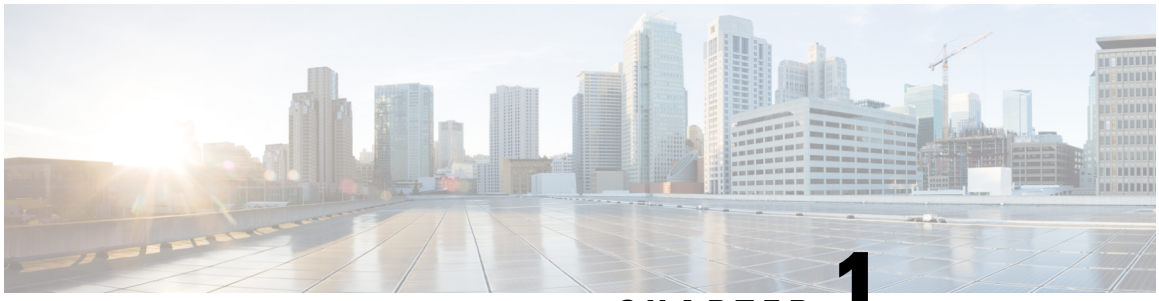
Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x

First Published: 2023-07-25

Last Modified: 2024-08-27

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

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

Configuration Groups and Feature Profiles

Table 1: Feature History

Feature Name	Release Information	Description
Configuration Groups and Feature Profiles	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature provides a simple, reusable, and structured approach for the configurations in Cisco Catalyst SD-WAN. You can create a configuration group, that is, a logical grouping of features or configurations that is applied to one or more devices in the network that is managed by Cisco Catalyst SD-WAN. You can also create profiles based on features that are required, recommended, or uniquely used, and then combine the profiles to complete a device configuration. The configuration group workflow in Cisco SD-WAN Manager provides a guided method to create configuration groups and feature profiles.

Feature Name	Release Information	Description

Configuration Groups and Feature Profiles (Phase II)	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
	Cisco vManage Release 20.9.1
		The following enhancements are introduced in the Configuration Group feature.
		• Adds support for the following features:
		  • SNMP
		  • Cellular Interface
		  • BGP Routing (transport and management profile)
		  • Wireless LAN
		  • Switch Port
		  • SVI Interface
		  • DHCP Server
		  • ThousandEyes
		• Adds IPv6 configuration support in the VPN, interface, and BGP features.
		• Adds the following options to the global settings that are a part of the system profile. These options have been added to the **Other Settings** tab.
		  • Generate keepalive timers when incoming or outgoing network connections are idle
		  • Enable small TCP and UDP servers
		  • Enable console logging
		  • Enable IP source routing
		  • Display log messages to a VTY session
		  • Enable SNMP IFINDEX persistence
		  • Enable BOOTP server

Create Configuration Group Workflow for a Single-Router Site	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature introduces the Create Configuration Group workflow. This simplified workflow consolidates the various settings pages into a single page so that you can easily review your configuration at once. The workflow also enables you to set up WAN and LAN routing in addition to the basic settings, at the time of creating a configuration group. As a result, a configuration that is created from the workflow is now immediately deployable.

Feature Name	Release Information	Description
Security Feature Profile in Configuration Groups	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This feature enables you to configure a security profile in configuration groups.

Localized Policy for QoS, ACL, and Routing	Cisco vManage Release 20.10.1
	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a
		This feature enables you to configure a policy profile, a QoS map policy, a route policy, and an ACL policy through feature profiles.
		The following enhancements are introduced in this feature:
		• Policy objects under policy profiles:
		  • AS Path
		  • Standard Community
		  • Expanded Community
		  • Data Prefix
		  • Extended Community
		  • Class Map
		  • Mirror
		  • Policer
		  • Prefix
		• QoS map policy under Service and Transport profiles
		• Route policy under Service and Transport profiles
		• ACL policy under Service and Transport profiles

Variables and Type 6 Encryption in CLI Profile	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	After you enter or import configuration into a CLI profile, you can convert certain values to device-specific variables or encrypt strings such as passwords, using Type 6 encryption.

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Remote Access Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device, using Cisco SD-WAN Manager. Configure Remote Access in the System feature profile in a configuration group. • Private IP Pool • Authentication • AAA Policy • IKEv2 Settings • IPSec Settings
Device Variables Option	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables you to modify system IP or site ID details of the device from the Associate Devices page while deploying devices.

Feature Name	Release Information	Description
Configuration Groups and Feature Profiles (Phase III)	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	The following new features are introduced to the feature profiles: • In the System Profile: • Fabric Security **Note** Before the Cisco Catalyst SD-WAN Manager Release 20.12.1, Fabric Security was called Cisco Security. • IPV4-Device-Access-Policy • IPV6-Device-Access-Policy • Remote Access • In the Transport Profile • OSPF Routing • VPN Interface GRE • IPSEC • Tracker Group • IPv6 Tracker • IPv6 Tracker Group • GPS • In the Service Profile • VPN Interface GRE • IPSEC • Tracker • Tracker Group • AppQoE • Multicast • In the Other Profile • UCSE

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enables you to configure the following Cisco Catalyst SD-WAN Remote Access features for a device in SSL-VPN mode, using Cisco SD-WAN Manager: • Private IP Pool • Authentication • AAA Policy

Feature Name	Release Information	Description
Configuration Groups and Feature Profiles (Phase IV)	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Control Components Release 20.12.1	

Feature Name	Release Information	Description
		The following new features are introduced to the feature profiles: • In the System Profile: • Flexible Port Speed • In the Transport Profile: • OSPFv3 IPv4 Routing • OSPFv3 IPv6 Routing • T1/E1 Controller • Subfeatures for transport VPN: • OSPFv3 IPv4 Routing • OSPFv3 IPv6 Routing • T1/E1/Serial • DSL PPPoE • DSL PPPoA • DSL IPoE • Ethernet PPPoE • In the Service Profile: • OSPFv3 IPv4 Routing • OSPFv3 IPv6 Routing • EIGRP Routing • Object Tracker • Object Tracker Group • Subfeatures for service VPN: • OSPFv3 IPv4 Routing • OSPFv3 IPv6 Routing • EIGRP Routing • Multilink Controller • Object Tracker • Object Tracker Group The **Route leak to Global VPN** option is added to the

Feature Name	Release Information	Description
		Route Leak parameter in the service VPN
Support for Dual Device Site Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature supports dual devices site configuration in the configuration groups workflow. You can select the dual router type configuration group workflow to deploy two devices in the same site considering the redundancy in the router.
Support for Specifying Default Values for Device-Specific Variables of a Feature	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	You can provide a default value along with description to feature parameters when you select the **Device Specific** scope. Cisco SD-WAN Manager applies the default value of the parameter to the device while deploying the configuration group.
Create a Configuration Group Without Using a Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature introduces a method for creating configuration groups directly on the **Configuration Groups** page of Cisco SD-WAN Manager without launching a workflow. After selecting a product solution, you can create a configuration group based on the available profiles for that solution. Cisco SD-WAN Manager creates the configuration group with the required profiles, which you can configure based on your requirement. This feature allows you to reuse previously created profiles. You can create, manage, and deploy the configuration group from one page.

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.

Note If you assign a private color to a WAN interface while configuring a site using the configuration group workflow in Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, a static IP address is assigned by default.

Private colors are metro-ethernet, mpls, private1, private2, private3, private4, private5, or private6.

- 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 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.

  From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, you can create, manage, and deploy the configuration group from one single window.

- End-to-end configuration without using a workflow

  From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, you can create a configuration group without using workflows. Choose the SD-WAN option from the solution drop-down list to view or create a

configuration group with just two mandatory profiles—the System profile and the Transport & Management profile.

You can create other profiles such as Service, Policy, CLI-Add-on, and so on, based on your requirement.

- Contextual method of adding features

  From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, you can add features to profiles on a contextual basis. For example, if you are editing a VPN feature, then only interfaces appear in the contextual menu for you to add, but other VPNs don't.

- 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.

  From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, you can share profiles between multiple configuration groups.

- 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

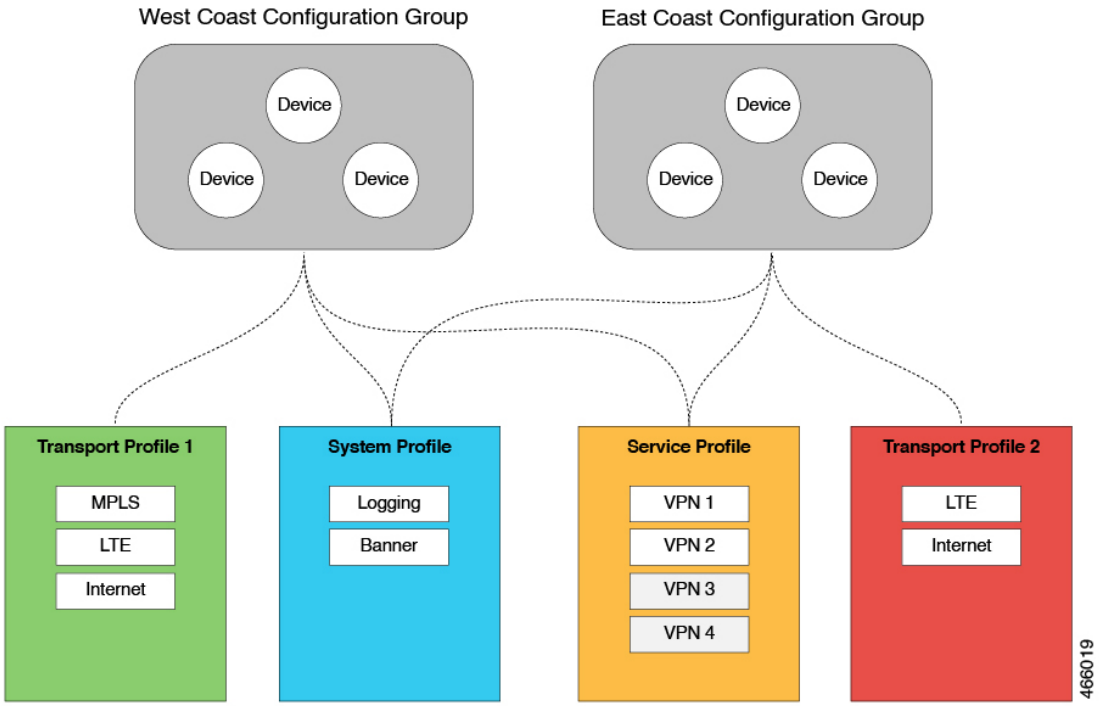
- You can associate a device to either a configuration group or a device template, but not both.
- You can add a device to only one configuration group.
- You can add only one tag rule to a configuration group.
- (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1) You can only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



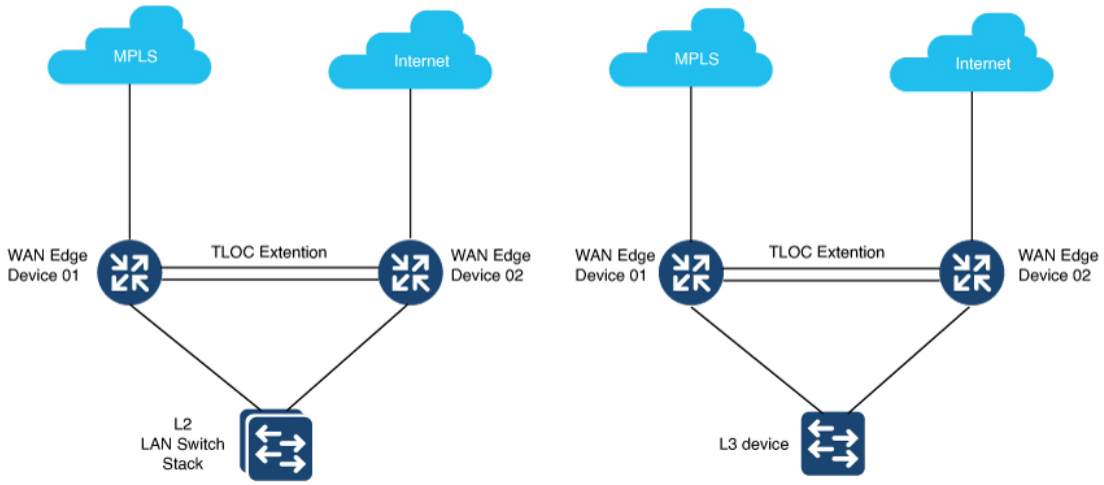
In this figure,

- 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

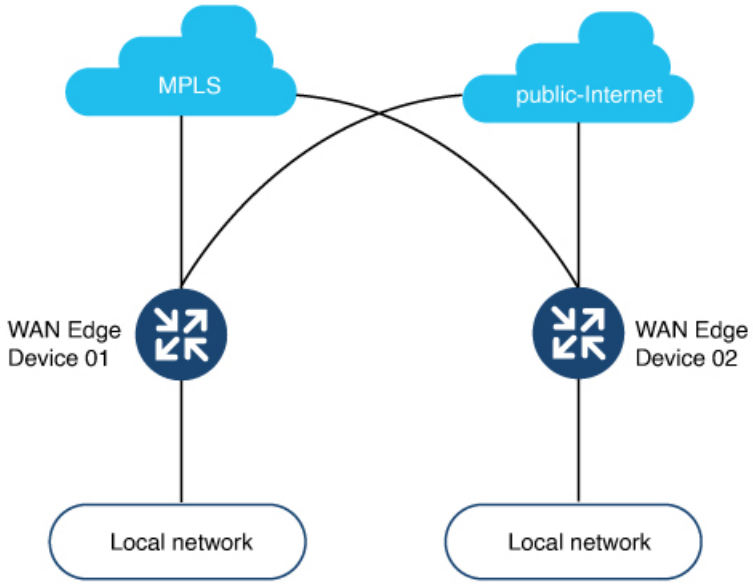
To deploy dual device site configuration, you can choose a TLOC extension or a full mesh topology in the dual router type configuration group workflow. Use of TLOC extensions is recommended for failure scenarios and redundancy.

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.

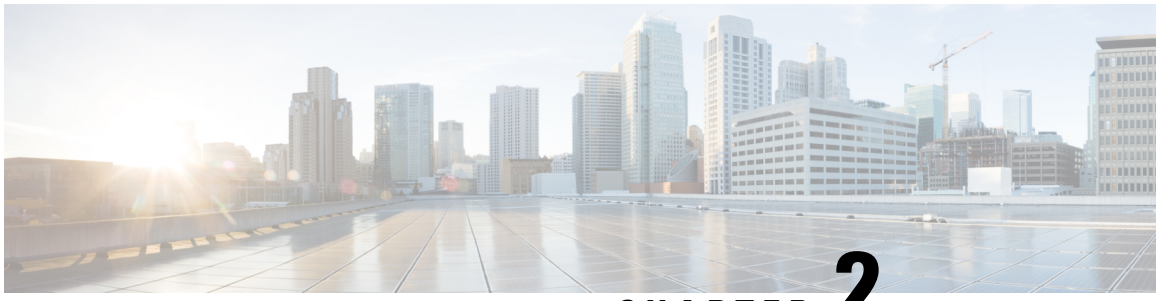
Figure 3: Full Mesh Topology



In the full mesh topology, there's no transport extension and there's an assumption that each device has its own public uplink.

PART I

Using Configuration Groups



CHAPTER 2

Using Configuration Groups, Cisco Catalyst SD-WAN Manager Release 20.15 and Later

Create a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Choose the SD-WAN option from the solution drop-down list to view or create a configuration group for Cisco Catalyst SD-WAN solution.

   The default solution is SD-WAN.
3. Click **Create Configuration Group** and configure the following:

Field	Description
Name	Enter a name for the new configuration group.
Description	Enter a description of the new configuration group.
CLI Configuration Group	Choose this option and enter CLI commands that create a configuration group.

Field	Description
Site Type	This option is available only for the SD-WAN solution type. Choose one of these site types: • **Single Router**: Deploy a configuration and distribute the transport side WAN and service-side LAN interface configurations to a single router. Default: Single router. • **Dual Router**: Provide a name to each of the routers. Use this option to deploy a dual-device site configuration and distribute the transport-side WAN and service side LAN interface configurations between the two devices.

4. (Optional) Alternatively, you can create a configuration group by choosing one of these options from the **Create Configuration Group** drop-down list:
   - **Import from Calalog**: Choose a configuration groups from a list of configuration catalogs. For more information, see Configuration Catalog.
   - **Create from Guided Workflow**: The workflow guides you in creating a configuration group.
5. Click **Create**.

   The Cisco SD-WAN Manager creates the configuration group with these mandatory feature profiles that you can configure:
   - System profile
   - Transport & Management profile
6. Click **Add Profile** to create more feature profiles.
7. Click the drop-down list in a feature profile to either choose an existing feature profile or create a new one by choosing the **Create New** option. When the new profiles are created, you must configure them before associating them to the configuration groups.

Create a CLI Based Configuration Group

You can create a CLI based configuration group when you choose SD-WAN or SD-Routing solutions.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Create Configuration Group** and choose **CLI Configuration Group**.
3. Enter a name and description for the CLI configuration group.
4. Click **Create**.
5. Load running configurations from reachable devices by choosing a reachable device from the **Load Running config from reachable device:** drop-down list.
6. Use **Search CLI** to search for particular lines of CLIs.

7. Click **Create Variable** and provide a name for the variable for the CLI-based configuration group.
8. Highlight text in the **Config Preview** code block and click **Encrypt Type6** to encrypt the text.
9. Click **Import Config File** to import a config file from your local storage.
10. Type the configurations manually in the config preview code block and add customized configuration.
11. Click **Save** to save the configuration.
12. Click **Done**

Create Feature Profiles

The feature profile tap displays previously defined feature profiles. The options that appear in a feature profile tabs depend on the solution, such as SD-WAN, SD-Routing, and so on. Choose from one of the following feature profiles by clicking the respective tab to view, add, or edit a new profile if you have selected the SD-WAN solution:

- System Profile
- Transport & Management Profile
- Service Profile
- CLI Add-On Profile
- UC Voice Profile
- Other Profile
- Policy Profile

View a Feature Profile

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click the feature profile tab.

   A list of available profiles appear, where you can view details such as history, description, or the number of configuration groups that share the profile.

   After you select a feature, the **SHARED** menu displays the count of configuration groups that share the feature. Hover over the count to view the names of the configuration groups that share the feature.

Add a Feature Profile

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click a feature profile tab and click **Add New**.

   Alternatively, click a configuration group from the available list and choose **+ Create New** from the drop-down list of a feature profile.

3. Click the pencil icon that is next to a feature profile or select a feature profile from the drop-down menu to add a feature profile to edit.
4. Enter a name and description for the feature profile.
5. Click **Create**.

Edit a Feature Profile

You can edit a feature profile from the **Configuration Groups** tab or by clicking a particular feature profile tab.

