allows external routes • **Normal** **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. Range: 0 through 16777215
Authentication Type	Specify the SPI and authentication key if you use IPSec SHA1. • **no-auth**: Select no authentication. • **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.
SPI	Specifies the Security Policy Index (SPI) value. 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. 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. 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. Range: 1 through 4294967 Mbps 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: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **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. Default: 100
Distance for External Routes	Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110
Distance for Inter-Area Routes	Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110
Distance for Intra-Area Routes	Set the distance for routes within an area. Range: 0 through 255 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. Range: 1 through 600000 ms (600 seconds) Default: 200 ms

Field	Description
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) 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. • **Immediately**: Force the maximum metric to take effect immediately, through operator intervention. • **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 5 through 86400 seconds 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. 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. • **Connected** • **Static** • **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. Allowed value: Any 32-bit integer
Area Type	Choose the type of OSPFv3 area: • **Stub**: No external routes • **NSSA**: Not-so-stubby area, allows external routes • **Normal** **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. Range: 0 through 16777215
Authentication Type	Specify the SPI and authentication key if you use IPSec SHA1. • **no-auth**: Select no authentication. • **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. 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. 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. 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. Range: 1 through 4294967 Mbps 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: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **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. Default: 100
Distance for External Routes	Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110
Distance for Inter-Area Routes	Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110
Distance for Intra-Area Routes	Set the distance for routes within an area. Range: 0 through 255 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. Range: 1 through 600000 ms (600 seconds) Default: 200 ms
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) 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. • **Immediately**: Force the maximum metric to take effect immediately, through operator intervention. • **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 5 through 86400 seconds 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: • **Address** • **AS Path List** • **Community List** • **Extended Community List** • **BGP Local Preference** • **Metric** • **Next Hop** • **OMP Tag** • **OSPF Tag**
Action Type	Specifies the action type. The options are **Accept** or **Reject**.

Field	Description
Accept Condition	Specifies the accept condition type. The options are: • **AS Path** • **Community** • **Local Preference** • **Metric** • **Metric Type** • **Next Hop** • **OMP Tag** • **Origin** • **OSPF Tag** • **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: • **esf**: Send T1 frames as extended superframes. This is the default. • **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: • **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • **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 • **short**: Set the transmission attenuation for cables that are 660 feet or shorter. • **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. There is no default length.
Clock Source	Select the clock source: • **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. • **internal**: Use the controller framer as the primary clock. • **loop-timed**: • **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: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do not use CRC4.
Line Code	Choose the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **hdb3**: Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Choose the clock source: • **internal**: Use the controller framer as the primary clock. • **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. • **Channel Group**: Enter a value for the channel group. Range: 0 through 30 • **Time Slot**: Type a value for the timeslot. Range: 0 through 31

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: • **http**

Field	Description
Endpoint	Choose an endpoint type: • **Endpoint IP**: When you choose this option, the following field appears: **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. • **Endpoint DNS Name**: When you choose this option, the following field appears: **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. • **Endpoint API URL**: When you choose this option, the following field appears: **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. Range: 20 to 600 seconds Default: 60 seconds (1 minute).
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range: 1 to 10 Default: 3
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds

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**. **OR** is the default boolean operation. An **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the interface is active. If you select the **AND** operation, the transport-interface status is reported as active if both the associated trackers of the tracker group report that the interface is active.

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. 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.
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IP address of the primary IPv6 DNS server in this VPN.

Field	Description
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:
	• **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **Address***: Enter the next-hop IPv4 address.
	  • **Administrative distance***: Enter the administrative distance for the route.
	• **dhcp**
	• **null0**: When you choose this option, the following field appears:
	  • **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.

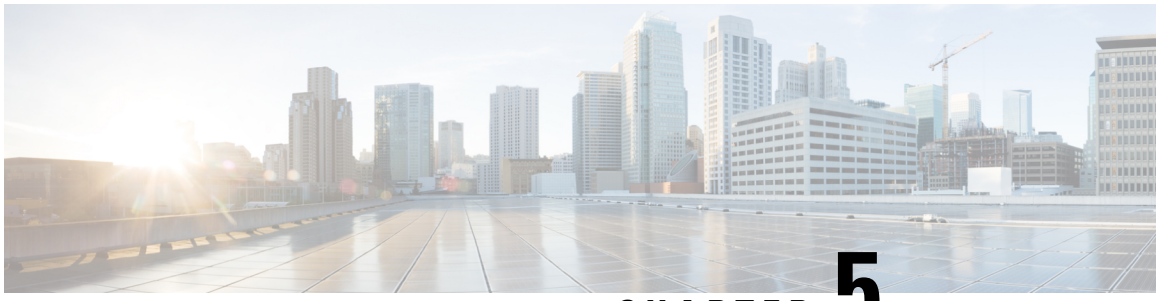
Field	Description
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **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. • **NAT**: When you choose this option, the following field appears: • **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. Default: Disabled

Service

Field	Description
Add Service	
Service Type	Choose the service available in the VPN. Value: **TE**



CHAPTER 5

Service Profile

ACL IPv4

1. In the **Add Feature** window, 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** window 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 rule's name 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 describe the options for configuring the ACL IPv4 feature.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Condition	Specifies the ACL condition. The options are: • DSCP • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Peer
Action Type	Specifies the action type. The options are: Accept or Reject.

Field	Description
Accept Condition	Specifies the accept condition type. The options are: • Counter • DSCP • Log • Next Hop • Mirror List • Class • Policer

You can select the specific ACL sequence in the ACL Policy window to edit, delete or add.

Note You can also configure **ACL Policy** features from Transport and Service Profile configuration groups.