Edit a Feature from the Configuration Groups Tab

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click the **Configuration Groups** tab.
3. Click a configuration group from the available list.
4. Click the pencil icon that is next to a feature profile and edit the feature.
5. If you have created a configuration group for dual router type, you can apply the configuration to all or individual routers by choosing one of the options: **All**, **EdgeDevice_01** or **EdgeDevice_02**.
6. Click **Save**.
7. If you have created a configuration group for dual router type, choose one of these options:
   - **Save on Both Devices**
   - **Save on EdgeDevice_01**
   - **Save on EdgeDevice_02**

Edit a Feature from the Feature Profile Tab

1. Click a feature profile tab.
2. Click the icon under the **Actions** column for a feature profile.
3. Click **Edit**.
4. Click the pencil icon that is next to a feature and edit the feature.
5. If you have created a configuration group for dual router type, you can apply the configuration to all or individual routers by choosing one of the options: **All**, **EdgeDevice_01** or **EdgeDevice_02**.
6. Click **Save**.
7. If you have created a configuration group for dual router type, choose one of these options:
   - **Save on Both Devices**
   - **Save on EdgeDevice_01**
   - **Save on EdgeDevice_02**

Add a Feature to a Feature Profile

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Add a feature in one of these two methods:
   a. From the **Configuration Groups** tab:
      1. Click a configuration group from the available list.
      2. Click the pencil icon that is next to a feature profile or choose a feature profile from the drop-down menu to add a feature profile to edit.
      3. Click **+ Add New Feature** and choose additional features from the **Add Features** pane to add to the feature profile.

   b. From the available feature profiles:
      1. Choose a feature profile tab.
      2. Click the icon under the **Actions** column for that feature profile.
      3. Click **Edit**.
      4. Click **+ Add New Feature** and choose additional features from the **Add Features** pane to add to the feature profile.

3. In the **Name** field, enter a name for the feature.

   The name can be up to 128 characters and can contain only alphanumeric characters.
4. 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.
5. Configure the options as needed.

   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 this table:

Parameter Scope	Scope Description
Global	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.

Parameter Scope	Scope Description
Device Specific	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. (Optional) Click the menu icon adjacent to the text box and provide a default value and a description. Cisco SD-WAN Manager applies the default value of the parameter to the device while deploying the configuration group. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Default	The default value is shown for parameters that have a default setting.

6. Click **Save**.

Add a Subfeature

1. Select a feature to edit and click the + icon to add subfeatures, where applicable.

   The **Add Feature** pane appears with a list of applicable subfeatures that you can add.

2. Choose a feature to add to the profile.

   Cisco SD-WAN Manager adds the feature to the profile and represents it as a tree structure.

3. Configure the subfeature by choosing **+ Add New** from the drop-down menu and click **Save**.

   The subfeature appears as a child under the parent feature. For example, Ethernet Interface is a subfeature of Transport VPN and Object Tracker and Object Tracker Group are subfeatures of the Service VPN feature.

Note Some subfeatures that you configure such as Route Policy or Object Tracker don't appear in the tree structure after creation. This is because these subfeatures apply to certain features during configuration and are available in the context of those features in a configuration group. For example, the ACL IPV4 subfeature is available in the **ACL** drop-down list for **ACL IPv4 ingress** or **ACL IPv4 egress** parameters in the Ethernet Interface feature.

You can view these subfeatures by clicking the **Manage All Features** icon adjacent to the **+ Add New Feature** menu.

Add Devices to a Configuration Group

After creating a configuration group, you can add devices to the group in one of these ways:

- Add the devices manually.
- Use rules to automatically add devices to the group.

Add Devices to a Configuration Group Manually

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click a configuration group from the available list.
3. Click the **+ Add** option adjacent to **Associated** in the **Deployment** area.
4. Click **Associated Devices**, and then click **Add Devices**.

   The **Add Devices to Configuration** workflow starts.
5. 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 the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click a configuration group from the available list.
3. Click the **+ Add** option adjacent to **Associated** in the **Deployment** area.
4. Click **Add and Edit Rules**.

   The **Automated Rules** sidebar is displayed.
5. In the **Rules** section, choose values for the following options:
   - **Rule Conditions**: Choose one of the two rules and configure the conditions: **Match All** or **Match Any**.
   - Choose one of these operators:
     - **Equals**
     - **Not equals**
     - **Contains**
     - **Not contains**
     - **Starts with**
     - **End with**

Note You cannot create a new rule if it conflicts with an existing rule.

6. Click **Apply**.

   Based on the rule, a list of devices that will be added to or removed from the configuration group appears.

7. Click **Confirm** to apply the changes.

Remove Devices from a Configuration Group

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.

You can 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.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click a configuration group from the available list.
3. Click the pencil icon (with the count of associated devices) adjacent to **Associated** in the **Deployment** area.
4. In the **Devices** table, choose the devices to remove from the configuration group.
5. Click **Save**.

Deploy a Configuration Group

The option to deploy a configuration group is available only after you:

1. create the mandatory features such as **System Profile** and **Transport & Management Profile**.

   For more information about creating profiles, see Add a Feature Profile.

2. configure and add features to the mandatory profiles, and
3. associate devices to the configuration group.

To deploy a configuration group:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click the **Configuration Groups** tab.
3. Click a configuration group from the available options.
4. Click the **Add** option next to **Associated** under **Deployment**.
5. Choose the devices to associate to the configuration group and click **Save**.
6. Click **Deploy** and follow the instructions in the Deploy Configuration Group workflow.

Edit a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click the ellipsis icon adjacent to the configuration group name and choose **Edit** to edit the name and description of the configuration group, or in case of dual routers, to edit the tags of the routers.

   Alternatively, click a configuration group to expand it and click the pencil icon to edit.

You can edit the various settings of a configuration group, such as adding or editing feature profiles, devices, or associating and deploying devices to a configuration group by clicking a configuration group.

View Configuration Groups

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** and use one of the filters to view certain cofiguration groups based on these categories:

- **Last Updated**: Choose a time range from the drop-down list to view configuration groups that are updated within that time range.
- **Status**: Choose one or more of these categories from the drop-down list
  - **All Devices in Sync**: Displays configuration groups with all the devices in sync.
  - **Has Out of Sync Devices**: Displays configuration groups with devices that are out of sync.
  - **No Devices Associated**: Displays configuration groups without any associated devices.

Copy a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click the ellipsis icon adjacent to the configuration group name and choose **Copy**.
3. In the **Copy Configuration Group** dialog box, enter these:

Field	Description
Name	Enter a name for the new configuration group.
Description	Enter a description for the new configuration group.

4. Click **Create**.

   Cisco SD-WAN Manager creates the new configuration group.

Import a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Import**.
3. Choose a tar.gz file from your local storage to import to Cisco SD-WAN Manager.
4. Click **Open**.
5. The **Device Group** page displays the import status.
6. Click the logs icon in the **Action** column to view the logs of the import.

Export a Configuration Group

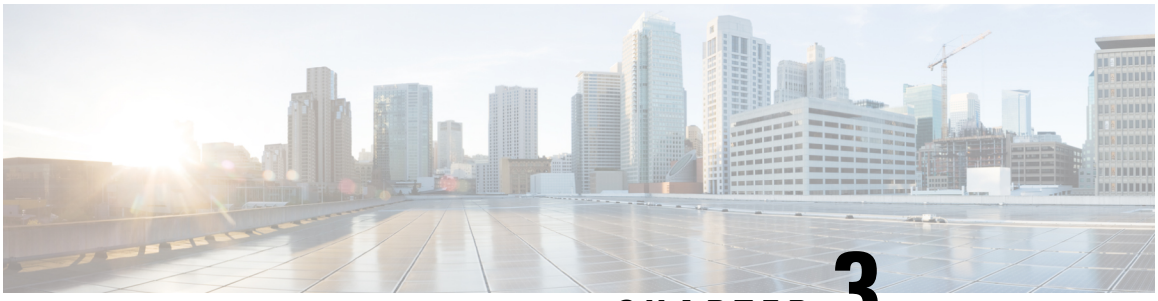
1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Export** and click the **Configuration Group** tab.
3. Choose one or more configuration groups to export.

   You can choose multiple configuration groups, policy groups, and topologies and export them as a single tar.gz file.
4. Click **Export**.
5. Based on your selection, Cisco SD-WAN Manager downloads the configuration group to your local storage as a tar.gz file.

Delete a Configuration Group

Before deleting a configuration group, ensure that there are no devices associated with that configuration group. For more information about removing devices from a configuration group, see Remove Devices from a Configuration Group.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click the ellipsis icon adjacent to the configuration group name and choose **Delete**.
3. In the confirmation dialog box, click **Yes**.



CHAPTER 3

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** > **Validator**.
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 2: 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 ([]).

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, only the **Cellular Gateway** in the configuration groups supports rollback timer.

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 30.

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.

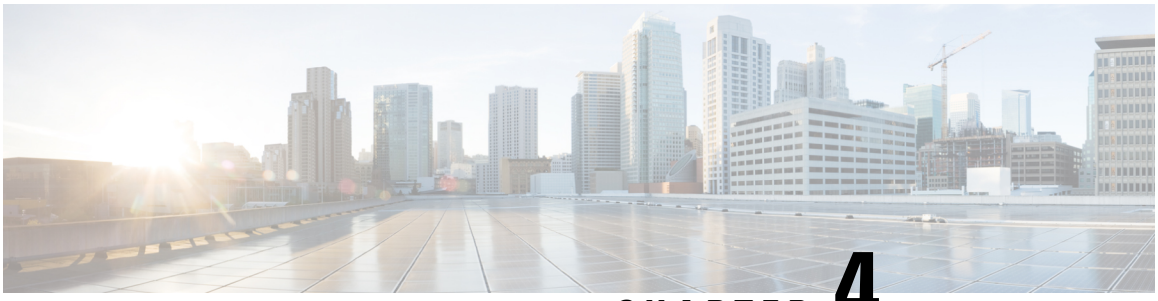
   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click a feature profile to open it.
4. Click **…** adjacent to a feature and choose **Edit 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**.



CHAPTER 4

Configuration Group Workflows

Use the Configuration Group Workflows

Before You Begin

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

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

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**.

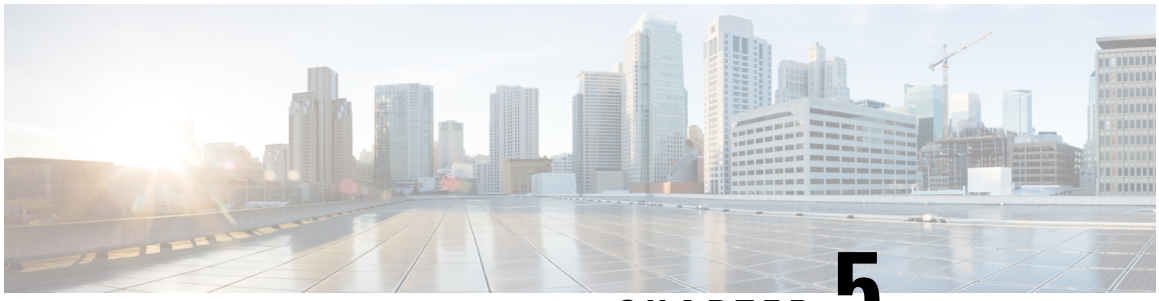
b. Resume an in-progress workflow: In the **In-progress** section, click **Custom Configuration Group**.

The workflow generates the following components:

- A configuration group
- Three feature profiles: System profile, transport and management profile, and service profile

PART II

Part Cisco IOS XE Devices (SD-WAN)



CHAPTER 5

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.
Transport Gateway	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enable transport gateway functionality for the device. A transport gateway connects routers that may or may not have direct connectivity. One common use case for transport gateways is to provide connectivity between routers in disjoint networks, such as between public and private WANs. Another use case for transport gateway functionality is to use a transport gateway as the hub in a hub-and-spoke topology.

Controller Settings

Field	Description
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
Affinity Group Number	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter an affinity group number. Range: 1 through 63
Affinity Group Number for VRFs and **Range of VRFs**	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter an affinity group number for a specific range of VRFs. You can click + to configure an affinity group number for additional VRF ranges. Range for affinity group: 1 through 63 Range for VRFs: 1 through 65531
Affinity Group Preference Auto	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Configure automatic affinity preference order. When you use this, a device prefers routes with a lower affinity group number. In this case affinity group numbers are not treated as arbitrary tags, but instead signify route priority, where a lower affinity group number means higher priority.
Affinity Group Preference	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter a comma-separated list of affinity group numbers. In a Multi-Region Fabric scenario, this determines the order of preference for connecting to a gateway. Affinity group preference also used for path filtering when using the **filter route outbound affinity-group preference** command on a Cisco SD-WAN Controller. Range for affinity groups: 1 through 63

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

Fabric Security

Note Before the Cisco Catalyst SD-WAN Manager Release 20.12.1, Fabric Security was called 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 Fabric 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)

Field	Description
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
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.
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
Role	• Border routers: Use **border-router**. • Edge routers: Use **edge-router**.

Parameter Name	Description
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

Advanced

Parameter Name	Description
Management Region	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1 Enable a management region in a Multi-Region Fabric scenario.
Management VPN	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1 Enter a VPN in which devices can connect to a management gateway. Range: 1 through 65531
Enable as Management Gateway	Enable management gateway functionality for the device. A management gateway is a device that other devices in the overlay (including edge devices and border routers, and devices enabled as transport gateways) connect to. All these devices establish direct tunnels with the management gateway.
Enable Migration Mode to Multi-Region Fabric	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.
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 Cisco IOS XE Catalyst SD-WAN device advertises routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistribute the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE Catalyst SD-WAN device can have up to four TLOCs, and by default advertises each route-TLOC tuple to the Cisco Catalyst SD-WAN Controller. If a local site has two Cisco IOS XE Catalyst SD-WAN devices, a Cisco Catalyst SD-WAN Controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised. 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 Cisco IOS XE Catalyst SD-WAN device 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. Range: 1 through 255
OMP Admin Distance Ipv6	To advertise a route over OMP, configure the OMP administrative distance for the IPv6 address lower than the leaked route administrative distance. Range: 1 through 255

Timers

Field	Description
Graceful Restart(In Second)	Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart. 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.
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.

Best Path

Field	Description
Treat Hierarchical and Direct Paths Equally	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, if using secondary regions, enable this option to enable packets to use all available paths rather than only direct paths. By default, when a direct path is available to reach a destination, the overlay management protocol (OMP) enables only the direct path to the routing forwarding layer because the direct path uses fewer hops. This logic is part of route optimization. The result is that the forwarding layer, which includes application-aware routing policy, can only use the direct path. **Treat Hierarchical and Direct Paths Equally** disables this comparison of the number of hops so that traffic can use either the direct secondary-region path (fewer hops) or the primary-region path (more hops). When you disable the comparison of the number of hops, OMP applies equal-cost multi-path routing (ECMP) to all routes, and packets can use all available paths.
Transport Gateway Path Behavior	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose one of the following: • **Prefer Transport Gateway Path**: For devices that can connect through a transport gateway, use only the transport gateway paths, even if other paths are available. • **Do ECMP Between Direct and Transport Gateway Paths**: For devices that can connect through a transport gateway and through direct paths, apply ECMP to all available paths.
Site Type	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) If you configure a value for **Transport Gateway Path Behavior**, this field appears. Optionally, choose one or more site types to apply the transport gateway path behavior only to those site types.

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**.

Remote Access

The following table describes options to specify the name and description for the remote access feature.

Field	Description
Type	Choose Remote Access feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Connection Type	Choose the connection type from the following: • **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.
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**.

Field	Description
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.
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

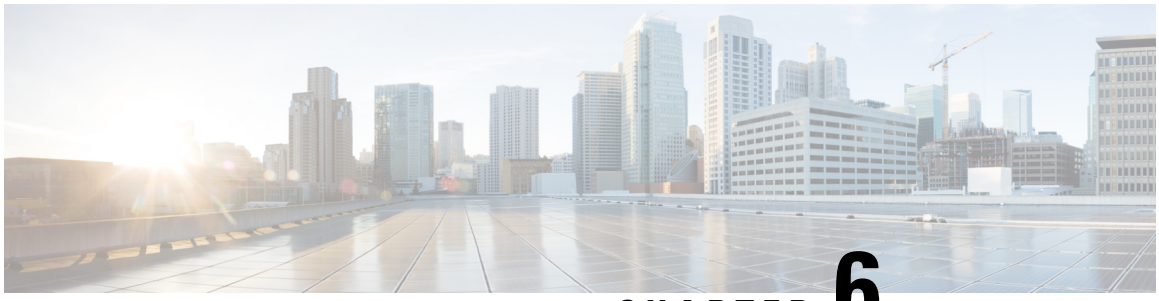
Field	Description
Shutdown	By default, SNMP is enabled.
Contact Person	Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN device. It can be a maximum of 255 characters.
Location of Device	Enter a description of the location of the device. It 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.
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

Field	Description
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.
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.

Field	Description
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.
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 6

Transport and Management

The Transport and Management Profile helps you configure a VRF at WAN level. 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.

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.

Field	Description
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES-encrypted key. From Cisco Catalyst SD-WAN Manager Release 20.15.1, when you enter the password as clear text, Cisco SD-WAN Manager encrypts the password. When you view the configuration preview, the password appears in its encrypted form.
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.

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.
Associated IPv6-Tracker/IPv6-Trackergroup	Choose an IPv6- 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

Field	Description
Tunnel Interface	Enable this option to create a tunnel interface.

Field	Description
Per-tunnel QoS	Enable this option to apply a Quality of Service (QoS) policy on individual tunnels.
Color	Choose a color for the TLOC.
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.
Groups	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
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
Port Hop	Enable port hopping. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). 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

Field	Description
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.
CTS SGT Propagation	Enable CTS SGT propagation on an interface.
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**
Encapsulation	

Field	Description
Encapsulation*	Choose an encapsulation type: • **gre**: Use GRE encapsulation on the tunnel interface. • **ipsec**: Use IPsec encapsulation on the tunnel interface. **Note** 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. When you choose **gre**, the following fields appear: • **GRE Preference**: Enter 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 When you choose **ipsec**, the following fields appear: • **IPSEC Preference**: Enter 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
Multi-Region Fabric **Note** These options appear only when Multi-Region Fabric is enabled.	
Connect to Core Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to a border router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the access region and core region. • **Keep Exclusive to Core Region**: Use the interface only for the core region.

Field	Description
Connect to Secondary Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to an edge router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the primary and secondary regions. • **Keep Exclusive to Secondary Region**: Use the interface only for the secondary region.

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)

Field	Description

Add Multiple NAT	Choose the NAT type:
	• **Interface**: This is the default value.
	• **Pool**: Configure the following:
	  • **Pool ID**: 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.
	  • **Range Start**: Enter a starting IP address for the NAT pool.
	  • **Range End**: Enter a closing IP address for the NAT pool.
	  • **Prefix length**: Specify the maximum number of source IP addresses that can be NATed in 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
	• **Loopback**: Provide a value for the NAT inside source loopback interface.

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.

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.

Field	Description
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.

GRE

Use the GRE feature for all Cisco IOS XE Catalyst SD-WAN devices.

The following tables describe the options for configuring the GRE feature.

Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface. Range: 1 through 255.
Interface Description	Enter a description of the GRE interface.
Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport VPN. Default: No
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

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 IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None

Field	Description
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

IPSEC

Use the IPsec feature to configure IPsec tunnels on Cisco IOS XE Catalyst SD-WAN devices that are being used for Internet Key Exchange (IKE) sessions.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the following table:

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. 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, type 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 appears for parameters that have a default setting.

The following tables describe the options for configuring the VPN Interface IPsec feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Basic Configuration

Field	Description
Interface Name	Enter the name of the IPsec interface.
Description	Enter a description of the IPsec interface.

Field	Description
Tunnel Mode	Choose from one of the following IPsec tunnel modes: • **ipv4**: IPsec tunnel with IPv4 overlay and IPv4 underlay. IPv4 underlay is the default value. • **ipv6**: IPsec tunnel with IPv6 overlay and IPv6 underlay. • **ipv4-v6overlay**: IPsec tunnel with IPv6 overlay and IPv4 underlay.
Multiplexing	Choose **Yes** to enable multiplexing, if there is a tunnel in the transport VPN. Default: No
Interface Address	Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.
Mask	Enter the subnet mask.
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.
Associated Tracker / Tracker Group	Choose a tracker or a tracker group from the drop-down list to associate with the IPsec tunnel.
Tunnel Source	Enter the source of the IPsec interface: • **IP Address**: Enter the source IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address that is based on your selection in the **Tunnel Mode** option. This address is on the local router. • **Interface**: Enter the physical interface in the **IPsec Source Interface** field, which is the source of the IPsec tunnel.

Tunnel Destination	Enter the destination IP address of the IPsec tunnel interface. This address is on a remote device.
	• **Address**: Enter the destination IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address based on your selection in the **Tunnel Mode** option.
	• **Application**: Choose an application from the drop-down list.
	  • **None**
	  • **Sig**

Internet Key Exchange

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1

Field	Description
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote endpoint identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you choose IKEv2.

IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds (1 hour)

Field	Description
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024 bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048 bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072 bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096 bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**

Advanced

Field	Description
Associated VPN	Select a VPN from the drop-down list to associate with the IPsec tunnel.
Tunnel Route Via	Specify the tunnel route details to steer the application traffic through. **Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Shutdown	Click **Off** to enable the 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 3: 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.

Field	Description
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.
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 4: IPv6 Tracker Group

Field	Description
Tracker Name	Enter a tracker name.
Tracker Elements	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to an interface.
Tracker Boolean	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**. **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.

Managed Cellular Activation - eSIM Controller

You can associate a Managed Cellular Activation cellular profile with a Managed Cellular Activation cellular controller.

1. Enter a feature name and description for **Managed Cellular Activation-eSIM Controller**.
2. Configure the Cellular ID based on the slot configuration of your device (for example, Cisco Catalyst 8200 Series, Cisco Catalyst 8300 Series, and ISR1000). Enter the interface slot and port number in which the cellular PIM card is installed.
3. To associate a Managed Cellular Activation cellular profile with a Managed Cellular Activation cellular controller, in the **Attach Profile** and **Data Profile** sections, choose the cellular profile.
4. Click **Save**.

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	
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	

Field	Description
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**

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
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.
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.

Parameter Name	Description
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	
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.

Parameter Name	Description
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. 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
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 Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes

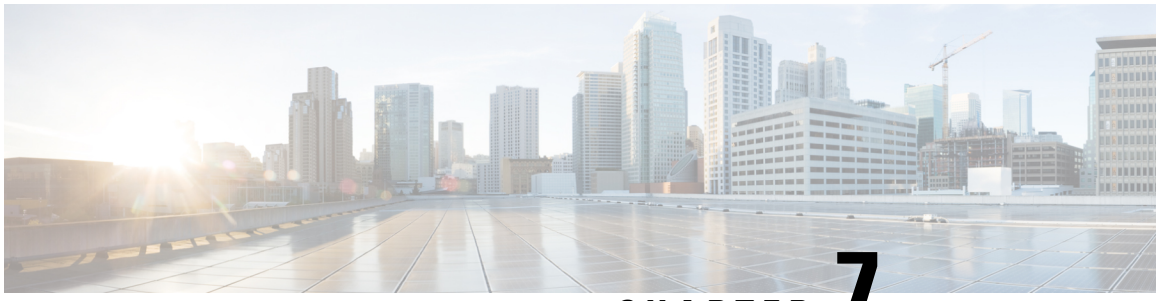
ACL

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.
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.

Parameter Name	Description
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).



CHAPTER 7

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.
	Note From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, an AppQoE cluster can either operate on IPv4 protocol or IPv6 protocol in the control plane.
	• **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.

Advanced

Field	Description
DRE Optimisation	Enable DRE optimisation

Field	Description
Resource Profile	Choose **Global** to choose a profile size from the options available in the drop-down list. Choose **Default**to apply the default DRE profile size for the device. Choose **Device Specific** to enter a value for the profile.

BGP Routing

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

Table 5: 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 6: 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.
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.

Field	Description
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.
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	

Field	Description
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 7: Neighbor

Field	Description
IPv4 Settings	
Address*	Specify the IP address of the BGP neighbor.
Description	Enter a description of the BGP neighbor.
Remote AS*	Enter the AS number of the remote BGP peer.
Interface Name	Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface.
Allowas in Number	Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used.
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.

Field	Description
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.
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.

BGP Routing

This feature helps you configure the Border Gateway Protocol (BGP) routing in VPN 0 or the WAN VPN.

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and choose one of the following:

Basic Configuration

Field	Description
AS Number	Enter the local AS number.
Router ID	Enter the BGP router ID, in decimal four-part dotted notation.
Propagate AS Path	Enable this option to carry BGP AS path information into OMP.

Field	Description
Propagate Community	Enable this option to propagate BGP communities between Cisco Catalyst SD-WAN sites, across VPNs using OMP redistribution.
External Routes Distance	Specify the BGP route administrative distance for routes learned from other sites in the overlay network. 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	
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.

Field	Description
Network	
Network Prefix*	Enter a network prefix to be advertised by BGP. The network prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0.
Aggregate Address	
Aggregate Prefix*	Enter the prefix of the addresses to aggregate for all BGP sessions. The aggregate prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0.
AS Set Path	Enable this option to generate set path information for the aggregated prefixes.
Summary Only	Enable this option to filter out more specific routes from BGP updates.
Table Map	
Policy Name	Enter the route map that controls the downloading of routes. 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 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.

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.

MPLS Interface

Field	Description
Interface Name*	Enter a name for the MPLS interface.

Neighbor

Field	Description
IPv4 Settings	
Address*	Specify the IP address of the BGP neighbor.

Field	Description
Description	Enter a description of the BGP neighbor.
Remote AS*	Enter the AS number of the remote BGP peer.
Interface Name	Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface.
Allows in Number	Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used.
AS Override	Enable this option to replace the AS number of the originating router with the AS number of the sending BGP router.
Shutdown	Disable this option to enable BGP for the VPN.
Advanced Options	
Next-Hop Self	Enable this option to configure the router to be the next hop for routes advertised to the BGP neighbor.
Send Community	Enable this option to send the BGP community attribute of the local router to the BGP neighbor.
Send Extended Community	Enable this option to send the BGP extended community attribute of the local router to the BGP neighbor.
EBGP Multihop	Set the time to live (TTL) for BGP connections to external peers. 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)

Field	Description
Hold Time (seconds)	Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor, to override the global hold time. 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.

Dual Router High Availability

This feature helps you configure the high-availability feature in Cisco Catalyst SD-WAN using the Cisco IOS XE Catalyst SD-WAN devices.

The following table describes the options for configuring the high-availability feature on Cisco IOS XE Catalyst SD-WAN devices.

Basic Configuration

Field	Description
Name	Enter a name for the high availability feature profile.
Description	Enter a description for the high availability feature profile.
VPN	Displays all available service-side VPNs.
EdgeDevice_01	When selected, the Cisco IOS XE Catalyst SD-WAN device is set as active for the specific VPN, while the other corresponding device is configured as standby.
EdgeDevice_02	When selected, the Cisco IOS XE Catalyst SD-WAN device is set as active for the specific VPN, while the other corresponding device is configured as standby.
None	Set the status to **None** for VPNs that are not configured for High Availability.
Preempt to home router	Click to allow the configured active Cisco IOS XE Catalyst SD-WAN device to automatically reclaim the active role upon recovery from a failure.
Optimize paths after switchover	Click to enable OMP Affinity to optimize routing paths after a failover.

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	

Parameter Name	Description
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.
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.

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.

GRE

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

The following tables describe the options for configuring the service VPN Interface GRE feature.

Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface, in the format **grenumber**. The value for **number** can be from 1 through 255.
Interface Description	Enter a description of the GRE interface.
Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

IPSEC

Field	Description
IPsec Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

Advanced

Field	Description
Shutdown	Click **Off** to enable the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv6 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of the IPv4 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None

Field	Description
IPv6 TCP MSS	Specify the maximum segment size (MSS) of the IPv6 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

IPSEC

Use the IPsec feature to configure IPsec tunnels on Cisco IOS XE Catalyst SD-WAN devices, used for Internet Key Exchange (IKE) sessions.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. 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, type 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.

The following tables describe the options for configuring the VPN Interface IPsec feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Basic Configuration

Field	Description
Interface Name	Enter the name of the IPsec interface.
Description	Enter a description of the IPsec interface.
Tunnel Mode	Choose from one of the following IPsec tunnel modes: • **ipv4**: IPsec tunnel with IPv4 overlay and IPv4 underlay. IPv4 underlay is the default value. • **ipv6**: IPsec tunnel with IPv6 overlay and IPv6 underlay. • **ipv4-v6overlay**: IPsec tunnel with IPv6 overlay and IPv4 underlay.
Interface Address	Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.
Mask	Enter the subnet mask.
Tunnel Source	Enter the source of the IPsec interface: • **IP Address**: Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.. This address is on the local router. • **Interface**: Enter the physical interface that is the source of the IPsec tunnel.
Tunnel Destination	Enter the destination of the IPsec interface: • **Address**: Enter the destination IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list. This address is on a remote device. • **Application**: Choose an application from the drop-down list. • None • Sig
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.

Field	Description
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

Internet Key Exchange

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IPsec Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel

Field	Description
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**

Advanced

Field	Description
Associated VPN	Select a VPN from the drop-down list to associate with the IPsec tunnel.
Tunnel Route Via	Specify the tunnel route details to steer the application traffic through. **Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.

Field	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Shutdown	Click **Off** to enable the interface.

Multicast

The Cisco IOS XE Catalyst SD-WAN multicast overlay software extends Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) over the Cisco Catalyst SD-WAN overlay using Overlay Management Protocol (OMP). Protocol Independent Multicast Sparse-Mode (PIM-SM) is deployed in the customer VPNs, and the Cisco IOS XE MVPN is used to integrate PIM in customer VPNs and OMP in the overlay. The OMP replicator is used in overlay multicast to optimize the multicast distribution tree across the overlay topology. The Cisco IOS XE Catalyst SD-WAN router supports IGMPv2 and IGMPv3 reports and advertises receiver's multicast interest to remote Cisco Catalyst SD-WAN routers using OMP. Depending on the level of optimization required, the Cisco Catalyst SD-WAN routers join or prune to or from the replicators, and replicators use OMP to relay the join or prune to the Cisco Catalyst SD-WAN router providing overlay connectivity to the PIM-RP or source.

The Cisco IOS XE Catalyst SD-WAN overlay multicast network supports the following protocols:

- Protocol Independent Multicast (PIM)
- Internet Group Management Protocol (IGMP)
- MSDP

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. 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 Multicast feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Table 8: Basic Configuration

Field	Description
SPT Only	Enable this option to ensure that the Rendezvous Points (RPs) can communicate with each other using the shortest-path tree.
Local Replicator	Enable this option to configure the Cisco IOS XE Catalyst SD-WAN device as a multicast replicator.
Threshold	Specify a value. Optional, keep it set to the default value if you are not configuring a replicator.

Table 9: PIM

Field	Description
Source Specific Multicast (SSM)	Enable this option to configure SSM.

Field	Description
ACL	Specify an access control list value. An access control list allows you to filter multicast traffic streams using the group and sometimes source IPv4 or IPv6 addresses. Configure an IPv4 access control list using a standard or extended access list and attach it to your device before enabling PIM. You must have created a valid standard or extended ACL before using the ACL in your multicast configuration. **Note** You cannot configure an ACL for a PIM feature template using Cisco SD-WAN Manager. You must configure the ACL using a CLI add-on template. For information on configuring ACL using the CLI add-on template, see the section **Configure an ACL for Multicast Using a CLI Add-On Template** in chapter **Multicast Overlay Routing** of the Cisco Catalyst SD-WAN Routing Configuration Guide.
SPT Threshold	Specify the traffic rate, in kbps, at which to switch from the shared tree to the shortest-path tree (SPT). Configuring this value forces traffic to remain on the shared tree and travel via the RP instead of via the SPT.
Add Interface	
Interface Name	Enter the name of an interface that participates in the PIM domain, in the format **ge** *slot /port*.
Query Interval(sec)	Specify how often the interface sends PIM query messages. Query messages advertise that PIM is enabled on the router.
Join/Prune Interval(sec)	Specify how often PIM multicast traffic can join or be removed from a rendezvous point tree (RPT) or shortest-path tree (SPT). Cisco IOS XE Catalyst SD-WAN device send join and prune messages to their upstream RPF neighbor.
How do you want to configure your Rendezvous Point (RP) Cisco IOS XE SD-WAN supports the following modes:	
Static	Click this check box to a specify the static IP address of a rendezvous point (RP).
Add Static RP	
IP Address	Specify the static IP address of a rendezvous point (RP).
ACL	Specify an ACL value.

Field	Description
Override	Enable this option for cases when dynamic and static group-to-RP mappings are used together and there is an RP address conflict. In this case, the RP address configured for a static group-to-RP mapping takes precedence. If you do not enable this option, and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
Auto RP	Click this check box to enable reception of PIM group-to-RP mapping updates. This enables reception on the Auto-RP multicast groups, 224.0.1.39 and 224.0.1.40.
RP Announce	Click this check box to enable transmission of Auto-RP multicast messages.
RP Discovery	Click this check box to enable Auto-RP automatic discovery of rendezvous points (RPs) in the PIM network so that the router can serve as an Auto-RP mapping agent. An Auto-RP mapping receives all the RPs and their respective multicast groups and advertise consistent group-to-RP mapping updates.
Interface	Specify the source interface for Auto-RP RP Announcements or RP Discovery messages.
Scope	Specify the IP header Time-to-Live (TTL) for Auto-RP RP Announcements or RP Discovery messages.
PIM-BSR	Configure a PIM BSR.
RP Candidate	
Interface Name	Choose the interface that you used for configuring the PIM feature template.
Access List	Add an access list value if you have configured the access list with a value.
Interval	Add an interval value if you have configured the interval with a value.
Priority	Specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device.
BSR Candidate (Maximum: 1)	
Interface Name	Chose the same interface from the drop-down list that you used for configuring the PIM feature template.
Hash Mask Length	Specify the hash mask length. Valid values for hash mask length are 0–32.
Priority	Specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device.
RP Candidate Access List	Add a value if you have configured the RP candidate access list with a value. An RP candidate uses a standard ACL where you can enter the name for the access list.

Table 10: IGMP

Field	Description
Add IGMP	
Interface	Enter the name of the interface to use for IGMP. To add another interface, click **Add**.
Version	Specify a version number. Optional, keep it set to the default version number.
Group Address	Enter a group address to join a multicast group.
Source Address	Enter a source address to join a multicast group.
Add	Click **Add** to add the IGMP for the group.

Table 11: MSDP

Field	Description
Originator-ID	Specify the ID of the originating device. This ID is the IP address of the interface that is used as the RP address.
Connection Retry Interval	Configure an interval at which MSDP peers will wait after peering sessions are reset before attempting to re-establish the peering sessions.
Mesh Group	
Mesh Group Name	Enter a mesh group name. This configures an MSDP mesh group and indicates that an MSDP peer belongs to that mesh group. **Note** All MSDP peers present on a device that participate in a mesh group must be in a full mesh with all other MSDP peers in the group. Each MSDP peer on each device must be configured as a peer using the **ip msdp peer** command, and as a member of the mesh group using the **ip msdp mesh-group** command.
Peer-IP	Configure an MSDP peer specified by an IP address.
Advanced Settings	
Connect-Source Interface	Enter the primary address of a specified local interface that is used as the source IP address for the TCP connection.
Peer Authentication Password	Enables MD5 password encryption for a TCP connection between two MSDP peers. **Note** MD5 authentication must be configured with the same password on both MSDP peers. Otherwise, a connection between them cannot be established.
Keep Alive	Configure an interval at which an MSDP peer will send keepalive messages.

Field	Description
Hold-Time	Configure an interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them as down.
Remote AS	Specifies the autonomous system number of the MSDP peer. This keyword and argument are used for display purposes only.
SA Limit	Limits the number of SA messages allowed in the SA cache from the specified MSDP.
Default Peer	Configure a default peer from which to accept all MSDP SA messages.

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	

Field	Description
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	
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 `geslot/port` or `loopback number`.

Field	Description
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
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.

Field	Description
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

Field	Description
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

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 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.

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.

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	

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.

Object Tracker

Use the object tracker feature to configure an object tracker.

Basic Settings

Parameter Name	Description
Tracker Type*	
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.
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.

Field	Description
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	

Field	Description
Protocol	Choose a protocol to configure route advertisements to OMP, for this VPN: • **bgp** • **ospf** • **ospfv3** • **connected** • **static** • **network** • **aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway. • **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	

Field	Description
Protocol	Choose a protocol to configure route advertisements to OMP, for this VPN: • **BGP** • **OSPF** • **Connected** • **Static** • **Network** • **Aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway.
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	
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.

Field	Description
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	
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.
	• **Interface**: When you choose this option, the following fields appear:
	  • **Interface Name**: Choose IPv6 interface name for the IPsec tunnel.
	  • **Next Hop**: Enter the IPv6 address and the administrative distance for the next hop.

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	
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.

Field	Description
Prefix Length*	Enter the NAT pool prefix length.
Range Start*	Enter a starting IP address for the NAT pool.
Range End*	Enter a closing IP address for the NAT pool.
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.

Field	Description
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in global VPN)	
Protocol*	Choose a protocol from the available options to redistribute the leaked routes.
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.

SVI Interface

This feature helps you configure a switch virtual interface (SVI) to configure a VLAN interface.

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and choose one of the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template. 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 tables describe the options for configuring the SVI Interface feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Associated VPN: VPN*	Choose a VPN.