ACL IPv6

1. In the **Add Feature** window, 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** window 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 rule's name 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 describe the options for configuring the ACL IPv6 feature.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Condition	Specifies the ACL condition. The options are: • Next Header • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Traffic Class
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • Counter • Log • Next Hop • Traffic Class • Mirror List • Class • Policer

You can select the specific ACL sequence in the ACL Policy window to edit, delete or add.

Note You can also configure **ACL Policy** features from Transport and Service Profile 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. **Note** **Service Node** is the default option. 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.
	• **Forwarder IP Address***: IP address of the device you've configured as a forwarder.
	• **AppQoE Service VPN***: Choose the service VPN attached to the interface of the forwarder.
	• **Service Node Group**: Click **Add Service Node Group** and enter the following details for the service node group:
	  • **Group Name**: Select the AppQoe group name.
	  • **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.
	  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.

BGP Routing

Use the Border Gateway Protocol (BGP) feature for service-side routing to provide reachability to networks at the local site.

Table 4: 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.
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. Range: 1 through 255 Default: 20
Internal Routes Distance	Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another. Range: 1 through 255 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. Range: 1 through 255 Default: 20

Table 5: 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. 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**. At a minimum, choose **omp**. By default, OMP routes are not redistributed into BGP.

Field	Description
Route Policy	Enter the name of the route policy to apply to redistributed routes. 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 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. 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. 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. 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**. At a minimum, choose **omp**. By default, OMP routes are not redistributed into BGP.

Field	Description
Route Policy	Enter the name of the route policy to apply to redistributed routes. 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. 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. 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 6: 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.

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. Range: 1 to 255 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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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.

Field	Description
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. 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. Route policy is not supported in Cisco vManage Release 20.9.1.
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **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. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **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. • **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.

Field	Description
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.
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. Range: 1 to 255 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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive time)
Add IPv6 Neighbor Address Family	

Field	Description
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. 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. Route policy is not supported in Cisco vManage Release 20.9.1.
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **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. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **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. • **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.

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.
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. Range: 1 through 255 Default: 20
Internal Routes Distance	Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another. Range: 1 through 255 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. Range: 1 through 255 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. 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	

Field	Description
Protocol*	Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, **eigrp**, and **nat**. 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. 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. 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 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. 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. 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. Range: 0 to 32

Field	Description
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**. 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. 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. 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. 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. 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.
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. Range: 1 to 255 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.

Field	Description
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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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. 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. Route policy is not supported in Cisco vManage Release 20.9.1.

Field	Description
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **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. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **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. • **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. Range: 1 to 255 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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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. 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. Route policy is not supported in Cisco vManage Release 20.9.1.

Field	Description
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **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. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **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. • **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. Range: 0 through 65535 seconds 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. Range: 0 through 65535 seconds 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.

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. Range: 60 through 31536000 seconds Default: 86400

Static Lease

Field	Description
Add Static Lease	

Field	Description
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. Range: 1-254
Type	Choose one of the three types: • **ASCII**: Specify an ASCII value. • **Hex**: Specify a hex value. • **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. 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.

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. Range: 1 through 65535 Default: None
Network	
IP Address*	Enter the IPv4 address.
Mask*	Enter the subnet mask.
Interface	
Add Interface	Provide values for the following fields: • **AF Interface**: Enter a value for the Address Family (AF) interface. • **Shutdown**: Enables the interface to run EIGRP by default. Toggle ON to disable the interface. • **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: • **bgp**: Redistribute Border Gateway Protocol (BGP) routes into EIGRP. • **connected**: Redistribute connected routes into EIGRP. • **nat-route**: Redistribute network address translation (NAT) routes into EIGRP. • **omp**: Redistribute Overlay Management Protocol (OMP) routes into EIGRP. • **ospf**: Redistribute Open Shortest Path First (OSPF) routes into EIGRP. **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: `redistribute ospf 1 metric 1000000 1 1 1 1500` For more information, see CLI Add-on Feature Templates. • **ospfv3**: OSPFv3 routes into EIGRP. • **static**: Redistribute static routes into EIGRP.

Parameter Name	Description
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. Range: 0 through 65535 Default: 15 seconds
Hello Interval (seconds)	Set the interval at which the router sends EIGRP hello packets. Range: 0 through 65535 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.

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. Range: 1 through 65535 Default: None
Network	
IP Address*	Enter the IPv4 address.
Mask*	Enter the subnet mask.
Interface	
Add Interface	Provide values for the following fields: • **AF Interface**: Enter a value for the Address Family (AF) interface. • **Shutdown**: Enables the interface to run EIGRP by default. Toggle ON to disable the interface. • **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: • **bgp**: Redistribute Border Gateway Protocol (BGP) routes into EIGRP. • **connected**: Redistribute connected routes into EIGRP. • **nat-route**: Redistribute network address translation (NAT) routes into EIGRP. • **omp**: Redistribute Overlay Management Protocol (OMP) routes into EIGRP. • **ospf**: Redistribute Open Shortest Path First (OSPF) routes into EIGRP. **Note** From Cisco IOS XE Catalyst SD-WAN Release 16.12.1b and later, you can set metric values for redistribution using the CLI add-on feature template. Use the following command: `redistribute ospf 1 metric 1000000 1 1 1 1500` For more information, see CLI Add-on Feature Templates. • **ospfv3**: OSPFv3 routes into EIGRP. • **static**: Redistribute static routes into EIGRP.

Parameter Name	Description
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. Range: 0 through 65535 Default: 15 seconds
Hello Interval (seconds)	Set the interval at which the router sends EIGRP hello packets. Range: 0 through 65535 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.