Basic Configuration

Field	Description
Shutdown	Enable or disable the VLAN interface.
VLAN Interface Name*	Enter a name for the VLAN interface. The name must contain a minimum of five characters. The name must be in the following format: `^Vlan(([1-9]\d|\d)/){0,2}(0|[1-9]\d*)([:|\.][1-9]\d*)?`
Interface Description	Enter a description for the interface.

Field	Description
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 9216 Default: 1500 bytes
IP MTU	Enter the maximum transmission unit (MTU) size of IP packets sent on an interface. Range: 576 through 9216 Default: 1500 bytes
Configure IPV4 Address	
IPv4 Address Prefix*	Enter the IPv4 address for the interface.
List of DHCP helper addresses*	Enter up to eight IP addresses for DHCP servers in the network to have the interface be a DHCP helper. Separate each address with a comma. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Configure IPV4 Secondary Address	
Secondary IP Address*	Enter up to four secondary IP addresses.
Configure IPV6 Address	
IPV6 address*	Enter the IPv6 address for the interface.
Configure IPV6 Secondary Address	
Address*	Enter up to four secondary IP addresses.
Configure IPV6 DHCP Helper	
Address*	Enter an IP address for DHCP servers in the network to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
VPN	VPN ID for the DHCP helper address.

ACL

Field	Description
Configure Access List V4	
Direction*	Choose a direction of the ACL: **in** or **out**.
Name of ACL*	Enter the name of the access list.
Configure Access List V6	

Field	Description
Direction*	Choose a direction of the ACL: **in** or **out**.
Name of ACL*	Enter the name of the access list.

VRRP

Field	Description
Configure VRRP	
Group ID*	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. 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.
Prefix List*	Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.
Add VRRP IP Address Secondary	
Address*	Enter an IP address for the secondary VRRP router.

Field	Description
TLOC Preference Change	Enable or disable this option to set whether the TLOC preference can be changed or not.
Add VRRP Tracking Object	
Tracker Id*	Enter the interface object ID or object group tracker ID.
Track Action*	Choose one of the options: • **decrement** • **shutdown**
Decrement Value	Enter a decrement value. Range: 1-255 From Cisco vManage Release 20.10.1, this option is enabled only when you choose **decrement** in **Track Action**.
Configure VRRP IPv6	
Group ID*	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. 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.

Field	Description
Track Prefix List	Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
Add VRRP IPv6 Primary	
IPv6 Link Local*	Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8.
Prefix	Enter the IPv6 address of the primary VRRP router.

ARP

Field	Description
Configure ARP	
IP Address*	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address*	Enter the MAC address in colon-separated hexadecimal notation.

Advanced

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1960 bytes Default: None
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 (20 minutes)

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/ICMPv6 Redirect Disable	ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. By default, an interface allows ICMP redirect messages.

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`.

Field	Description
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.
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.

Field	Description
Pae Enable	The Cisco Catalyst SD-WAN device acts as a port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port.
MAC Authentication Bypass	Enable this option to allow MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-IEEE 802.1X–compliant clients using a RADIUS server.
Host Mode	Choose whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients). • **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
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**
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

Field	Description
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. The tracker name must not contain capital letters and special characters.
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

Field	Description
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.

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
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.

Parameter Name	Description
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.
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.

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.
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	
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.

Parameter Name	Description
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
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**

Parameter Name	Description
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. 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 Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes

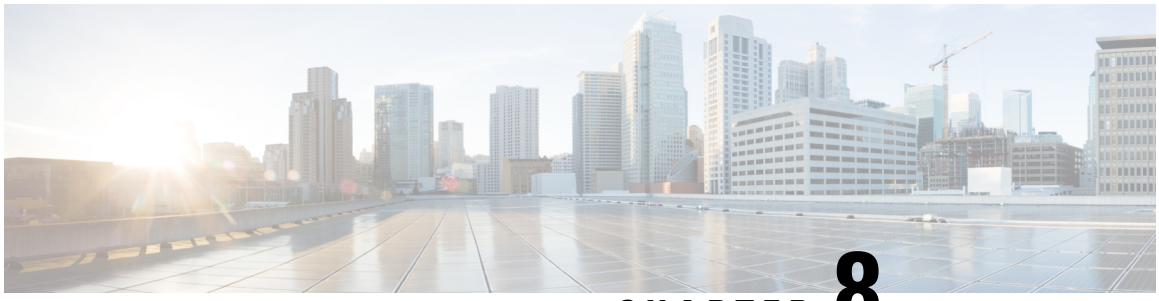
ACL

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.
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

Parameter Name	Description
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).



CHAPTER 8

Policy Object Profile

A Cisco Catalyst SD-WAN policy is made up of at least one list, a policy definition, and an application. The list identifies values, the policy definition defines actions, and the application defines where the policy is applied. The policy object profile has lists such as AS path, class map, data prefix, mirror, policer, and so on.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, when the policy objects are more than 50, the list is paginated to ease the configuration of policy object profiles.

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.
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.

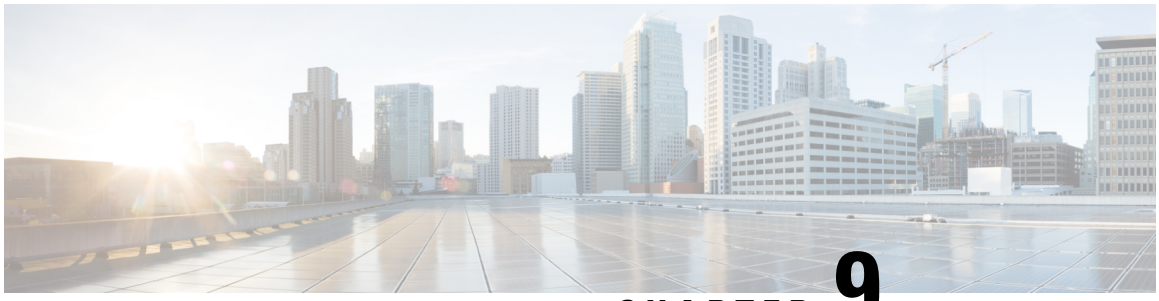
Field	Description
Add Expanded Community	Specifies the standard community. the options are: • *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the Internet community. This 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 9

Cisco Unified Communications Voice Profile

Table 12: Feature History

Feature Name	Release Information	Description
Support for Cisco Unified Communications DSP Farm Feature	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature introduces the UC voice profile with support for the DSP farm feature.
Support for Additional Unified Communications Features	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature adds support for the following features in the UC voice profile: • Analog Interface • Call Routing • Digital Interface • Media Profile • SRST • Server Group • Supervisory Disconnect • Translation Profile • Translation Rule • Trunk Group • Voice Global • Voice Tenant

Analog Interface

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Analog Interface feature provides options for configuring parameters for a voice card analog interface.

If you are using an NIM-2FX/4FXOP, SM-X-24FXS/4FXO, SM-X-16FXS/2FXO, or SM-X-8FXS/12FXO combo card, configure two instances of this feature, one for FXS and one for FXO. Ensure that you use the same module location for each instance. When you deploy this feature, the configuration preview displays the correct port mapping for the FXS and FXO ports.

Note If you want to remove or replace the analog interface configuration on a device:

1. Delete all configuration instances for this feature (Basic, Station ID, Line Params, Tuning Params, DID Timer, Caller ID, Connection Plar, and Associations).
2. Add one Basic configuration instance with default settings.
3. Deploy this updated interface feature configuration to the device, which resets the analog interface configuration on the device.
4. Delete this feature or configure a new one.

The following tables describe the options for configuring the Analog Interface feature.

Field	Description	Cisco IOS CLI Equivalent
Name	Enter a unique name for the analog interface configuration. The name can contain any characters.	—
Description	Enter a description of the analog interface configuration.	**description** *string*
Voice Interface Templates	Choose a group of voice interface FXO or FXS analog ports to be provisioned.	—
Use DSP	Check this check box if you want to allow local calls between analog ports on the same device to use the built-in DSPs. Default: Unchecked	**no local-bypass**

Field	Description	Cisco IOS CLI Equivalent
Module Location	Choose the slot and sub-slot location for the group of analog ports to be provisioned. For a list of supported modules, see Supported Devices for Cisco Unified Voice Services using the Workflow Library or Configuration Groups.	**voice-card** *slot/subslot*

Basic

Field	Description	Cisco IOS CLI Equivalent
Add Basic	Click to configure the basic options for the group of analog ports. You can add multiple instances of these options so that you can configure different basic options for different ports.	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Signal Type	Choose the signal type that indicates an on-hook or off-hook condition for calls that the ports receive. Options are **LoopStart**, **GroundStart**, and **DID**. The **DID** option is available only for FXS voice interface templates.	**signal** {**groundstart** | **loopstart**}
DID Signal Mode	Applies only if you choose **DID** for an FXS voice interface template. Choose the mode for the DID signal type Options are **Delay Dial**, **Immediate**, and **Wink Start**.	**signal did** {**delay-dial** | **immediate** | **wink-start**}
Shutdown	Enable this option to shut down ports that are not being used.	**shutdown**
Description	Enter a description of this basic configuration.	**description** *string*
Action	Click the **Recycle Bin** icon to delete the corresponding Basic options instance.	—

Station ID

Field	Description	Cisco IOS CLI Equivalent
Add Station ID	Click to configure the station name and station number from which caller ID information is sent. You can add multiple instances of these options so that you can configure different station ID options for different ports.	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Station Name	Enter the name of the station. The station name can contain up to 50 letters, numbers, spaces, dashes (-), and underscores (_).	**station-id name** *name*
Station Number	Enter the phone number of the station in E.164 format. For example: 4085550111 The station number can contain up to 15 numbers.	**station-id number** *number*
Action	Click the **Recycle Bin** icon to delete the corresponding Station ID options instance.	—

Line Params

Field	Description	Cisco IOS CLI Equivalent
Line Params	Click and configure options for adjusting voice and tone parameters for the port or ports. You can add multiple instances of these options so that you can configure different line parameters options for different ports.	—

Field	Description	Cisco IOS CLI Equivalent
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Gain	Enter the amount of gain, in decibels (dB), for voice input. Range: Integers –6 through 14 Default: 0	**input gain** *decibels*
Attenuation	Enter the amount of attenuation, in dB, for transmitted voice output. Range: Integers –6 through 14 Default: 0	**output attenuation** *decibels*
Echo Canceller	Choose **Enable** to apply echo cancellation to voice traffic. This option is disabled by default.	**echo-cancel** *enable*
Voice Activity Detection (VAD)	Choose **Enable** to apply VAD to voice traffic. This option is disabled by default.	**vad**
Compand Type	Choose the companding standard to be used to convert between analog and digital signals in PCM systems. Options are **U-law** and **A-law**.	**compand-type** {**u-law** | **a-law**}
Impedance	Choose the terminating impedance for calls. Default: 600r	**impedance** {**600c** | **600r 900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}
Call Progress Tone	Choose the locale for the call progress tone.	**cptone** *locale*
Action	Click the **Recycle Bin** icon to delete the corresponding Line Params options instance.	—

Tuning Params

Field	Description	Cisco IOS CLI Equivalent
Tuning Params	Appears only when the **Signal Type** option in the **Basic** tab is configured as **LoopStart** or **GroundStart**. Click to configure the options for various tuning parameters. You can add multiple instances of these options so that you can configure different tuning parameter options for different ports.	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Pre Dial Delay	Applies only to FXO voice interface templates. Enter the time, in seconds, of the delay on the FXO interface between the beginning of the off-hook state and the initiation of DTMF signaling. Range: Integers 0 through 10 Default: 1	**pre-dial-delay** *seconds*
Supervisory Disconnect	Applies only to FXO voice interface templates. Choose the type of tone that indicates that a call has been released and that a connection should be disconnected: • **Signal**: A disconnect signal indicates a supervisory disconnect • **Anytone**: Any tone indicates a supervisory disconnect • **Dualtone**: A dual tone indicates a supervisory disconnect Default: signal	• Anytone: **supervisory disconnect anytone** • Signal: **supervisory disconnect** • Dualtone: **supervisory disconnect dualtone** {**mid-call** | **pre-connect**}

Field	Description	Cisco IOS CLI Equivalent
Dial Type	Applies only to FXO voice interface templates. Choose the dialing method for outgoing calls: • **dtmf**: Dual-tone multifrequency dialer • **pulse**: Pulse dialer • **mf**: Multifrequency dialer Default: dtmf	**dial-type** {**dtmf** | **pulse** | **mf**}
Timing Sup-Disconnect	Applies only to FXO voice interface templates. Enter the minimum time, in milliseconds (ms), that is required to ensure that an on-hook indication is intentional, and not an electrical transient on the line, before a supervisory disconnect occurs. Range: Integers 50 through 1500 Default: 350	**timing sup-disconnect** *milliseconds*

Field	Description	Cisco IOS CLI Equivalent
Battery Reversal	Applies only to FXO voice interface templates. Battery reversal reverses the battery polarity on a PBX when a call connects, then changes the battery polarity back to normal when the far-end disconnects. Choose one of the following options. If you choose **Detection Delay** or **Both**, enter a value, in ms, of the delay time after which the port acknowledges a battery-reversal signal. • **Answer**: Configures the port to support answer supervision by detection of battery reversal • **Detection Delay**: Configures the delay time after which the card acknowledges a battery-reversal signal • **Both**: Configures answer and detection delay behavior Detection delay range: Integers 0 through 800 Detection delay default: 0 (no delay) **Note** If an FXO port or its peer FXS port does not support battery reversal, do not configure this battery reversal option to avoid unpredictable behavior,	**battery-reversal** [**answer**] **battery-reversal-detection-delay** *milliseconds*
Timing Hookflash Out	Applies only to FXO voice interface templates. Enter the duration, in ms, of the hookflash indications that the gateway generates on the FXO interface. Range: Integers 50 through 1550 Default: 4000	**timing hookflash-out** *milliseconds*
Timing Guard Out	Applies only to FXO voice interface templates. Enter the time, in ms, after a call disconnects before another outgoing call is allowed. Range: Integers 300 through 3000 Default: 2000	**timing guard-out** *milliseconds*

Field	Description	Cisco IOS CLI Equivalent
Timing Hookflash In	Applies only to FXS voice interface templates. Enter the minimum and maximum duration, in ms, for an on-hook condition to be interpreted as a hookflash by the FXS card. Range for minimum duration: 0 through 400 Default minimum range value: 50 Range for maximum duration: 50 through 1500 Default maximum range value: 1000	**timing hookflash-in** *maximum-milliseconds minimum-milliseconds*
Pulse Digit Detection	Applies only to FXS voice interface templates. Enable this option to enable pulse digit detection at the beginning of a call. Default: Enabled	**pulse-digit-detection**
Loop Length	Applies only to FXS voice interface templates. Choose the length for signaling on FXS ports (**Long** or **Short**). Default: Short	**loop-length** [**long** | **short**]
Ring Frequency	Applies only to FXS voice interface templates. Choose the frequency, in Hz, of the alternating current that, when applied, rings a connected device. Default: 23	**ring frequency** *number*
DC Offset	Applies only to FXS voice interface templates when **Loop Length** is set to **Long**. Choose the voltage threshold below which a ring does not sound on devices. Options are **10-volts**, **20-volts**, **24-volts**, **30-volts**, and **35-volts**.	**ring dc-offset** *number*

Field	Description	Cisco IOS CLI Equivalent
Ringer Equivalence Number (REN)	Applies only to FXS voice interface templates. Choose the REN for calls that the port processes. This number specifies the loading effect of a telephone ringer on a line. Range: Integers 1 through 5 Default: 1	**ren** *number*
Action	Click the **Recycle Bin** icon to delete the corresponding Tuning options instance.	—

DID Timer

Field	Description	Cisco IOS CLI Equivalent
Add DID Timer	Appears only to FXS voice interface templates when the **Signal Type** option in the **Basic** tab is configured as **DID**. Click to configure the options for timers for DID calls. You can add as multiple instances of these options so that you can configure different DID timer options for different ports.	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Wait before Wink	Enter the amount of time, in ms, that the port waits after receiving a call before sending a wink signal to notify the remote side that it can send DNIS information. Range: Integers 100 through 6500 Default: 550	**timing wait-wink** *milliseconds*
Wink Duration	Enter the maximum amount of time, in ms, of the wink signal for the port. Range: Integers 50 through 3000 Default: 200	**timing wait-duration** *milliseconds*

Field	Description	Cisco IOS CLI Equivalent
Clear Wait	Enter the minimum amount of time, in ms, between an inactive seizure signal and the call being cleared for the port. Range: Integers 200 through 2000 Default: 400	**timing clear-wait** *milliseconds*
Dial Pulse Min Delay	Enter the amount of time, in ms, between wink-like pulses for the port. Range: Integers 0, or 140 through 2000 Default: 140	**timing dial-pulse min-delay** *milliseconds*
Answer Winkwidth	Enter the minimum delay time, in ms, between the start of an incoming seizure and the wink signal. Range: Integers 110 through 290 Default: 210	**timing answer-winkwidth** *milliseconds*
Action	Click the **Recycle Bin** icon to delete the corresponding DID Timer options instance.	—

Caller ID

Field	Description	Cisco IOS CLI Equivalent
Caller ID	Click to configure the options for enabling caller ID for the port or ports. Caller ID is an analog service by which a telephone central office switch sends digital information about an incoming call. The Caller ID feature for analog FXS ports is configurable on a per-port basis to phones that are connected to analog FXS voice ports. Caller ID also is available on analog FXO ports. Caller ID-related features are based on the identity of the calling party. **Note** • These caller ID options apply only when the **Signal Type** option in the **Basic** tab is configured as **LoopStart** or **GroundStart**. • If an FXS voice port has caller-id commands configured, remove all the caller-id configurations before changing the signaling type from loop-start or ground-start to DID. • If you remove a voice port from a device after a caller ID command is configured, remove the caller ID configuration from the device. Otherwise, a voice port configuration mismatch occurs between the Cisco IOS configuration and the Cisco Catalyst SD-WAN configuration.	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Caller ID Mode	Choose a noncountry, standard caller ID mode for a receiving FXO or a sending FXS voice port: • **BT**: Frequency-Shift Keying (FSK) with Dual Tone Alerting Signal (DTAS) used by British Telecom • **FSK**: FSK before or during a call • **DTMF**: DTMF digits with the start and end digit codes	**caller-id mode** {**BT** | **FSK** | **DTMF**}
DTMF Start	Applies only if you choose **DTMF** for the caller ID mode. Choose the character that indicates the start of a DTMF string.	**caller-id mode** {**dtmf** {**start** | **end**}{**#** | ***** | **A** | **B** | **C** | **D**}}

Field	Description	Cisco IOS CLI Equivalent
DTMF End	Applies only if you choose **DTMF** for the caller ID mode. Choose the character that indicates the end of a DTMF string.	**caller-id mode** {**dtmf** {**start** | **end**} {**#** | ***** | **A** | **B** | **C** | **D**}}
Alerting Options	Choose the alerting method for on-hook caller ID information: • **Line-Reversal**: Sets the line-reversal alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending FXS voice port and for an on-hook caller ID at a receiving FXO voice port. • **Pre-ring**: Sets a 250 ms pre-ring alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending FXS and a receiving FXO voice port. • **Ring 1**, **Ring 2**, **Ring 3**, or **Ring 4**: Sets the ring-cycle method for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving FXO or a sending FXS voice port.	**caller-id alerting** {**line-reversal** | **pre-ring** | **ring** {**1** | **2** | **3** | **4**}}
DSP Pre-Allocate Alerting	Applies only to FXO voice interface templates. Enable this option to statically allocate a DSP voice channel for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving FXO voice port.	**caller-id alerting dsp pre-allocate**
Caller ID Block	Applies only to FXS voice interface templates. Enable this option to request blocking of caller ID information display at the far end of a call that originates from an FXS port.	**caller-id block**
Caller ID Format E911	Applies only to FXS voice interface templates. Enable this option to use the enhanced 911 format for calls that are sent on the FXS port.	**caller-id format e911**
Action	Click the **Recycle Bin** icon to delete the corresponding Caller ID options instance.	—

Connection Plar

Field	Description	Cisco IOS CLI Equivalent
Connection Plar	Click to configure the options for the connection Private Line Automatic Ringdown (PLAR). You can add multiple instances of these options so that you can configure different connection PLAR options for different ports.	—

Field	Description	Cisco IOS CLI Equivalent
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Connection Plar Pattern	Enter the PLAR extension to which the selected ports forward inbound calls.	**connection plar** *digits*
OPX	Applies only to FXO voice interface templates. Check this check box to enable Off-Premises Extension for the PLAR extension.	**connection plar opx** *digits*
Action	Click the **Recycle Bin** icon to delete the corresponding Connection Plar options instance.	—

Association

Field	Description
Association	Click to configure options for associating other configured UC voice features with the port or ports. When you associate a feature in this way, the configuration options in that feature are applied to the designated ports. You can add multiple instances of these options so that you can configure different association options for different ports.
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port 1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** to specify ports 1 through 5.
Trunk Group	Choose a configured Trunk Group feature to associate with the port.
Trunk Group Priority	Enter the priority of the trunk group. The number you enter is the priority of the POTS dial peer in the trunk group for incoming and outgoing calls. Range: Integers 1 through 64
Translation Profile	Choose a configured Translation Profile feature to associate with the port.

Field	Description
Translation Profile Direction	Choose the direction of the traffic to which to apply the selected Translation Profile feature: • **Incoming**: Applies the corresponding Translation Profile feature to traffic that is incoming to the port • **Outgoing**: Applies the corresponding Translation Profile feature to traffic that is outgoing from the port
Supervisory Disconnect	Applies only to FXO voice interface templates. Choose a configured Supervisory Disconnect feature to associate with the port.
Action	Click the **Recycle Bin** icon to delete the corresponding Association options instance.

Call Routing

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Call Routing feature provides options for configuring TDM-SIP trunking, including options for dial peers, fax operations, and modem operations. Dial peers make up a dial plan, which defines how a router routes traffic.

A plain old telephone system (POTS) dial peer defines the characteristics of a traditional telephony network connection. POTS dial peers map a dialed string to a specific voice port on the local router, normally the voice port connecting the router to the local PSTN, PBX, or telephone.

A SIP dial peer defines the characteristics of a packet network connection. SIP dial peers map a dialed string to a remote network device, such as the destination router that is connected to the remote telephony device.

Both POTS and SIP dial peers are needed to establish voice connections over a packet network.

You can configure a standalone call routing feature, or configure multiple call routing features that are mapped to different Analog Interface or Digital Interface features.

The following tables describe the options for configuring the Call Routing feature.

Field	Description
Name	Enter a unique name for the call routing configuration. The name can contain any characters.
Description	Enter a description of the call routing configuration.
Dial Peer Tag Prefix	Enter a unique number to be pretended to a dial peer tag to ensure that the dial peer tag can be uniquely identified across this feature.
Description	Enter a description of the analog or digital interface configuration to which this call routing configuration is to be associated.

Field	Description
Voice Module Location Parcel Name	Choose the Analog or Digital Interface feature to which the POTS dial peer call routing port-related configuration is to be associated.

Dial Peer

Field	Description	Cisco IOS CLI Equivalent
Add Dial Peers	Click to add a dial peer to a dial plan. Configure the following options in the **Add Dial Peer** dialog box, then click **Save**	—
Add Dial Peer Dialog Box Options		
Tag	Enter a number to be used to reference the dial peer. Range: Integers 1 through 214748364	**dial-peer voice** *number* {**pots** | **voip**}
Dial peer type	Choose the type of dial peer that you are creating. Options are **pots** and **sip**.	**dial-peer voice** *number* {**pots** | **voip**}
Direction	Choose the direction of traffic on the dial peer. Options are **incoming** and **outgoing**.	• Incoming: **dial-peer voice** *number* {**pots** | **voip**} **incoming called-number** *string* • Outgoing: **dial-peer voice** *number* {**pots** | **voip**} **destination-pattern** *string*
Description	Enter a description of the dial peer.	**description**
Number pattern	Enter the string that the router uses to match incoming calls to the dial peer. Enter the string as an E.164 format regular expression in the following form: (ipv6:\[([0-9A-Fa-f.:])+\](:[0-9]+)?))	• Incoming: **dial-peer voice** *number* {**pots** | **voip**} **incoming called-number** *string* • Outgoing: **dial-peer voice** *number* {**pots** | **voip**} **destination-pattern** *string*

Field	Description	Cisco IOS CLI Equivalent
Forward Digits Type	Applies only when **Dial peer type** is configured as **pots** and **direction** is configured as **outgoing**. Choose how the dial peer transmits digits in outgoing numbers: • **all**: The dial peer transmits all digits • **none**: The dial peer does not transmit digits that do not match the destination pattern • **some**: The dial peer transmits the specified number of right-most digits Default: none	• All: **dial-peer voice** *number* **pots** **forward-digits all** • None: **dial-peer voice** *number* **pots** **forward-digits 0** • Some: **dial-peer voice** *number* **pots** **forward-digits** *number*
Forward Digits	Applies only when you choose **Some** for **Forward Digits Type**. Enter the number of right-most digits in the outgoing number to transmit. For example, if you set this option to 7 and the outgoing number is 1112223333, the dial peer transmits 2223333.	**dial-peer voice** *number* **pots** **forward-digits** *number*
Prefix	Applies only when **Dial peer type** is configured as **pots** and **direction** is configured as **outgoing**. Enter a string to be pretended to the dial string for outgoing calls. Valid values: Integers 0 through 9 and comma (,)	**dial-peer voice** *number* **pots** **prefix** *string*
Transport Protocol	Applies only when **Dial peer type** is configured as **sip**. Choose the transport protocol for SIP control signaling. Options are **tcp** and **udp**.	**dial-peer voice** *number* **voip** **session transport** {**tcp** | **udp**}

Field	Description	Cisco IOS CLI Equivalent
Preference	Enter the preference of the dial peer. If dial peers have the same match criteria, the system uses the one with the highest preference value. Range: Integers 0 through 10 Default: 0	**dial-peer voice** *number* **voip** **preference** *value* **dial-peer voice** *number* **pots** **preference** *value*
Port	Applies only when **Dial peer type** is configured as **pots**. Enter the voice port that the router uses to match calls to the dial peer. For an analog port, enter the port you want. For a digital T1 PRI ISDN port, enter a port with the suffix **23**. For a digital E1 PRI ISDN port, enter a port with the suffix **15**. For an outgoing dial peer, the router sends the calls that match the dial peer to this port. For an incoming dial peer, this port serves as an additional match criterion. The dial peer is matched only if a call comes in on this port.	**dial-peer voice** *number* **pots** • For an analog port: **port** *slot*/*subslot*/*port* • For a digital port: **port** *slot*/*subslot*/*port***:15** **port** *slot*/*subslot*/*port***:23**
Destination Address	Applies only when **Dial peer type** is configured as **sip** and **direction** is configured as **outgoing**. Enter the network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched. Enter the address in one of these formats: • **dns:***hostname.domain* • **sip-server** • **ipv4:***destination-address* • **ipv6:***destination-address*	**session target** {**ipv4:***destination-address* | **ipv6:***destination-address* | **sip-server** | **dns:***hostname.domain*}
Dial Peer File Options		

Field	Description	Cisco IOS CLI Equivalent
Download Dial Peer List	To create or edit a dial peer CSV file, click this option to download the Cisco provided file named Dial-Peers.csv. The first time that you download this file, it contains field names but no records. Update this file as needed by using an application such as Microsoft Excel. For detailed information about this file, see Dial Peer CSV File.	—
Upload Dial Peer List	To import configuration information from a dial peer CSV file that you have created, click this option, choose the file to upload, then click **Save**.	—
Action	Click **Edit** to edit the corresponding Dial Peer options instance. Click **Delete** to delete the corresponding Dial Peer options.	—

Fax

Field	Description	Cisco IOS CLI Equivalent
Add Fax Protocol	Click to configure the options for the fax protocol capability for a SIP dial peer endpoint.	—
Dial Peer Range	Enter the tag or tags of the SIP dial peers for which to enable fax options. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify SIP dial peer tag 1; **1,2,3** to specify tags 1, 2, and 3; or **1-5** so specify tags 1 through 5.	—

Field	Description	Cisco IOS CLI Equivalent

Primary Protocol	Choose a set of fax protocol options. Each option is a bundled set of related fax commands.
	For a detailed description of each bundle, see the "Primary Fax Protocol Command Bundles" table in Configure SIP Dial Peers for a Voice Policy.
	The descriptions of the bundles include the following components:
	• **nse**: Uses NSEs to switch to T.38 fax relay mode
	• **force**: Unconditionally uses Cisco Network Services Engines (NSE) to switch to T.38 fax relay
	• **version**: Specifies a version for configuring fax speed:
	  • **0**: Configures version 0, which uses T.38 version 0 (1998–G3 faxing)
	  • **3**: Configures version 3, which uses T.38 version 3 (2004–V.34 or SG3 faxing)
	• **none**: No fax pass-through or T.38 fax relay is attempted
	• **Pass-through**: The fax stream uses one of the following high-bandwidth codecs:
	  • **g711ulaw**: Uses the G.711 ulaw codec
	  • **g711alaw**: Uses the G.711 alaw codec
		fax protocol { **none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**] | **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]

Field	Description	Cisco IOS CLI Equivalent
Fallback Protocol	Available when the primary protocol bundle name that you selected in the **Primary Protocol** field begins with “T.38” or “Fax Pass-through." Choose the fallback mode for fax transmissions. This fallback mode is used if the primary fax protocol cannot be negotiated between device endpoints. For a detailed description of each option, see the "Fallback Protocol Options” table in Configure SIP Dial Peers for a Voice Policy.	**fax protocol** {**none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**] | **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy value** [**hs-redundancy value**]] [**fallback** {**none**|**pass-through** {**g711ulaw** | **g711alaw**}}]}
Low Speed Redundancy	Available when the primary protocol bundle name that you selected in the **Primary Protocol** field begins with “T.38.” Enter the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range: Integers 0 (no redundancy) to 5 Default: 0	**ls-redundancy** *value*
High Speed Redundancy	Available when the primary protocol bundle name that you selected in the **Primary Protocol** field begins with “T.38.” Enter the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range: Integers 0 (no redundancy) to 2 Default: 0	**hs-redundancy** *value*
Action	Click the **Recycle Bin** icon to delete the corresponding Fax options instance.	—

Modem

Field	Description	Cisco IOS CLI Equivalent
Add Modem Passthrough	Click to configure the modem pass-through feature for a SIP dial peer endpoint.	—
Dial Peer Range	Enter the tag or tags of the SIP dial peers for which to enable modem options. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify SIP dial peer tag 1; **1,2,3** to specify tags 1, 2, and 3; or **1-5** so specify tags 1 through 5.	—
Protocol	Choose the protocol for the modem pass-through: • **None**: Modem pass-through is disabled on the device • **NSE G.711ulaw**: Uses named signaling events (NSEs) to communicate G.711 ulaw codec switchover between gateways • **NSE G.711alaw**: Uses named NSEs to communicate G.711 alaw codec switchover between gateways	• None: **no modem passthrough** • NSE G.711ulaw: **modem passthrough nse codec g711ulaw** NSE G.711alaw: **modem passthrough nse codec g711alaw**
Action	Click the **Recycle Bin** icon to delete the corresponding Modem options instance.	—

Association

Field	Description
Association	Click to configure the following options for associating other configured UC features with the dial plan. When you associate a feature in this way, the configuration options in that feature are applied to the designated POTS or SIP dial peers. You can add multiple instances of these options so that you can configure different association options for different ports.
Dial Peer Range	Enter the dial peer or peers to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify dial peer 1; **1,2,3** to specify dial peers 1, 2, and 3; or **1-5** to specify dial peers 1 through 5.
Media Profile Name	Choose a configured Media Profile feature to associate with the SIP dial peer.
Server Group	Choose a configured Server Group feature to associate with the SIP dial peer.
Trunk Group	Choose a configured Trunk Group feature to associate with the POTS dial peer.

Field	Description
Trunk Group Priority	Enter the priority of the trunk group, which specifies the priority of the POTS dial peer in the trunk group for incoming and outgoing calls. Range: Integers 1 through 64
Translation Profile	Choose a configured Translation Profile feature to associate with the port.
Translation Profile Direction	Choose the direction of the traffic to which to apply the selected Translation Profile feature: • **Incoming**: Applies the corresponding Translation Profile feature to traffic that is incoming to the port • **Outgoing**: Applies the corresponding Translation Profile feature to traffic that is outgoing from the port
Voice Tenant	Choose a configured Voice Tenant feature to associate with the port.
Action	Click the **Recycle Bin** icon to delete the corresponding Association options instance.

DSP Farm

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

The DSP Farm feature provides options for configuring parameters for a Digital Signal Processor (DSP) farm.

A DSP farm is a collection of DSP resources that are available on a voice gateway for conferencing, transcoding, and MTP services. These resources can be configured and managed as out-of-box resources by Cisco Unified Call Manager through the SCCP application, and as inbox transcoder resources by Cisco Unified Border Element (CUBE).

The following tables describe the options for configuring the DSP Farm feature.

Field	Description
Name	Enter a unique name for the DSP farm configuration. The name can contain any characters.
Description	Enter a description of the DSP farm configuration.

Services

Field	Description	Cisco IOS CLI Equivalent
Services	Click to configure options for a DSP farm service. DSP farm services are conferencing, transcoding, and media termination point (MTP).	—

Field	Description	Cisco IOS CLI Equivalent
DSP Services	Enable this option to use hardware DSP resources. Disable this option if the device does not have any hardware DSP resources and you want to use the software MTP DSP service. This option is enabled by default.	—
Module Location	If **Services** is enabled, choose the slot and sub-slot location for the hardware DSP. You can configure as many module locations as needed. For a list of supported modules, see Configure UC Voice Services Using the Workflow Library or Configuration Groups.	**voice-card** *slot*/*subslot* **dsp service dspfarm**
SCCP	Check this check box to enable the SCCP application for provisioning conference, transcoding, and MTP services. Then configure the **Profile** options as described in the following table.	—
CUBE	Check this check box to enable the CUBE application for provisioning inbox transcoding services. Then configure the **Profile** options as described in the following table.	—
Action	Click the **Recycle Bin** icon to delete the corresponding Services options instance.	—

Profile

Field	Description	Cisco IOS CLI Equivalent
Add Profile	Click and, in the **Profile** dialog box for a DSP farm profile, configure the options that this table describes. Click **Add** in the dialog box to add the profile to the table of profiles. A profile includes options for provisioning a specific DSP farm service type, which can be transcoding, conferencing, or MTP. A profile is associated with either the SCCP application or CUBE, which invokes the resources for a service as needed. You can add multiple instances of these options so that you can configure different profile options for as needed.	—
Profile ID	Displays a unique system-generated identifier for the profile.	**profile-identifier**
Application	Choose the application with which to associate the profile. Options are **sccp** and **cube**.	**associate application**{**sccp** | **cube**}

Field	Description	Cisco IOS CLI Equivalent
Profile Type	For the **sccp** application, choose the service type to provision. Options are **transcode**, **conference**, and **mtp**. For the **cube** application, **transcode** is selected automatically as the service to provision.	**dspfarm profile** *profile-identifier* { **conference** | **mtp** | **transcode**}
Transcode Universal Profile Type	For the **transcode** profile type, check this check box to allow transcoding between codecs of any type. When this check box is unchecked, transcoding is allowed only between the G.711 codec and other codecs.	**dspfarm profile** *profile-identifier* **transcode** [**universal**]
MTP Type Hardware	For the **mtp** profile type, check this check box to have MTP translations and conversions performed by the hardware DSP resources.	**maximum session hardware**
MTP Type Software	For the **mtp** profile type, check this check box to have MTP translations and conversions performed by the router CPU.	**maximum session software**
Profile Name	For the **transcode** or **conference** profile type for the **sccp** application, or for the **cube** application, enter a unique name that you can use to identify the profile.	—

Field	Description	Cisco IOS CLI Equivalent
Codec List		**codec** *codec-name*

Field	Description	Cisco IOS CLI Equivalent
	Choose the codecs to be available for the DSP farm service that this profile defines. For the **mtp** profile type, you can choose **pass-through** and one other option. To change a codec, remove the current one before choosing a new one. The following codecs are supported: • For the **transcode** profile type: • g711alaw • g711ulaw • g729abr8 • g729ar8 • g729br8 • g729r8 • g722-64 • ilbc • iSAC • opus • pass-through • For the **conference** profile type: • g711alaw • g711ulaw • g722r-64 • g729abr8 • g729ar8 • g729br8 • g729r8 • For the **mtp** profile type when **MTP Type Hardware** or both **MTP Type Hardware** and **MTP Type Software** are chosen: • g711ulaw • g711alaw • pass-through	

Field	Description	Cisco IOS CLI Equivalent
	• For the **mtp** profile type when **MTP Type Software** is chosen: • g711ulaw • g711alaw • g722-64 • g729abr8 • g729ar8 • g729br8 • g729r8 • ilbc • iSAC • pass-through	
Feature List	For the **cube** application, choose the features to enable for in-box transcoding.	—
Maximum Sessions	For the **transcode** or **conference** profile type, enter the maximum number of sessions that this profile can support. This value depends on the maximum number sessions that can be configured with the DSP resources that are available on the router. These resources are based on the type of modules in the router. To determine these resources, you can use the Cisco DSP Calculator.	**maximum sessions** *number*
MTP Maximum Hardware Sessions	If you checked **MTP Type Hardware**, enter the maximum number of hardware sessions that can be used for MPT translations and conversions. Range: Integers 1 through 4000	**maximum session hardware** *number*
MTP Maximum Software Sessions	If you checked **MTP Type Software**, enter the maximum number of CPU sessions that can be used for MRP translations and conversions. Range: Integers 1 through 6000	**maximum session software** *number*
Shutdown	Enable this option to take this profile out of service.	**shutdown**
Action	Click **Edit** to edit the corresponding Profile options instance. Click **Delete** to delete the corresponding Profile options.	—