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. Range: 1 through 255 Default: 110
Distance for Inter-Area Routes	Specify the OSPF route administration distance for routes coming from one area into another. Range: 1 through 255 Default: 110
Distance for Intra-Area Routes	Specify the OSPF route administration distance for routes within an area. Range: 0 through 255 Default: 110

Redistribute

Field	Description
Add Redistribute	
Protocol	Choose the protocol from which to redistribute routes into OSPF. • Static • Connected • BGP • OMP • NAT • 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. Choose a type: • **administrative**: Force the maximum metric to take effect immediately, through operator intervention. • **on-startup**: Advertise the maximum metric for the specified time.

Area

Field	Description
Add Area	
Area Number*	Enter the number of the OSPF area. Range: 32-bit number
Set the area type	Choose the type of OSPF area: • Stub • NSSA
Add Interface	Configure the properties of an interface in an OSPF area.
Name*	Enter the name of the interface, in the format **`ge`**`slot/port` or **`loopback`** `number`.
Hello Interval (seconds)*	Specify how often the router sends OSPF hello packets. Range: 1 through 65535 seconds 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. Range: 1 through 65535 seconds Default: 40 seconds (four times the default hello interval)
LSA Retransmission Interval (seconds)*	Specify how often the OSPF protocol retransmits LSAs to its neighbors. Range: 1 through 65535 seconds Default: 5 seconds
Interface Cost	Specify the cost of the OSPF interface. 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. Range: 0 through 255 Default: 1
OSPF Network Type	Choose the OSPF network type to which the interface is to connect: • Broadcast network • Point-to-point network • Non-broadcast network • 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. Default: Disabled
Authentication Type	Choose the authentication type: • **simple**: Password is sent in clear text. • **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. 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. Range: 1 through 4294967 Mbps 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: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **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. Range: 1 through 600000 milliseconds (60 seconds) Default: 200 milliseconds
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 milliseconds (60 seconds) Default: 1000 milliseconds
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 Default: 10000 milliseconds (60 seconds)

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	
Protocol	Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions. • **Connected** • **Static** • **Nat-route** • **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. Allowed value: Any 32-bit integer
Area Type	Choose the type of OSPFv3 area: • **Stub**: No external routes • **NSSA**: Not-so-stubby area, allows external routes • **Normal** **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. Range: 0 through 16777215

Field	Description
Authentication Type	Specify the SPI and authentication key if you use IPSec SHA1 authentication type. • **no-auth**: Select no authentication. • **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.
SPI	Specifies the Security Policy Index (SPI) value. 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. 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. 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. Range: 1 through 4294967 Mbps 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: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **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. Default: 100
Distance for External Routes	Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110
Distance for Inter-Area Routes	Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110
Distance for Intra-Area Routes	Set the distance for routes within an area. Range: 0 through 255 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. Range: 1 through 600000 ms (600 seconds) Default: 200 ms
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) 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. • **Immediately**: Force the maximum metric to take effect immediately, through operator intervention. • **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 5 through 86400 seconds 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. • **Connected** • **Static** • **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. Allowed value: Any 32-bit integer

Field	Description
Area Type	Choose the type of OSPFv3 area: • **Stub**: No external routes • **NSSA**: Not-so-stubby area, allows external routes • **Normal** **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. Range: 0 through 16777215
Authentication Type	Specify the SPI and authentication key if you use IPSec SHA1. • **no-auth**: Select no authentication. • **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.
SPI	Specifies the Security Policy Index (SPI) value. 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. 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. 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. Range: 1 through 4294967 Mbps 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: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **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. Default: 100
Distance for External Routes	Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110
Distance for Inter-Area Routes	Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110
Distance for Intra-Area Routes	Set the distance for routes within an area. Range: 0 through 255 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. Range: 1 through 600000 ms (600 seconds) Default: 200 ms
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) 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. • **Immediately**: Force the maximum metric to take effect immediately, through operator intervention. • **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 5 through 86400 seconds Maximum metric is disabled by default.

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: • **Object tracker ID***: Enter the object tracker ID number. Range: 1-1000 • **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: • **Object tracker ID***: Enter the object tracker ID number. Range: 1-1000 • **Route IP***: Enter the IPv4 address of the route. • **Route IP Mask***: Select a value for the subnet mask. • **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. 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: • **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. • **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.

Route Policy

You can configure quality of service (QoS) to classify data packets and control how traffic flows out of and in to the interfaces and on the interface queues. With access lists, you can provision QoS which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted.

1. In **Add Feature** window, 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 window 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 describe the options for configuring the QoS Map 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.

Field	Description
Condition	Specifies the routing condition. The options are: • Address • AS Path List • Community List • Extended Community List • BGP Local Preference • Metric • Next Hop • OMP Tag • Origin • OSPF Tag • Peer
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • Aggregator • AS Path • Atomic Aggregate • Community • Local Preference • Metric • Metric Type • Next Hop • OMP Tag • Origin • Originator • OSPF Tag • Weight

You can select the specific route sequence in the Route Policy window to edit, delete or add.

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	
Protocol	Choose a protocol to configure route advertisements to OMP, for this VPN: • **bgp** • **ospf** • **ospfv3** • **connected** • **static** • **network** • **aggregate** • **eigrp** • **lisp** • **isis**
Select Route Policy	Enter the name of the route policy. 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: • **BGP** • **OSPF** • **Connected** • **Static** • **Network** • **Aggregate**
Select Route Policy	Enter the name of the route policy. 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	

Field	Description
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.
Next Hop/Null 0/VPN/DHCP	Choose one of the following options to configure the next hop to reach the static route: • **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. When you click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter the administrative distance for the route. When you click **Add Next Hop with Tracker**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter 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. • **Null 0**: When you choose this option, the following field appears: • **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. • **VPN**: When you choose this option, the following field appears: • **IPv4 Route VPN***: Selects VPN as the gateway to direct packets to the transport VPN. • **DHCP**: When you choose this option, the following field appears: • **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	

Field	Description
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:
	• **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **Address***: Enter the next-hop IPv6 address.
	  • **Administrative distance***: Enter the administrative distance for the route.
	• **Null 0**: When you choose this option, the following field appears:
	  • **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.
	• **NAT**: When you choose this option, the following field appears:
	  • **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. 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. Tracking is enabled by default.