CUCM

Field	Description	Cisco IOS CLI Equivalent
CUCM	Click to configure the Cisco Unified Communications Manager servers to which the profiles that you define register. You can configure up to 12 Cisco Unified Communications Manager servers. **Note** These options do not appear if you enable DSP services and check only the **CUBE** option.	—
Configure Local Interface	Enter the local interface that DSP services that are associated with the SCCP application use to register with Cisco Unified Communications Manager. Enter the interface in this format: *interface-type/interface-number/port* where: • *interface-type*: Type of interface that the services use to register with Cisco Unified Communications Manager. The type can be a Gigabit Ethernet interface or a port channel interface. • *interface-number*: Interface number that the services use to register with Cisco Unified Communications Manager. • *port*: (Optional) Port on which the interface communicates with Cisco Unified Communications Manager. If you do not specify a port, the default value 2000 is used. For example: GigabitEthernet0/0/0.	**sccp local** *interface-type interface-number* [**port** *port-number*]
IP Precedence	Enter the IP precedence value to be used by the SCCP application for IP packets. Range: 1 (lowest) through 7 (highest) Default: 5	**sccp ip precedence** *value*
Add Configure Server List	Click to display the following options for a Cisco Unified Communications Manager server: • **Server Identifier**: Unique system-generated identifier of the Cisco Unified Communications Manager server • **Server IP**: Enter the IP address of the Cisco Unified Communications Manager server	• Server identifier: *identifier-number* • Server IP: **sccp ccm** {*ipv4-address* | i*pv6-address* | *dns*} **identifier** *identifier-number* **version 7.0+**

Field	Description	Cisco IOS CLI Equivalent
Action	Click the **Recycle Bin** icon to delete the corresponding CUCM options instance.	—

CUCM Group

Field	Description	Cisco IOS CLI Equivalent
Add CUCM Group	Click and, in the **CUCM Group** dialog box, configure a Cisco Unified Communications Manager group by using the options that this table describes. Each group includes up to 4 Cisco Unified Communications Manager servers that control the DSP farm services that, in turn, are associated with the servers. Click **Add** in the dialog box when you are finished. You can add multiple Cisco Unified Communications Manager groups. **Note** These options do not appear if you enable DSP services and check only the **CUBE** option.	—
CUCM Media Resource Name	Enter a unique name that is used to register a DSP farm profile to the Cisco Unified Communications Manager servers. The name must contain from 6 to 15 characters. Characters can be letter, numbers, slashes (/), hyphens (-), and underscores (_).	**associate ccm** *profile-identifier* **register** *device-name*
Profile Name	Enter the name that you entered for the DSP farm profile that is to be registered to this Cisco Unified Communications Manager group.	—

Field	Description	Cisco IOS CLI Equivalent
Server Groups Priority Order	Designate the priority in which the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group are used. The drop-down list displays the server identifiers of the Cisco Unified Communications Manager servers that you configured. Choose the server that you want to be the primary server. This server has the highest priority. Then choose the server that you want to be a redundant server with the next highest priority. Continue in this way to choose other redundant servers. The servers in the field appear in descending order of priority, with the highest priority server appearing first. To remove a server from the field, click its **X** icon. To change the priority order of servers, remove the servers and add them back in the desired order.	**associate ccm** *cisco-unified-communications-manager-id* **priority** *priority*
CUCM Switchback	Choose the switchback method that the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group use to switch back after a failover: • **guard**: Switchback occurs when active sessions are terminated gracefully or when the guard timer expires, whichever happens first • **graceful**: Switchback occurs after all active sessions terminate gracefully • **immediate**: Performs the Cisco Unified Communications Manager switchback to the higher priority Cisco Unified Communications Manager immediately when the timer expires, whether or not there is an active connection Default: graceful	**switchback method**{ **graceful** | **guard** [*timeout-guard-value*] | **immediate**}
Server Switchover	Choose the switchover method that Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group use when failing over: • **graceful**: Switchover occurs after all active sessions terminate gracefully • **immediate**: Switchover occurs immediately, whether or not there is an active connection Default: graceful	**switchover method** {**graceful** | **immediate**}

Field	Description	Cisco IOS CLI Equivalent
Keep Alive Retries	Enter the number of keepalive retries from the SCCP application to Cisco Unified Communications Manager. Range: Integers 1 to 180 Default: 3	**keepalive retries** *number*
Keep Alive Time Out	Enter the number of seconds between successive keepalive messages from the SCCP application to Cisco Unified Communications Manager. Range: Integers 1 to 180 Default: 20	**keepalive retries** *seconds*
Bind Interface	Enter the interface to bind with the Cisco Unified Communications Manager group.	**bind interface** *interface-name*
Action	Click **Edit** to edit the corresponding CUCM Group options instance. Click **Delete** to delete the corresponding CUCM Group options.	—

Digital Interface

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Digital Interface feature provides options for configuring parameters for a voice card digital interface.

Note If you want to remove or replace the digital interface configuration on a device, delete all configuration instances for this feature (Basic, ISDN Timer, ISDN Map, Shutdown, Line Params, Outgoing IE, and Associations), and add one Basic configuration instance with default settings. Then deploy this updated interface feature configuration to the device, which resets the digital interface configuration on the device. You can then delete this feature or configure a new one.

The following tables describe the options for configuring the Digital Interface feature.

Field	Description	Cisco IOS CLI Equivalent
Name	Enter a unique name for the digital interface configuration. The name can contain any characters.	—
Description	Enter a description of the digital interface configuration.	**description** *string*

Field	Description	Cisco IOS CLI Equivalent
Voice Interface Templates	Choose a group of voice interface T1 or E1 ISDN digital ports to be provisioned for the digital interface.	—
Module Location	Choose the slot and sub-slot location for the group of digital ports to be provisioned. For a list of supported modules, see Configure UC Voice Services Using the Workflow Library or Configuration Groups.	**voice-card** *slot/subslot*
Use DSP	Check this check box if you want to allow local calls between digital ports on the same device to use DSPs. Default: Unchecked	**no local-bypass**

Field	Description	Cisco IOS CLI Equivalent
Port and Clock Selector	Click **Selected** and, in the **Port and Clock Selector** dialog box, follow these steps to configure the clock source for each T1 or E1 port on the voice interface template that you chose: **1.** Check the check box that corresponds to each port that you want to configure. The number of ports that you can configure depends on the voice interface template that you chose. **2.** For each port, choose one of the following options to set the clock source: • **Line**: Sets the line clock as the primary clock source. With this option, the port clocks its transmitted data from a clock that is recovered from the line receive data stream. This option is the default. • **Network**: Sets the backplane clock or the system oscillator clock as the module clock source. • **Primary Clock**: Sets the port to be a primary clock source. • **Secondary Clock**: Sets the port to be a secondary clock source. You can chose 1 port to be the primary clock source and 1 port to be the secondary clock source. Choosing a primary clock source does not require you to choose a secondary clock source. **3.** Click **Save**.	**controller** {**t1** | **e1**} *slot*/*sub-slot*/*number* **clock source** {**network** | **line** | **line primary** | **line secondary**}

Basic

Field	Description	Cisco IOS CLI Equivalent
Add Basic	Click to configure basic options for the group of digital ports. You can add as multiple instances of these options so that you can configure different basic options for different ports.	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Time slots	Enter the number of time slots of the interface. Ranges: • For T1 PRI: Time slots 1 through 24. The 24th time slot is the D channel. • For E1 PRI: Time slots 1 through 31. The 16th time slot is the D channel.	**controller e1/t1** *slot*/*sub-slot*/*port* **pri-group timeslots** *timeslots-range* [**voice-dsp**]
Line Termination	Applies to E1 voice interface templates only. Choose the termination type for the interface: • **75-ohm**: 75 ohm unbalanced termination • **120-ohm**: 120 ohm balanced termination (default)	**controller e1** *slot*/*sub-slot*/*port* **line-termination** {**75-ohm** | **120-ohm**}

Field	Description	Cisco IOS CLI Equivalent
Cable Length Type	Applies to T1 voice interface templates only. Choose the cable length type for the interface: • **Long**: Applies to cables that are longer than 660 feet (201.2 m). Attenuates the pulse from the transmitter by using pulse equalization and line build-out. This value is the default • **Short**: Applies to cables that are 660 feet (201.2 m) or less in length. Sets transmission attenuation for the cable.	**controller t1** *slot/sub-slot/port* **cablelength** {**short | long**}
Cable Length	Applies to T1 voice interface templates only. Choose the length of the cable for the interface: • For a **Long** cable length, enter the loss value, decibels (dB). Options are **–7.5**, **–15**, **–22.5**, and **0**. The default value is 0. • For a **Short** cable length (up to 660 feet (201.2 m), enter the value that most closely exceeds the length of the cable. For example, if the cable length is 180 feet (55 m) enter **220**.	**controller t1** *slot/subslot/port* **cablelength** {**[short [110ft | 220ft | 330ft | 440ft | 550ft | 660ft]] [long [-15db |-22db |-7.5db | 0db]]**}

Field	Description	Cisco IOS CLI Equivalent
Line Code	Choose the line code type for the interface. For a T1 voice interface template: • **ami**: Use alternate mark inversion as the line code type • **b8zs**: Use binary 8-zero substitution as the line code type (default) For an E1 voice interface template: • **amiami**: Use alternate mark inversion as the line code type • **hdb3**: Use high-density bipolar 3-zero as the line code type (default)	**linecode** {**ami** | **b8zs** | **hdb3**
Framing	Choose the frame type for the interface. For a T1 voice interface template: • **esf**: Extended super frame (default) • **sf**: Super frame For an E1 voice interface template: • **ccr4**: CRC4 framing type (default) • **no-crc4**: No CRC4 framing type	**controller t1** *slot*/*sub-slot*/*port* **framing** [**esf** | **sf**] **controller e1** *slot*/*sub-slot*/*port* **framing** [**crc4** | **no-crc4**] [**australia**]
Framing Australia	Applies to E1 voice interface templates only. Enable this option to use the Australia framing type.	**controller e1** *slot*/*sub-slot*/*port* **framing** [**crc4** | **no-crc4**] **australia**
Network Side	Enable this option to have the device to which this configuration is to be associated use the standard PRI network-side interface. Default: Disabled	**interface** **serial** *slot*/*sub-slot*/**port:** {**15**| **23**} **isdn protocol-emulate** [**network** | **user**]

Field	Description	Cisco IOS CLI Equivalent
Switch Type	Choose the ISDN switch type for this interface: • **primary-qsig**: Supports QSIG signaling according to the Q.931 protocol. Network side functionality is assigned with the **isdn protocol-emulate** command. • **primary-4ess**: Lucent (AT&T) 4ESS switch type for the United States. • **primary-5ess**: Lucent (AT&T) 5ESS switch type for the United States. • **primary-dms100**: Nortel DMS-100 switch type for the United States. • **primary-net5**: NET5 ISDN PRI switch types for Asia, Australia, and New Zealand. ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system. • **primary-ni**: National ISDN switch type. • **primary-ntt**: Japanese NTT ISDN PRI switches.	**interface serial** *slot*/*sub-slot*/**port:**{**15** | **23**} **isdn switch-type** [**primary-4ess** | **primary-5ess** | **primary-dms100** | **primary-net5** | **primary-ni** | **primary-ntt** | **primary-qsig**]
Delay Connect Timer	Enter the duration, in ms, to delay connect a PRI ISDN hairpin call. Range: Integers 0 through 200 Default: 20	**voice-port** *slot*/*sub-slot*/**port:**{**15** | **23**} **timing delay-connect** *value*
Action	Click the **Recycle Bin** icon to delete the corresponding Basic options instance.	—

ISDN Timer

Field	Description	Cisco IOS CLI Equivalent
Add ISDN Timer	Click to configure options for the ISDN timer for the interface. You can add multiple instances of these options so that you can configure different ISDN timer options for different ports.	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—

Field	Description	Cisco IOS CLI Equivalent
ISDN Timer and Value		**interface serial** *slot*/*sub-slot*/**port:**{**15**| **23**} **isdn timer T200** *value* **isdn timer T203** *value* **isdn timer T301** *value* **isdn timer T303** *value* **isdn timer T306** *value* **isdn timer T309** *value* **isdn timer T310** *value* **isdn timer T321** *value*

Field	Description	Cisco IOS CLI Equivalent
	Click to configure an ISDN timer. Configure the following fields in the **ISDN Timer and Value** dialog box, then click **Save**. • **Port Range**: Displays the ports that you chose • **ISDN Timer**: Displays the ISDN timers that you can provision. • **Value**: Enter the value, in ms, for the corresponding ISDN timer: • For the **T200** ISDN timer: • Range: 400 through 400000 • Default for all switch types: 1000 • For the **T203** ISDN timer: • Range: Integers 400 through 400000 • Default for QSIG, ETSI Net5, and DMS-100 switch types: 10000 • Default for 4ESS, 5ESS, NTT, and NI switch types: 30000 • For the **T301** ISDN timer: • Range: 180000 through 86400000 • Default for NTT and ETSI Net5 switch types: 180000 • Default for other switch types: 300000 • For the **T303** ISDN timer: • Range: 400 through 86400000 • Default for QSIG switch type: 6000 • Default for other switch types: 4000 • For the **T306** ISDN timer: • Range: 400 through 86400000 • Default for all switch types: 30000 • For the **T309** ISDN timer: • Range: 0 through 86400000 • Default for all switch types when network side configuration is false (User): 90000	

Field	Description	Cisco IOS CLI Equivalent
	• Default for all switch types when network side configuration is true (Network): 5000 • For the **T310** ISDN timer: • Range: 400 through 400000 • Default for NI , 4ESS and 5ESS switch types when network side configuration is false (User): 30000 • Default for NI, 4ESS, and 5ESS switch types when network side configuration is true (Network): 10000 • Default for ETSI Net5 switch types: 4000 • Default for QSIG switch type: 120000 • Default for NTT switch type: 3000 • Default for DMS-100 switch type when network side configuration is false (User): 1000 • Default for DMS-100 switch type when network side configuration is true (Network): 4000 • Default for other switch types: 4000 • For the **T321** ISDN timer: • Range: 0 through 86400000 • Default for ETSI Net5 switch type: 30000 • Default for other switch types: 40000	
Action	Click the **Recycle Bin** icon to delete the corresponding ISDN Timer options instance.	—

ISDN Map

Field	Description	Cisco IOS CLI Equivalent
Add ISDN Map	Click to configure the following options to override with custom values the default ISDN type and plan that the router generates. You can add multiple instances of these options so that you can configure different ISDN mapping options for different ports.	—

Field	Description	Cisco IOS CLI Equivalent
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Digit Range	Enter a digit or range of digits to map to ISDN telephone numbers that are used internally	**isdn map address {{** *address* **|** *reg-exp***} plan** *plan* **type** *type* **| transparent}**
Plan	Choose an ISDN numbering plan: • **data**: X.121 data numbering plan • **isdn**: E.164 ISDN/Telephony numbering plan • **national**: Number called to reach a subscriber in the same country, but outside the local network • **privacy**: Private numbering plan • **reserved/*extension***: Reserved for the extension	**isdn map address {{** *address* **|** *reg-exp***} plan** *plan* **type** *type* **| transparent}**
Type	Choose an ISDN number type: • **abbreviated**: Abbreviated representation of the complete number as supported by your network • **international**: Number called to reach a subscriber in another country • **national**: Number called to reach a subscriber in the same country, but outside the local network • **reserved/5**: Reserved for the extension	**isdn map address {{** *address* **|** *reg-exp***} plan** *plan* **type** *type* **}**
Action	Click the **Recycle Bin** icon to delete the corresponding ISDN Map options instance.	—

Shutdown

Field	Description	Cisco IOS CLI Equivalent
Add Shutdown	Click to configure to disable or enable the controller, serial interface, or voice port that is associated with the interface port. You can add multiple instances of these options so that you can configure different shutdown options for different ports.	—
Port ID	Enter the port or ports to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—
Controller	Enable this option to shut down a controller.	**controller e1/t1** *slot*/*sub-slot*/*port* **shutdown**
Serial	Check this check box to shut down a serial interface.	**interface** **serial** *slot*/*sub-slot*/**port:**{ **15** | **23**} **shutdown**
Voice Port	Check this check box to shut down a voice port.	**voice-port** *slot*/*sub-slot*/**port:**{ **15** | **23**} **shutdown**
Action	Click the **Recycle Bin** icon to delete the corresponding Shutdown options instance.	—

Line Params

Field	Description	Cisco IOS CLI Equivalent
Add Line Params	Click to configure options for adjusting various line parameters for the port or ports. You can add multiple instances of these options so that you can configure different line parameters for different ports .	—
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—

Field	Description	Cisco IOS CLI Equivalent
Gain	Enter the amount of gain, decibels (dB), for voice input. Range: Integers –6 through 14 Default: 0	**input gain** *decibels*
Attenuation	Enter the amount of attenuation, decibels (dB), for transmitted voice output. Range: Integers –6 through 14 Default: 3	**output attenuation** *decibels*
Echo Canceller	Choose **Enable** to apply echo cancellation to voice traffic. This option is disabled by default.	**echo-cancel** *enable*
Voice Activity Detection	Choose **Enable** to apply VAD to voice traffic. This option is disabled by default.	**vad**
Compand Type	Choose the companding standard to be used to convert between analog and digital signals in PCM systems (**U-law** or **A-law**). The default is **U-law**.	**compand-type** {**u-law** | **a-law**}
Call Progress Tone	Choose the locale for the call progress tone.	**cptone** *locale*
Action	Click the **Recycle Bin** icon to delete the corresponding Line Params options instance.	—

Outgoing IE

Field	Description	Cisco IOS CLI Equivalent
Add Outgoing IE	Click to configure the following options for the outgoing Information Element. You can add multiple instances of these options so that you can configure outgoing Information Element options for different ports.	—
Port Range	Enter the port or ports within the voice interface template to which the following option applies. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** so specify ports 1 through 5.	—

Field	Description	Cisco IOS CLI Equivalent
Type	Choose one or more of the following options to specify the Information Elements to pass in outgoing ISDN messages: To remove an option from the field, click its **X** icon. • **called-number**: Indicates the outgoing call number • **called-subaddr**: Indicates the subaddress of the outgoing call • **caller-number**: Indicates the incoming call number • **caller-subaddr**: Indicates the subaddress of the incoming call • **connected-number**: Indicates the number of the remaining caller if a disconnect occurs during a conference • **connected-subaddr**: Indicates the subaddress of the remaining caller if a disconnect occurs during a conference • **display**: Provides information about the text display • **extended-facility**: Provides information about extended facility requests • **facility**: Provides information about facility requests • **high-layer-compat**: Provides information about higher layer compatibility • **low-layer-compat**: Provides information about lower layer compatibility • **network-facility**: Provides information about network facility requests • **notify-indicator**: Provides information about notifications • **progress-indicator**: Provides information about the call in progress • **redirecting-number**: Indicates the number that is redirecting the call • **user-user**: Provides information about the users at either end of the call	**isdn outgoing ie** *type*
Action	Click the **Recycle Bin** icon to delete the corresponding Outgoing IE options instance.	—

Associations

Field	Description
Association	Click to configure options for associating other configured UC voice features with the port or ports. When you associate a feature in this way, the configuration options in that feature are applied to the designated ports. You can add multiple instances of these options so that you can configure different association options for different ports.

Field	Description
Port Range	Enter the port or ports within the voice interface template to which these options apply. Enter a number, a comma separated string of numbers, or a range of numbers separated with a hyphen. For example, enter **1** to specify port 1; **1,2,3** to specify ports 1, 2, and 3; or **1-5** to specify ports 1 through 5.
Trunk Group	Choose a configured Trunk Group feature to associate with the port.
Trunk Group Priority	Enter the priority of the trunk group. The number you enter is the priority of the POTS dial peer in the trunk group for incoming and outgoing calls. Range: Integers 1 through 64
Translation Profile	Choose a configured Translation Profile feature to associate with the port.
Translation Profile Direction	Choose the direction of the traffic to which to apply the selected Translation Profile feature: • **Incoming**: Applies the corresponding Translation Profile feature to traffic that is incoming to the port • **Outgoing**: Applies the corresponding Translation Profile feature to traffic that is outgoing from the port
Supervisory Disconnect	Applies only to FXO voice interface templates. Choose a configured Supervisory Disconnect feature to associate with the port.
Action	Click the **Recycle Bin** icon to delete the corresponding Associations options instance.

Media Profile

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Media Profile feature provides options for configuring the codecs to be available for the SIP trunk communication with remote dial peers, and DTMF relay options to use for SIP calls. You can configure multiple Media Profile features.

The following table describes the options for configuring the Media Profile feature.

Field	Description	Cisco IOS CLI Equivalent
Name	Enter a unique name for the media profile configuration. The name can contain any characters.	—
Description	Enter a description of the media profile configuration.	—

Field	Description	Cisco IOS CLI Equivalent
Media Profile Number	Enter a number for this SIP media profile. Range: Integers 1 through 10000	**voice class codec** *tag-number*
DTMF Target	Choose the DTMF relay options that you want the system to use for SIP calls: • **rtp-nte**: Real-Time Transport Protocol (RTP) Named Telephone Events (NTE). An in-band DTMF relay method, which uses RTP Named Telephony Event (NTE) packets to carry DTMF information instead of voice. • **sip-notify**: A Cisco proprietary out-of-band DTMF relay mechanism that transports DTMF signals using SIP NOTIFY messages. • **sip-kpml**: Keypad Markup Language (KPML) is used to indicate DTMF tones in SIP messaging. It transmits DTMF tone indications via SIP NOTIFY messages Choose the option that you want to have the highest priority. Then choose the option that you want to have the next highest priority. Continue in this way to choose a third option. The options in the field appear in descending order of priority, with the highest priority option appearing first. To remove an option from the field, click its **X** icon. To change the priority order of options, remove the options and add them back in the desired order.	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Codec List	Choose the codecs that you want to be made available for the SIP trunk to use when communicating with the remote dial peer. Choose the codec that you want to have the highest priority. Then choose the codec that you want to have the next highest priority. Continue in this way to choose other codecs. The codecs in the field appear in descending order of priority, with the highest priority option appearing first. To remove a codec from the field, click its **X** icon. To change the priority order of codecs, remove the codecs and add them back in the desired order.	**voice class codec** *tag-number* **codec preference** *value codec-type*

SRST

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The SRST feature provides options for configuring parameters for Cisco Unified Survivable Remote Site Telephony (SRST) for SIP. With Cisco Unified SRST, if the WAN goes down or is degraded, SIP IP phones

in a branch site can register to the local gateway (device) so that they continue to function and provide PSTN breakout services without requiring the WAN resources that are no longer available.

The following tables describe the options for configuring the SRST feature.

Field	Description
Name	Enter a unique name for the SRST configuration. The name can contain any characters.
Description	Enter a description of the SRST configuration.

Global

Field	Description	Cisco IOS CLI Equivalent
Max Phones	Enter the number of phones that the system can register to the local gateway when the gateway is in Cisco Unified SRST mode.	**voice register global** **max-pool** *max-voice-register-pools*
Max Directory Numbers	Enter the number of directory numbers that the gateway supports when the gateway is in Cisco Unified SRST mode. The maximum values that you can enter depend on the device that you are configuring.	**voice register global** **max-dn** *max-directory-numbers*
Music on Hold	Enable this option to play music on hold on endpoints when a caller is on hold and the gateway is in Cisco Unified SRST mode.	—
Music on Hold File	Enter the path and filename of the audio file for music on hold. The file must be in the system flash and must be in the .au or .wav format. In addition, the file format must contain 8-bit 8-kHz data, for example, CCITT a-law or u-law data format.	**call-manager-fallback** **moh** *filename*
System Message	Enter a message that displays on endpoints when Cisco Unified SRST mode is in effect.	**voice register global** **system message** *string*

Phone Profile

Field	Description	Cisco IOS CLI Equivalent
Add New Phone Pool Profile	Click to configure the options for providing registration permission control and certain dial-peer attributes that are applied to the dynamically created VoIP dial peers when SIP phone registrations match the pool You can add multiple instances of these options so that you can configure different options for different pool tags.	—

Field	Description	Cisco IOS CLI Equivalent
Pool Tag	Enter the unique sequence number of the set of SIP phones to be configured. Range: Integers 1 to the number of phones that you configured with the **Max Phones** option.	**voice register pool** *pool-tag*
IPv4/6 Network Access	Enter the IPv4 or IPv6 prefix of the network that contains the set of SIP phones to be configured.	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]
Action	Click the **Recycle Bin** icon to delete the corresponding Phone Profile options instance.	—

Call Forward

Field	Description	Cisco IOS CLI Equivalent
Add New Call Forward	Click to configure the options for forwarding incoming voice calls to SIP phones. You can add multiple instances of these options so that you can configure different options for different pool tags.	—
Pool Tag	Enter one of the pool tags that you defined for the phone profile to associate with call forwarding actions.	—
Action	Choose the situation that causes a directory number to be forwarded to another directory number when the gateway is in SRST mode: • **busy**: Forwards a call to another directory number when a phone is busy • **all**: Forwards all incoming calls to another directory number • **noan**: Forwards a call to another directory number when no answer is received after a configured timeout	**call-forward b2bua all** {*number* **|** **busy** *number* **|** **noan** *number* [**timeout** *seconds*]}
Digit String	Enter the directory number to which forwarded calls are sent.	**call-forward b2bua all** {*number* **|** **busy** *number* **|** **noan** *number* [**timeout** *seconds*]}
Timeout	For a call forward **noan** action, enter the number of seconds that a call rings with no answer after which the call is forwarded to the directory number that the**Digit String** option defines. Range: Integers 3 to 60000 Default: 20	**call-forward b2bua noan** {*number* [**timeout** *seconds*]}

Field	Description	Cisco IOS CLI Equivalent
Action	Click the **Recycle Bin** icon to delete the corresponding Call Forward options instance.	—

Association

Field	Description
Association	Click to configure options for associating other configured UC voice features with the port or ports. When you associate a feature in this way, the configuration options in that feature are applied to the designated set of SIP phones. You can add as multiple instances of these options so that you can configure different association options for different phone pools.
Pool Tag	Enter the unique sequence number of the set of SIP phones to be configured.
Media Profile	Choose a configured Media Profile feature to associate with the phone pool profile.
Translation Profile	Choose a configured Translation Profile feature to associate with the port.
Translation Profile Direction	Choose the direction of the traffic to which to apply the selected Translation Profile feature: • **Incoming**: Applies the corresponding Translation Profile feature to traffic that is incoming to the port • **Outgoing**: Applies the corresponding Translation Profile feature to traffic that is outgoing from the port
Action	Click the **Recycle Bin** icon to delete the corresponding Association options instance.

Server Group

Minimum supported releases: .

Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Server Group feature lets you configure a group of up to five destination SIP servers for an outbound dial peer.

When a call matches a dial peer that is configured with a server group, the destination is selected from the list of servers based on the Server Group feature configuration.

When you associate a server group with an outbound dial peer, the session target information in the dial plan must point to the provisioned server group

The following tables describe the options for configuring the Server Group feature

Field	Description
Name	Enter a unique name for the server group configuration. The name can contain any characters.

Field	Description
Description	Enter a description of the server group configuration.

Basic Configuration

Field	Description	Cisco IOS CLI Equivalent
Server Group ID	Enter a unique identification number for this server group. Range: Integers 1 through 10000	**voice class server-group** *server-group-id*
Description	Enter a description of this server group.	**description** *string*
Hunt Scheme	Choose the hunt method for the order of selection of target server IP addresses, which are IP addresses of the servers in the server group, for setting up outgoing calls. (Server addresses are configured as described in the following **Address List** table.) Options are: • **none**: No hunt scheme defined. If a hunt scheme is not defined, an available IP address of the highest **Preference** value is selected. (The preference is configured as described in the following **Address List** table.) • **round-robin**: Searches IP addresses in turn for the next available server, starting with the server that follows the last used member of the server group.	**hunt-scheme round-robin**
Shutdown	Enable this option to put this server group in shutdown mode, which causes the outbound SIP dial peers that use this server group to be out of service.	—

Address List

Field	Description	Cisco IOS CLI Equivalent
Add Address List	Click to configure options for adding a server to the server group. You can add up to 5 instances of these options that you can add up to 5 servers to the server group.	—
IPv4/6 Address	Enter the IPv4 or IPv6 address of the server.	**ipv4**|**ipv6**} *address*
Port	Enter the number of the server port that is listening for SIP calls.	**port** *port*

Field	Description	Cisco IOS CLI Equivalent
Preference	Applies only if the **Hunt Scheme** Basic Configuration option is set to **none**. Choose the order of selection preference of the server for the setting up of outgoing calls. Range: Integers 0 (highest preference) through 5 (lowest preference) Default: 0	**preference** *preference-order*
Action	Click the **Recycle Bin** icon to delete the corresponding Address List options instance.	—

Hunt Stop Rules

Field	Description	Cisco IOS CLI Equivalent
Add Hunt Stop Rules	Click to configure options for configuring a hunt stop rule. This rule stops hunting for servers in the server group based on configured SIP response codes. You can add up to 10,000 instances of these options so that you can configure different hunt stop rules for different response codes.	—
Rule ID	Enter the identifier of the hunt stop rule. Range: Integers 1 through 1000	**huntstop** *rule-tag* **resp-code** *from_resp_code* to *to_resp_code*
Response Code Start	Enter the first SIP response code in a range of codes for the hunt stop rule. Range: Integers 400 through 599	**huntstop** *rule-tag* **resp-code** *from_resp_code* to *to_resp_code*
Response Code End	Enter the last SIP response code in a range of codes for the hunt stop rule. For example, huntstop 1 resp-code 401. Range: Integers 400 through 599	**huntstop** *rule-tag* **resp-code** *from_resp_code* to *to_resp_code*
Action	Click the **Recycle Bin** icon to delete the corresponding Hunt Stop Rules options instance.	—

Supervisory Disconnect

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Supervisor Disconnect feature provides options for configuring supervisory disconnect events.

The following tables describe the options for configuring the Supervisory Disconnect feature.

Field	Description
Name	Enter a unique name for the supervisory disconnect configuration. The name can contain any characters.
Description	Enter a description of the supervisory disconnect configuration.

Custom CPTone

Field	Description	Cisco IOS CLI Equivalent
Add Custom CPTone	Click to configure options for custom call progress tones for a supervisory disconnect event. You can add as multiple instances of these options so that you can configure different dual-tone options for a supervisory name.	—
Supervisory Name	Enter a name for the supervisory disconnect event. The name can contain up to 32 characters. Valid characters are letters, numbers, dashes (-), and underscores (_).	**voice class custom-cptone** *cptone-name*
Dualtone	Choose the type of dual-tone that causes a supervisory disconnect event: • **Busy** • **Disconnect** • **Number Unobtainable** • **Out of Service** • **Reorder** • **Ringback**	**dualtone {ringback | busy | reorder | out-of-service | number-unobtainable | disconnect}**
Cadence	Enter the cadence interval, in ms, of the dual-tones that cause a supervisory disconnect event. Enter the cadence as an on/off value pair, separated with a space. You can enter up to 4 on/off value pairs, separated with spaces.	**cadence** *cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time* [*cycle-3-on-time cycle-3-off-time* [*cycle-4-on-time cycle-4-off-time*]]]
Dualtone Frequency	Enter the frequency, in Hz, for each tone in the dual tone. Range for each tone: Integers 300 through 3600	**frequency** *frequency-1 [frequency-2]*
Action	Click the **Recycle Bin** icon to delete the corresponding Custom CPTone options instance.	—

Dual Tone Detection Params

Field	Description	Cisco IOS CLI Equivalent
Add Dual Tone Detection Params	Click to configure the following options for dual-tone detection parameters for a supervisory disconnect event. You can add multiple instances of these options.	—
Supervisory Number	Enter a unique number to identify dual-tone detection parameters. Range: Integers 1 through 10000	**voice class dualtone-detect-params** *tag-number*
Cadence-Variation	Enter the maximum time, in ms, by which the tone onset can vary from the specified onset time and still be detected. The system multiplies the value that you enter by 10. Range: Integers 0 through 200 (0 through 2000 ms) Default: 10 (100 ms)	**cadence-variation** *time*
Frequency Max Delay	Enter the maximum delay, in milliseconds, before a supervisory disconnect occurs after the dual-tone is detected. The system multiplies the value that you enter by 10. Range: Integers 0 through 100 (0 through 1000 ms) Default: 10 (100 ms)	**freq-max-delay** *time*
Frequency Max Deviation	Enter the maximum deviation, in Hz, by which each tone can deviate from configured frequencies and be detected. Range: Integers 0 through 125 Default: 10	**freq-max-deviation** *hertz*
Frequency Max Power	Enter the power of the dual-tone, in dBm0, above which a supervisory disconnect is not detected. Range: Integers 0 through 20 Default: 10	**freq-max-power** *dBm0*
Frequency Min Power	Enter the power of the dual-tone, in dBm0, below which a supervisory disconnect is not detected. Range: Integers 0 through 35 Default: 3	**freq-min-power** *dBm0*
Frequency Power Twist	Enter the difference, in dBm0, between the minimum power and the maximum power of the dual-tone above which a supervisory disconnect is not detected. Range: Integers 0 through 15 Default: 6	**freq-power-twist** *dBm0*

Field	Description	Cisco IOS CLI Equivalent
Action	Click the **Recycle Bin** icon to delete the corresponding Dual Tone Detection Params options instance.	—

Translation Profile

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Translation Profile feature provides options for configuring translation profiles.

The following table describes the options for configuring the Translation Profile feature.

Note You must configure the Translation Rule feature before you can configure the Translation Profile feature.

Field	Description
Name	Enter a unique name for the translation profile configuration. The name can contain any characters.
Description	Enter a description of the translation profile configuration.

Basic Configuration

Field	Description	Cisco IOS CLI Equivalent
Name	Enter a unique name for the translation profile. If you do not enter a name, "Translation Profile" is used as the name.	—
Add Translation Profile Configuration	Click to configure options for mapping rules that are defined by the Translation Rule feature for calling and called numbers. You can add up to 2 instances of these options, one instance for the **calling** call type and one for the **called** call type.	—
Select Call Type	Choose the type of call to which to map a translation rule set: • **calling**: Maps a translation rule set for the number that is calling in • **called**: Maps a translation rule set for the number that is being called	• Calling: **translate calling** *translation-rule-number* • Called: **translate called** *translation-rule-number*

Field	Description	Cisco IOS CLI Equivalent
Select Translation Rule	Choose a provisioned Translation Rule feature to associate with to the call type that you chose.	—
View Rule	Click to view the translation rule that you chose.	—

Translation Rule

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Translation Rule feature provides options for creating translation rules for calling and called numbers. You can create up to 100 translation rules for a card.

The Translation Rule feature is used to match called party or calling party numbers for configured digit manipulation. Because the Translation Rule feature can contain a set of rules, it can be used to match one or more patterns of numbers and have each pattern manipulated in a different way.

The following table describes the options for configuring the Translation Rule feature.

Field	Description
Name	Enter a unique name for the translation rule configuration. The name can contain any characters.
Description	Enter a description of the translation rule configuration.

Basic Settings

Field	Description	Cisco IOS CLI Equivalent
Translation rule set number	Enter a unique number to assign to a translation rule set that you are creating.	**voice translation rule** *number*
Import	Click to copy translation rules from a CSV file to Cisco Catalyst SD-WAN Manager.	—
Export	Click to save existing translation rules that your created in a CSV file.	—
Add Rule	Click to configure the options for the Translation Rule feature.	—
Rule number	Displays a number that designates the precedence for this rule.	—
Matching pattern	Enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash.	—

Field	Description	Cisco IOS CLI Equivalent
Action	Choose one of the following options to designate the action that the system performs for calls that match the string in the **Matching pattern** field: • **reject**: Causes the system to reject the call. • **replace**: Causes the system to replace the string in the **Matching pattern** field with a string that you specify.	**voice translation-rule** *number* • Match and replace rule: **rule** *precedence* */match-pattern/ / replace-pattern/* • Reject rule: **rule** *precedence* **reject** */match-pattern/*
Replacement pattern	If you choose the **replace** action for the rule, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string. To include the backslash character (\) in a replace string, precede the backslash with a backslash. For example, if you specify a matching pattern of /^9/ and a replacement pattern string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212.	—
Action	Click the **Recycle Bin** icon to delete the corresponding Rule options instance.	—

Trunk Group

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Trunk Group feature provides options for configuring voice ports as members of a trunk group. You can configure one trunk group for a voice card.

The following tables describe the options for configuring the Trunk Group feature.

Field	Description
Name	Enter a unique name for the trunk group configuration. The name can contain any characters.
Description	Enter a description of the trunk group configuration.