Service Route

Field	Description
Add Service Route	

Field	Description
Prefix*	Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route.
Service*	Configure routes pointing to any service. 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.

Field	Description
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. 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. 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)	

Field	Description
Protocol*	Choose a protocol from the available options to redistribute the leaked routes.
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.

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. Range: 0, 10 through 1000000 seconds Default: 300 seconds
Configure Interface	
Interface Name	Enter the name of the interface to associate with the bridging domain, in the format **`geslot/port`**.
Mode	Choose the switch port mode. • **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: **Switchport Access Vlan**: Enter the VLAN number, which can be a value from 1 through 4094. • **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: • **Allowed Vlans**: Enter the number of the VLANs for which the trunk can carry traffic and a description for the VLAN. • **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.

Field	Description
Port Control	Choose the port control mode to enable IEEE 802.1X port-based authentication on the interface. • **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. • **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. • **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.
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). • **single-host**: Grant access only to the first authenticated host. This is the default. • **multi-auth**: Grant access to one host on a voice VLAN and multiple hosts on data VLANs. • **multi-host**: Grant access to multiple hosts. • **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. Default: 60 seconds

Field	Description
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.

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: • **http**

Field	Description
Endpoint	Choose an endpoint type: • **Endpoint IP**: When you choose this option, the following field appears: **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. • **Endpoint DNS Name**: When you choose this option, the following field appears: **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. • **Endpoint API URL**: When you choose this option, the following field appears: **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. Range: 20 to 600 seconds Default: 60 seconds (1 minute).
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range: 1 to 10 Default: 3
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds

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**. **OR** ensures that the static route status is reported as active if either one of the associated trackers of the tracker group report that the route is active. If you select **AND**, the static route status is reported as active if both the associated trackers of the tracker group report that the route is active.

Wireless LAN

This feature helps you configure a wireless controller.

The following tables describe the options for configuring the Wireless LAN feature.

Basic Configuration

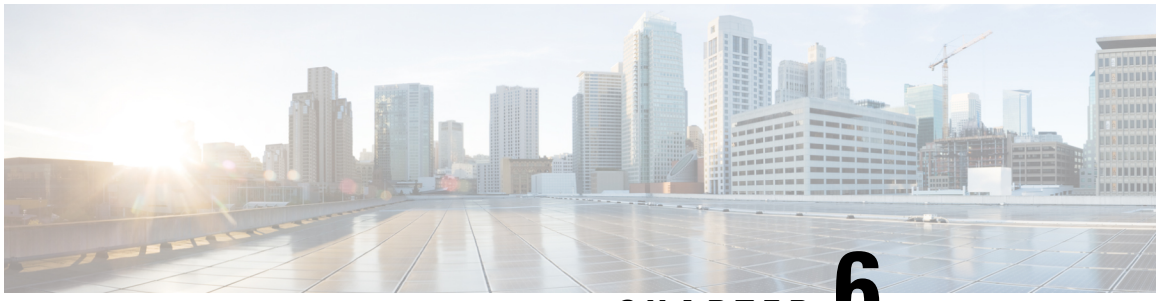
Field	Description
Enable 2.4G*	Disable this option to shut down the radio type of 2.4 GHz. Default: Enabled
Enable 5G*	Disable this option to shut down the radio type of 5 GHz. Default: Enabled
Country*	Choose the country where the router is installed.
Username*	Specify the username of Cisco Mobility 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. 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: • **2.4GHz** • **5GHz** • **All**
Security Type*	Choose a security type: • **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server. • **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase. • **Open**: Choose this option to allow access to the wireless network without authentication.
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.



CHAPTER 6

Policy Object Profile

AS Path

1. Choose the **AS Path** policy object from the **Select Policy Object** drop-down list.
2. Enter the AS Path list name in the **AS Path List Name** field.
3. In the **Add AS Path** field, enter the AS path number.
4. Click **Save**.

The following table describe the options for configuring the class map.

Field	Description
AS Path List Name	Enter a name for the class map list.
Add AS Path	Specifies the AS path number. The range is 1 to 65535.

Class Map

1. Choose the **Class Map** policy object from the **Select Policy Object** drop-down list.
2. Enter the class map name in the **Class** field.

3. In the **Select a Queue** drop-down list, choose the required queue.
4. Click **Save**.

The following table describe the options for configuring the class map.

Field	Description
Class	Enter a name for the class map list.
Queue	Specifies the queue number.

Data Prefix

1. Choose the **Data Prefix** policy object from the **Select Policy Object** drop-down list.
2. Enter the **Data Prefix List Name**.
3. In the **Internet Protocol** field, click **IPv4** or **IPv6**.
4. Click **Save**.

The following table describe the options for configuring the data prefix.

Field	Description
Prefix List Name	Enter a name for the prefix list.
Internet Protocol	Specifies the internet protocol. The options are IPv4 and IPv6.

Prefix

1. Choose the **Prefix** policy object from the **Select Policy Object** drop-down list.
2. Enter the **Prefix List Name**.
3. In the **Internet Protocol** field, click **IPv4** or **IPv6**.
4. Under **Add Prefix**, enter the prefix for the list. Optionally, click the **Choose a file** link to import a prefix list.
5. Click **Save**.

The following table describe the options for configuring the prefix.

Field	Description
Prefix List Name	Enter a name for the prefix list.

Field	Description
Internet Protocol	Specifies the internet protocol. The options are IPv4 and IPv6.

Expanded Community

1. Choose the **Expanded Community** policy object from the **Select Policy Object** drop-down list.
2. Enter the **Expanded Community List Name**.
3. In the **Add Expanded Community** field, enter the community details. The format example is given in the field.
4. Click **Save**.

The following table describe the options for configuring the expanded community.

Field	Description
Expanded Community List Name	Enter a name for the community list.
Add Expanded Community	Specifies the expanded community.

Extended Community

1. Choose the **Extended Community** policy object from the **Select Policy Object** drop-down list.
2. Enter the **Extended Community List Name**.
3. In the **Add Extended Community** field, enter the community details. The format example is given in the field.
4. Click **Save**.

The following table describe 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	Specifies the extended community. The format is as follows: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.

Mirror

1. Choose the **Mirror** policy object from the **Select Policy Object** drop-down list.
2. Enter the **Mirror List Name**.
3. In the **Remote Destination IP** field, enter the IP address of the destination for which to mirror the packets.
4. In the **Source IP** field, enter the IP address of the source of the packets to mirror.
5. 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 describe the options for configuring the mirror.

Field	Description
Mirror List Name	Enter a name for the mirror list.
Remote Destination IP	Specifies the IP address of the remote destination.
Source IP	Specifies the IP address of the source.

Policer

1. Choose the **Policer** policy object from the **Select Policy Object** drop-down list.
2. Enter the **Policer List Name**.

3. In the **Burst (bytes)** field.
4. In the **Exceed** drop-down list, choose the action **Drop** or **Remark**.
5. Enter the **Rate (bps)**
6. Click **Save**.

The following table describe the options for configuring the policer.

Field	Description
Policer List Name	Enter a name for the policer list.
Burst (bytes)	Specifies the maximum traffic burst size. Range is from 15000 to 10000000.
Exceed	Specifies an action to take when the burst size or traffic rate is exceeded. The options are: **Drop**—Sets the packet loss priority (PLP) to low. **Remark**—Sets the PLP to high. The default option is **Drop**.
Rate	Specifies the maximum traffic rate. It can be a value from 8 through 2^{64} bps (8 through 100000000000).

Standard Community

1. Choose the **Standard Community** policy object from the **Select Policy Object** drop-down list.
2. Enter the **Standard Community List Name**.
3. In the **Add Standard Community** field, enter the community details. The format example is given in the field.
4. Click **Save**.

The following table describe the options for configuring the standard community.

Field	Description
Expanded Community List Name	Enter a name for the community list.

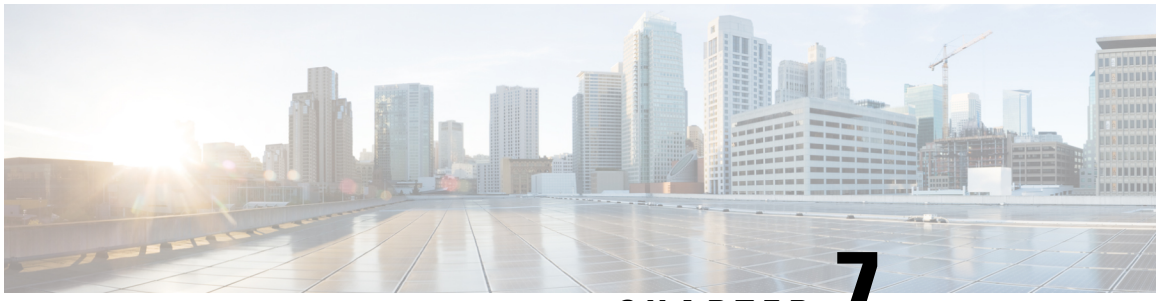
Field	Description
Add Expanded Community	Specifies the standard community. the options are: • *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS number. • **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.

VPN

1. Choose the **VPN** policy object from the **Select Policy Object** drop-down list.
2. Enter the **VPN List Name** and the **Add VPN**fields based on the hints.
3. Click **Save**.

The following table describe the options for configuring the VPN object.

Field	Description
VPN List Name	Enter a name for the VPN list.
Add VPN	Enter the VPN number. The number can be 100 or 200 separated by commas or 1000—2000 range.



CHAPTER 7

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. 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. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, 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. 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. 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.
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. **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. 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.

Field	Description
Proxy Type	If the Cisco ThousandEyes Enterprise agent must use proxy server for external access, choose one of the following as proxy type: • **static** • **pac** • **none** Static proxy settings: • **Proxy Host**: Set the configuration as a **Global** setting and enter the hostname of the proxy server. • **Proxy Port**: Set the configuration as a **Global** setting and enter the port number of the proxy server. PAC settings: • **PAC URL**: Set the configuration as a **Global** setting and enter the URL of the proxy auto-configuration (PAC) file.

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. 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. 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. 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.

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. 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.