Basic Settings

Field	Description	Cisco IOS CLI Equivalent
Name	Enter the name of the trunk group. The name can contain up to 32 characters.	**trunk group** *name*
Hunt Scheme	Choose the hunt scheme in the hunt group for outgoing calls. **Note** Depending on the hunt scheme that you choose, the **Channel** field, **Direction** field, or both appear. • **least-idle**: Searches for an idle channel with the shortest idle time • **least-used**: Searches for a trunk group member that has the highest number of available channels (applies only to PRI ISDN cards) • **longest-idle**: Searches for an idle channel with the longest idle time **round-robin**: Searches trunk group members in turn for an idle channel, starting with the trunk group member that follows the last used • **sequential**: Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk group • **random**: Searches for a trunk group member at random and selects a channel from the member at random	**hunt-scheme least-idle** [**even** | **odd** | **both**] **hunt-scheme least-used** [**even** | **odd** | **both** [**up** | **down**] **hunt-scheme longest-idle** [**even** | **odd** | **both**] **hunt-scheme random** **hunt-scheme round-robin** [**even** | **odd** | **both** [**up** | **down**] **hunt-scheme sequential** [**even** | **odd** | **both** [**up** | **down**]
Max Calls In	Enter the maximum number of incoming calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of incoming calls. If the maximum number of incoming calls is reached, the trunk group becomes unavailable for more calls. Range: Integers 0 through 1000	**trunk group** *name* **max-calls** **voice** *number-of-calls* **direction in**
Max Calls Out	Enter the maximum number of outgoing calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of outgoing calls. If the maximum number of outgoing calls is reached, the trunk group becomes unavailable for more calls. Range: Integers 0 through 1000	**trunk group** *name* **max-calls** **voice** *number-of-calls* **direction out**

Field	Description	Cisco IOS CLI Equivalent
Channel	This option does not appear when the **Hunt Scheme** option is set to **random**. Choose the type of channel that the hunt scheme searches for: • **Both**: Searches both even- and odd-numbered channels. • **Even**: Searches for an idle even-numbered channel. If no idle even-numbered channels are available, an odd-numbered channel is sought. • **Odd**: Searches for an idle odd-numbered channel. If no idle odd-numbered channels are available, an even-numbered channel is sought.	—
Direction	This option appears when the **Hunt Scheme** option is set to **round-robin** or **sequential**. Choose the order in which the hunt scheme searches for channels: • **up**: Searches channels in ascending order within a trunk group member. • **down**: Searches channels in descending order within a trunk group member.	—
Max Retry	Enter the maximum number of outgoing call attempts that the trunk group makes if an outgoing call fails. If you do not enter a value and a call fails, the system does not attempt to make the call again. Range: Integers 1 through 5	**trunk group** *name* **max-retry** *attempts*

Voice Global

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

The Voice Global feature provides options for configuring system-wide call routing and network clock parameters.

The following tables describe the options for configuring the Voice Global feature

Field	Description
Name	Enter a unique name for the voice global configuration. The name can contain any characters.
Description	Enter a description of the voice global configuration.

Call Routing

Field	Description	Cisco IOS CLI Equivalent
Trusted IPv4/6 Prefix List	Enter a comma separated list of IPv4 or IPv6 addresses with which the router can communicate through SIP. Enter each IPv4 address in CIDR format. For example, 10.1.2.3/32. The router does not communicate with other addresses, which prevents fraudulent calls being placed through the router. A Trusted IPv4 or IPv66 prefix is required for TDM to IP calls.	**voice service voip** **ip address trusted list** **ipv4** *ipv4-address*/*ipv4-network-mask*
Source Interface	Enter the name of the source interface from which the router initiates SIP control and media traffic. This information defines how the return/response to this traffic should be sent.	**voice service voip** **sip** **bind control source-interface** *interface-id* **bind media source-interface** *interface-id*

Network Clock

Field	Description	Cisco IOS CLI Equivalent
Participation	Enable this option to configure all T1 or E1 digital interfaces to participate in the backplane clock. Disable this option to remove the clock synchronization with the backplane clock for the module. Default: Enabled	**network-clock synchronization participate** *slot sub-slot*

Field	Description	Cisco IOS CLI Equivalent
Clock Priority Sorting	Appears only if you have configured a digital interface and selected either a primary or secondary clock source for the interface. Designate the priority of up to 6 clock sources for the digital interface. The drop-down list displays the interface ports for which a primary or secondary clock source is defined and that is configured for network participation. Choose the port that you want to have the highest priority. Then choose the port that you want to have the next highest priority. Continue in this way to choose other ports. The ports in the field appear in descending order of priority, with the highest priority port appearing first. To remove a port from the field, click its **X** icon. To change the priority order of ports, remove the ports and add them back in the desired order. We recommend that all ports in the priority list be of the same type, either E1-PRI or T1-PRI.	**network-clock-input-source** priority **controller [t1|e1]** *slot/sub-slot/port*
Automatically Sync	Choose **true** to enable network synchronization between all modules and the router. Choose **false** to disable network synchronization between all modules and the router. Default: False	**network-clock synchronization automatic**
Wait to restore clock	Enter the amount of time, in ms, that the router waits before including a primary clock source in the clock selection process. Range: Integers 0 through 86400 Default: 300	**network-clock wait-to-restore** *milliseconds*

Voice Tenant

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1.

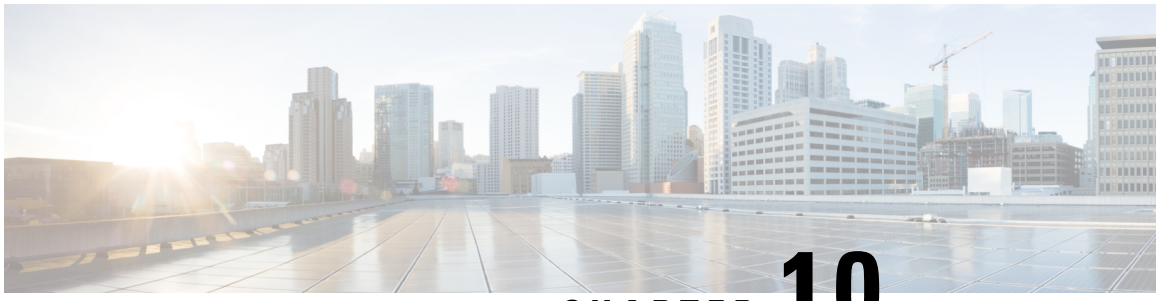
The Voice Tenant feature provides options for configuring SIP-specific attributes for a tenant. The voice tenant configuration can be then applied to individual dial peers.

The following tables describe the options for configuring the Voice Tenant feature.

Field	Description
Name	Enter a unique name for the voice tenant configuration. The name can contain any characters.
Description	Enter a description of the voice tenant configuration.

Basic Configuration

Field	Description	Cisco IOS CLI Equivalent
Tag	Enter a unique name for this voice tenant configuration.	**voice class tenant** *tag*
Bind Interface	Choose the type of packets that are bound to network interfaces for advertising the source IP address of the tenant: • **Both**: Control and media packets • **Control**: Control packets • **Media**: Media packets • **Disabled**: Bind interface is not configured	—
Transport Type	Choose the transport protocol for SIP control signaling for the tenant. Options are **TCP**, **UDP**, and **TCP TLS**.	**session transport** {**udp** | **tcp** [**tls**]}
Bind Control Interface Name	Enter a network interface name for binding control packets.	**bind control source-interface** *interface-id*
Bind Media Interface Name	Enter a network interface name for binding media packets.	**bind media source-interface** *interface-id*



CHAPTER 10

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.

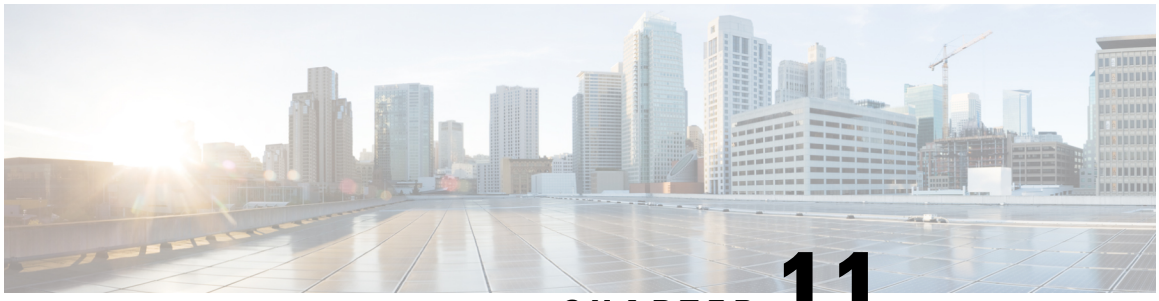
IMC

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 11

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 313.

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 312.

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
   ```

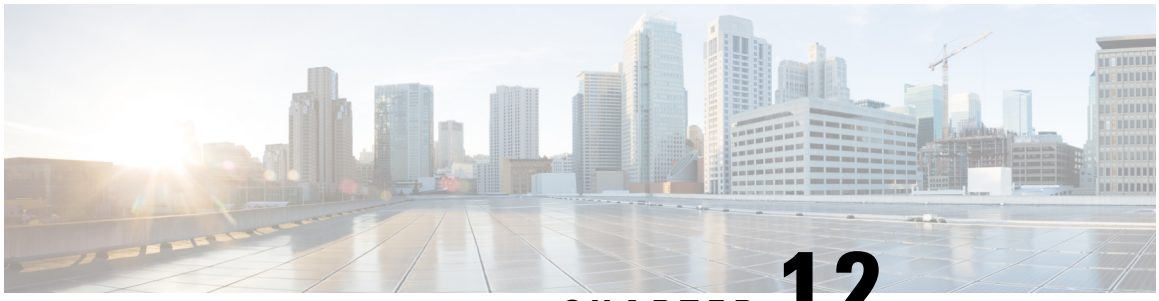
   For more information about type 6 encryption, see Type 6 Passwords on Cisco IOS XE SD-WAN Routers in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

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

6. Click **Save**.

PART III

Part Teleworker (Mobility)



CHAPTER 12

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.
Transport Gateway	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enable transport gateway functionality for the device. A transport gateway connects routers that may or may not have direct connectivity. One common use case for transport gateways is to provide connectivity between routers in disjoint networks, such as between public and private WANs. Another use case for transport gateway functionality is to use a transport gateway as the hub in a hub-and-spoke topology.

Controller Settings

Field	Description
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

Field	Description
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
Affinity Group Number	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter an affinity group number. Range: 1 through 63
Affinity Group Number for VRFs and **Range of VRFs**	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter an affinity group number for a specific range of VRFs. You can click + to configure an affinity group number for additional VRF ranges. Range for affinity group: 1 through 63 Range for VRFs: 1 through 65531
Affinity Group Preference Auto	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Configure automatic affinity preference order. When you use this, a device prefers routes with a lower affinity group number. In this case affinity group numbers are not treated as arbitrary tags, but instead signify route priority, where a lower affinity group number means higher priority.
Affinity Group Preference	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter a comma-separated list of affinity group numbers. In a Multi-Region Fabric scenario, this determines the order of preference for connecting to a gateway. Affinity group preference also used for path filtering when using the **filter route outbound affinity-group preference** command on a Cisco SD-WAN Controller. Range for affinity groups: 1 through 63

GPS

Field	Description
GPS Latitude	Enter the latitude of the device, in the format decimal-degrees.

Field	Description
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.

Field	Description
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES-encrypted key. From Cisco Catalyst SD-WAN Manager Release 20.15.1, when you enter the password as clear text, Cisco SD-WAN Manager encrypts the password. When you view the configuration preview, the password appears in its encrypted form.
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

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 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.
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

Field	Description
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
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.

Field	Description
Allow Service	Allow or disallow the following services on the interface: • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
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.

Field	Description
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
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

Field	Description
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
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.

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.

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.

Field	Description
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.
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.
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.

Field	Description
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
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.

Field	Description
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.
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

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.
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.
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
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

Field	Description
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.
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.
Associated IPv6-Tracker/IPv6-Trackergroup	Choose an IPv6- 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.
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.

Field	Description
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

Field	Description
Tunnel Interface	Enable this option to create a tunnel interface.
Per-tunnel QoS	Enable this option to apply a Quality of Service (QoS) policy on individual tunnels.
Color	Choose a color for the TLOC.
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.
Groups	Enter a group number. Range: 1 through 4294967295
Border	Enable this option to set the TLOC as a border TLOC.

Field	Description
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 100 Default: 2
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
Port Hop	Enable port hopping. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). 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.
CTS SGT Propagation	Enable CTS SGT propagation on an interface.
Network Broadcast	Enable this option to accept and respond to network-prefix-directed broadcasts.

Field	Description
Allow Service	Allow or disallow the following services on the interface: • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
Encapsulation	

Field	Description
Encapsulation*	Choose an encapsulation type: • **gre**: Use GRE encapsulation on the tunnel interface. • **ipsec**: Use IPsec encapsulation on the tunnel interface. **Note** 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. When you choose **gre**, the following fields appear: • **GRE Preference**: Enter 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 When you choose **ipsec**, the following fields appear: • **IPSEC Preference**: Enter 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
Multi-Region Fabric **Note** These options appear only when Multi-Region Fabric is enabled.	
Connect to Core Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to a border router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the access region and core region. • **Keep Exclusive to Core Region**: Use the interface only for the core region.

Field	Description
Connect to Secondary Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to an edge router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the primary and secondary regions. • **Keep Exclusive to Secondary Region**: Use the interface only for the secondary region.

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)

Field	Description

Add Multiple NAT	Choose the NAT type:
	• **Interface**: This is the default value.
	• **Pool**: Configure the following:
	  • **Pool ID**: 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.
	  • **Range Start**: Enter a starting IP address for the NAT pool.
	  • **Range End**: Enter a closing IP address for the NAT pool.
	  • **Prefix length**: Specify the maximum number of source IP addresses that can be NATed in 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
	• **Loopback**: Provide a value for the NAT inside source loopback interface.

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`**.

Fabric Security

Note Before the Cisco Catalyst SD-WAN Manager Release 20.12.1, Fabric Security was called 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 Fabric 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)

Field	Description
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
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.
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).

GRE

Use the GRE feature for all Cisco IOS XE Catalyst SD-WAN devices.

The following tables describe the options for configuring the GRE feature.

Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface. Range: 1 through 255.
Interface Description	Enter a description of the GRE interface.
Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport VPN. Default: No
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

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 IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None

Field	Description
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

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 Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. 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.

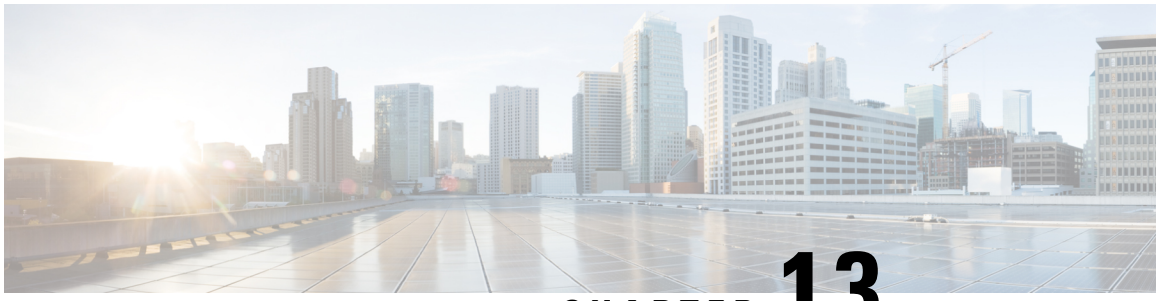
ME IP Config

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.



CHAPTER 13

Troubleshoot Configuration Groups

Overview

This chapter provides links to documents authored by Cisco subject matter experts (SMEs). They aim to help you resolve technical issues without requiring a support ticket. If these documents are unable to resolve your issue, we recommend visiting the applicable Cisco Community. There is a wealth of information and advice available from fellow Cisco customers who may have experienced this issue already and provided a solution. If you are not able to find a resolution on the Community, it may be best that you raise a support ticket at Cisco Support. In cases where a support ticket has to be raised, these documents provide guidance about the data that should be collected and added to the support ticket. Specify the support document you referred, and TAC can create an improvement request with the document owner.

Support Articles

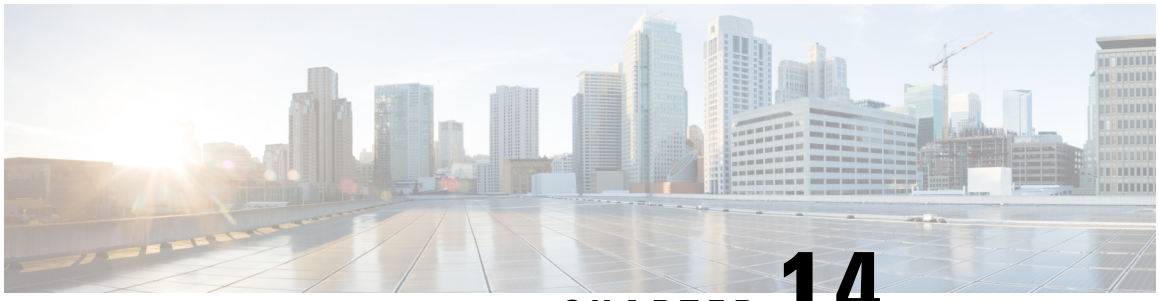
The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following are the support articles associated with this technology:

Document	Description
Configure SD-WAN Edge Router with Configuration Groups	This document describes how to Configure Cisco SD-WAN Edge Routers with Configuration Groups.

PART IV

Part Configuration Catalog



CHAPTER 14

Configuration Catalog

Note Cisco provides the configurations below "as is" for your convenience. These configurations have been built using industry best practices, observed across multiple deployments, which may be beneficial to you. Cisco is not responsible for any technical issues, bugs, or other issues that may arise from your use of these configurations and any resulting indirect, incidental, reliance, consequential, special or exemplary damages or loss of actual or anticipated revenue, profit, business, savings, data goodwill or use, business interruption, damaged data, wasted expenditure or delay in delivery (in all cases, whether direct or indirect).

Configuration Catalog

Table 13: Feature History

Feature Name	Release Information	Description
Configuration Catalog	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature provides a catalog of pre-defined configurations and policies. The Cisco Catalyst SD-WAN Portal hosts the catalog service, which is managed by Cisco. Cisco SD-WAN Manager connects to the cloud-hosted Cisco Catalyst SD-WAN Portal to download catalog entries. You can modify the catalog entries before deploying them to devices in your network.

Information About the Configuration Catalog

The Configuration Catalog feature provides a validated set of configurations and policies that you can use for setting up the Cisco Catalyst SD-WAN network.

Cisco SD-WAN Manager is connected to the catalog service hosted in the Cisco Catalyst SD-WAN Portal. You can enable the connectivity between the catalog portal and Cisco SD-WAN Manager using smart account credentials.

Restrictions for the Configuration Catalog

The catalog service supports only configuration groups, policy groups, and topology groups. There is no support for templates or legacy policies.

Install a Catalog Entry

Before You Begin

Enable **Cloud Services** from the **Administration** > **Settings** > **Cloud Services** page to enable the **Configuration Catalog** page.

1. From the Cisco SD-WAN Manager menu, click **Configuration** > **Configuration Catalog**.
2. Choose the catalog entry label from the **Choose labels** drop-down list to view the available catalogs.
3. Click **View details** on a specific catalog entry to check catalog entry details, detailed description, and customizable and default field information.
4. Click **Install** to install the catalog entry to your configuration or **Uninstall** to uninstall the catalog entry from your configuration.

Note You cannot add additional features to the configurations after it is installed. However, you can copy and modify the features if needed.