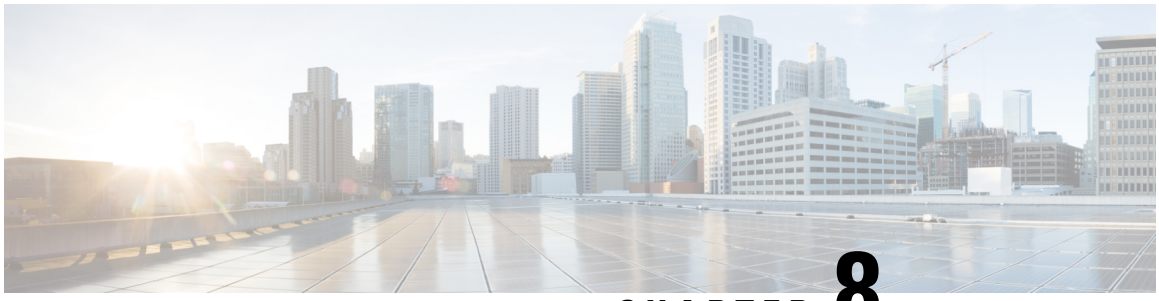
IMC

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. Not all hardware models have a dedicated access port. See the release notes for your Cisco Catalyst SD-WAN release for the supported hardware. Available options: • **Dedicated** • **Shared** Configure the appropriate port (GE or TE) based on the hardware module.
IPv4 Address*	Provide the UCS-E management port address.
Default Gateway*	Gateway tracking determine, for static routes, whether the next hop is reachable before adding that route to the device's route table. 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.

Field	Description
UCSE Interface VPN	Specify the details of the UCS-E interface VPN.
IPv4 Address	Provide the UCS-E management port address.



CHAPTER 8

CLI Add-On Profile

Information About the CLI Add-On Profile

Using a CLI add-on profile, you can specify CLI commands to execute on devices. You can execute device configurations that are not available through other configuration group features.

Commands in a CLI add-on profile operate together with the configurations provided through configuration group features. However, commands in the CLI add-on profile override configurations specified by corresponding configuration group features. One use case for the CLI add-on profile is to add commands to temporarily override a setting configured in a configuration group feature without changing the feature.

Format

When you add commands to a CLI add-on profile, enter them as they appear in the output of the **show sdwan running-config** command.

CLI Add-On Profile Restrictions

- Ensure that you only use configuration commands as they appear in the output of the **show sdwan running-config** command.
- Use only supported commands in the CLI add-on profile, which are the qualified commands documented in the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference*. Using unsupported commands in the CLI add-on profile can cause errors when deploying a configuration group to devices.

Create a CLI Add-On Profile

Before You Begin

Ensure that there is at least one configuration group in the **Configuration Groups** list.

This procedure adds a CLI add-on profile to a configuration group that does not have one. For information about editing an existing CLI add-on profile, see Edit a CLI Add-On Profile, on page 163.

Create a CLI Add-On Profile

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Adjacent to a configuration group, click **…** and choose **Edit**.
3. In the **Feature Profiles - Unconfigured** area, locate **CLI Profile**.

Note If the configuration group already has a CLI profile configured, this option will not appear.

4. On the **CLI Profile** card, click **Start Configuration**.

   An **Edit Config Feature** pane opens.
5. Enter a name and, optionally, a description for a new CLI add-on profile.
6. Enter configuration commands in the **CLI Configuration** area or click **Import Config File** to import a configuration.
7. To convert a configuration value to a variable, select the value and click **Create Variable**.

   Enter the variable name, and click **Create Variable**. You can also type a variable name directly, in the format {{variable-name}}. Example: {{hostname}}

   Variables enable you to enter values for the variables individually for each device when you deploy a configuration group to devices. During the deployment, you can enter values manually or using a CSV file.
8. To encrypt a plain-text password using type 6 encryption, select the password and click **Encrypt Type 6**.

   In the example below, you can select the password, ABCD, and click **Encrypt Type 6** to encrypt the password.

   ```
   server-private 10.0.0.1 key 0 ABCD
   ```

   For more information about type 6 encryption, see Type 6 Passwords on Cisco IOS XE SD-WAN Routers in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Note Encrypt only passwords. Encrypting a CLI command may cause a failure when deploying the configuration group to devices.

9. Click **Save**.

Edit a CLI Add-On Profile

Before You Begin

Ensure that there is a configuration group with a CLI add-on profile configured, in the **Configuration Groups** list. For information about creating a CLI add-on profile, see Create a CLI Add-On Profile, on page 162.

Edit a CLI Add-On Profile

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. In the CLI add-on profile, adjacent to the config feature, click **…** and choose **Edit Feature**.
3. Edit the configuration commands in the **CLI Configuration** area or click **Import Config File** to import a configuration.
4. To convert a configuration value to a variable, select the value and click **Create Variable**.

   Enter the variable name, and click **Create Variable**. You can also type a variable name directly, in the format {{variable-name}}. Example: {{hostname}}

   Variables enable you to enter values for the variables individually for each device when you deploy a configuration group to devices. During the deployment, you can enter values manually or using a CSV file.
5. To encrypt a plain-text password using type 6 encryption, select the password and click **Encrypt Type 6**.

   In the example below, you can select the password, ABCD, and click **Encrypt Type 6** to encrypt the password.

   ```
   server-private 10.0.0.1 key 0 ABCD
   ```

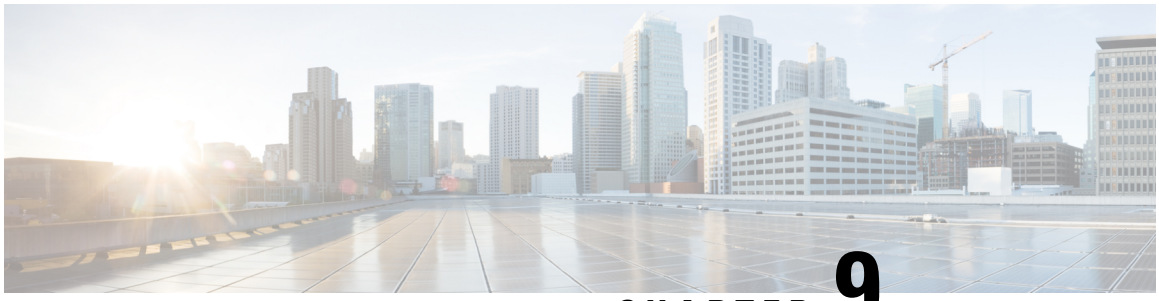
   For more information about type 6 encryption, see Type 6 Passwords on Cisco IOS XE SD-WAN Routers in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Note Encrypt only passwords. Encrypting a CLI command may cause a failure when deploying the configuration group to devices.

6. Click **Save**.

PART II

Part Teleworker (Mobility)



CHAPTER 9

Global 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	

Field	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. 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. Each username must have a password. Users are allowed to change their own passwords. 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.
Privilege	Select between privilege level 1 or 15. • Level 1: User EXEC mode. Read-only, and access to limited commands, such as the ping command. • 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. Range: 0 through 65535. Default: 1813

Field	Description
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. Default: 1812
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 seconds
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS 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 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. Default: 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.

Accounting

Field	Description
Add Accounting Rule	
Rule Id*	Enter the accounting rule ID.

Field	Description
Method*	Specifies the accounting method list. Choose one of the following: • **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level. • **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**: Runs accounting for all network-related service requests. • **system**: Performs accounting for all system-level events not associated with users, such as reloads. **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.
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.

Field	Description
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.

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.
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. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps). Default: 9600
Overlay ID	Specifies the overlay ID of a device in the Cisco Catalyst SD-WAN overlay network. Range: 0 - 4294967295 ($2^{32} – 1$) 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. 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. 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. Default: Enabled
Track Interface Tag	Set the tag string to include in routes associated with a network that is connected to a non-operational interface. 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. 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. Values: 0 through 19
On Demand Tunnel	Enable dynamic on-demand tunnels between any two Cisco Catalyst SD-WAN spoke devices.

Field	Description
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. Range: 1 to 65535 minutes Default: 10 minutes
Control Session PPS	Enter a maximum rate of DTLS control session traffic to police the flow of control traffic. Range: 1 through 65535 pps 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. Default: Enabled

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. Range: 1 through 15
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.

Field	Description
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.

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.
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. Range: 0 through 65535 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. Range: 3 to 7 minutes 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 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.
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. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
Color	Choose a color for the TLOC.

Field	Description
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 600000 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. Range: 12 through 6000 seconds Default: 12 seconds
Last-Resort Circuit	Enable this option to use the tunnel interface as the circuit of last resort.
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. 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. Range: 0 through 100 Default: 2
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
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. Range: 1 through 100
Manager 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

Field	Description
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. Default: Enabled
Low-Bandwidth Link	Enable this option to characterize the tunnel interface as a low-bandwidth link.
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. Range: 500 to 1460 bytes 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: • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**

Field	Description
Encapsulation	
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. 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	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
GRE Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. 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. 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. Range: 1 through 255 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. Range: 1 through 8947 minutes Default: 1 minutes

Field	Description
TCP Timeout*	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes 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. Range: 576 through 9216 Default: 1500 bytes
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 9216 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: 500 to 1460 bytes Default: None

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. **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.
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. 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. 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. 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.

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). 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. • **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. • **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**. 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. • **IP Address***: Enter the IP address. • **Subnet Mask:** Enter the subnet mask.
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.

Field	Description
IPv6 Settings	Configure an IPv6 VPN interface. • **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. • **Static**: Choose **Static** to enter an IP address that doesn't change. • **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: • **pool** • **loopback** 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.
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. Default: Enabled
NAT Loopback	Enter the IP address of the loopback interface.

Field	Description
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minutes
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes 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. • **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. • **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: • **Source Prefix***: Enter the source IPv6 prefix. • **Translated Source Prefix***: Enter the translated source prefix. • **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. 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. Range: 1 through 254 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 . Range: 100 through 40950 seconds 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. Range: 100 to 4294967295
Add VRRP IP Address Secondary	
IP Address*	Enter an IP address for the secondary VRRP router.
Subnet Mask	Enter the subnet mask.
Add VRRP Tracking Object	
Tracker ID*	Enter the interface object ID or object group tracker ID.

Field	Description
Tracker Action*	Choose one of the options: • **decrement** • **shutdown**
Decrement Value*	Enter a decrement value. 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. 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. Range: 1 through 254 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 . Range: 100 through 40950 seconds 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.
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.

Field	Description
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. 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. Default: full
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. Range: 576 through 9216 Default: 1500 bytes

Field	Description
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet) 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: 500 to 1460 bytes Default: None
Speed	Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. 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. Range: 0 through 2147483 seconds 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: • **auto-select**: A connection is automatically selected. • **rj45**: Specifies an RJ-45 physical connection. • **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.
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. By default, an interface allows ICMP redirect messages.

Field	Description
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. 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.

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). 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.

Field	Description
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. • **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. • **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**. 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. • **IP Address**: Enter the IP address. • **Subnet Mask:** Enter the subnet mask.
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. • **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. • **Static**: Choose **Static** to enter an IP address that doesn't change. • **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: • **interface** • **pool** • **loopback** Default: **interface**. It is supported for NAT64.
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minute
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes 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. • **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. • **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.

Field	Description
Select NAT	Choose NAT64 or NAT66. When you choose NAT66, the following fields appear: • **Source Prefix**: Enter the source IPv6 prefix. • **Translated Source Prefix**: Enter the translated source prefix. • **Source VPN ID**: Enter the source VPN ID. • **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. Default: full
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. Range: 576 through 9216 Default: 1500 bytes
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet) 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: 500 to 1460 bytes Default: None

Field	Description
Speed	Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. 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. Range: 0 through 2147483 seconds 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: • **auto-select**: A connection is automatically selected. • **rj45**: Specifies an RJ-45 physical connection. • **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media.
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. **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.

Field	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. 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.
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. By default, an interface allows ICMP redirect messages.

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. Range: 1 to 20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the oldest files. Range: 1 to 10 Default: 10

TLS Profile

Field	Description
Add TLS Profile	
TLS Profile Name*	Enter the name of the TLS profile.
TLS Version	Choose a TLS version: • **TLSv1.1** • **TLSv1.2**
Authentication Type*	Choose **Server**.
Cipher Suite List	Choose groups of cipher suites (encryption algorithm) based on the TLS version. The following is the list of cipher suites. • **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 • **dhe-aes-cbc-sha2**: Encryption type tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **dhe-aes-gcm-sha2**: Encryption type tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 and above) • **ecdhe-ecdsa-aes-gcm-sha2**: Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 and above) SuiteB • **ecdhe-rsa-aes-cbc-sha2**: Encryption type tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 and above) • **ecdhe-rsa-aes-gcm-sha2**: Encryption type tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 and above) • **rsa-aes-cbc-sha2**: Encryption type tls_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **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. 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. 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: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **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: **TLS Properties Custom Profile**: Enable this option to choose a TLS profile. When you enable this option, the following field appears: **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. 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. 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: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **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.

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.

Field	Description
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. Range: 0 to 65530
Set authentication key for the server	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. 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. Range: 1 to 4 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. 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. When you enable this option, the following field appears: **Stratum**: Enter the stratum value for the primary NTP router. The stratum value defines the hierarchical distance of the router from its reference clock. 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. For example, enter **`GigabitEthernet1`** or **`Loopback0`**.

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. Range: 10 through 1209600 seconds (14 days) 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. This option is turned off by default. Click **On** to enable it. Enabling the feature displays the **Extended Anti-Replay Window** field. Range: 10 ms to 2048 ms Default: 256 ms

Field	Description
Replay Window	Specify the size of the sliding replay window. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets. 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: • **esp**: Enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header. • **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. • **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. • **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.

Field	Description
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). A MAC is computed for a TCP segment using a configured MAC algorithm, relevant traffic keys, and the TCP segment data prefixed with a pseudoheader. When options are included, the content of all options is included in the MAC with TCP-AO's **MAC** field is filled with zeroes. 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. 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. Range: 0 through 255.
Send ID*	Specify the send identifier for the key. Range: 0 through 255.
TCP	Specify the algorithm to compute MACs for TCP segments. You can choose one of the following: • **aes-128-cmac** • **hmac-sha-1** • **hmac-sha-256**
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: • **Accept Local**: This option is disabled by default. Click **On** to enable it. • **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. • **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).

Field	Description
Send Lifetime	The following fields appear when you click this field: • **Send Local**: This option is disabled by default. Click **On** to enable it. • **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. • **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).

VPN Interface GRE

Use the VPN Interface GRE feature for all Cisco vEdge Cloud and Cisco vEdge router devices.

The following tables describe the options for configuring the 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 IPv6 packets on the interface. Range: 576 through 9216 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 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 through 1460 bytes Default: None

VPN QoS Map

Associate a QoS map with each VPN list and define the minimum and maximum bandwidth that must be used by traffic belonging to the VPNs in the VPN list.

The following tables describe the options for configuring the VPN QoS Map feature.

Add VPN QoS

Field	Description
Minimum Bandwidth(Kbps)*	Enter the minimum bandwidth allocated to each VPN or each group of VPNs. Input value must be an integer. The minimum input value is 8.
QoS Map*	Specify the name of the QoS map to apply to packets being transmitted out the interface. Apply the Qos Map to each VPN or each group of VPNs based on the QoS Map configuration.
Shaping Rate(Kbps)	Specify the value of the maximum bandwidth in kilobits per second (kbps), allocated to each VPN or each group of VPNs. Input value must be an integer. The minimum input value is 8.
VPN Group*	Choose a VPN group from the dropdown list.

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. Range: 1 through 65535

Parameter Name	Description
PPP Authentication Protocol	Select the authentication protocol used by the multilink interface: • **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters. • **PAP**: Enter the username and password provided by your ISP. *username* can be up to 255 characters. • **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. 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. 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. 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: • **esf**: Send T1 frames as extended superframes. This is the default. • **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing.

Parameter Name	Description
Clock Source	Select the clock source: • **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. • **internal**: Use the controller framer as the primary clock.
Line Code	Select the line encoding to use to send T1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • **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 • **short**: Set the transmission attenuation for cables that are 660 feet or shorter. • **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. 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: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do no use CRC4.
Clock Source	Select the clock source: • **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. • **internal**: Use the controller framer as the primary clock.
Line Code	Select the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **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. Range: 0 through 30
Time Slot	To configure the serial WAN on the interface, enter a value for the timeslot. 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. 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. Range: 0 through 8 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. 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. Range: 0 through 8 Default: 5

Parameter Name	Description
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. 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. 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. Specify the MSS of TPC SYN packets passing through the . By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. 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.: • **Unidirectional**: The server initiates the authentication. • **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. Range: 500 through 1460 bytes 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. Range: 0 through 1000 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. Range: 576 through 1804 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).

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. Default: Enabled
Enable 5G*	Disable this option to shut down the radio type of 5 GHz. 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. 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: • **2.4GHz** • **5GHz** • **All**

Field	Description
Security Type*	Choose a security type: • **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server. • **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase. • **Open**: Choose this option to allow access to the wireless network without authentication.
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.