Configuration Groups for SD-Routing Devices, Release 17.16.x

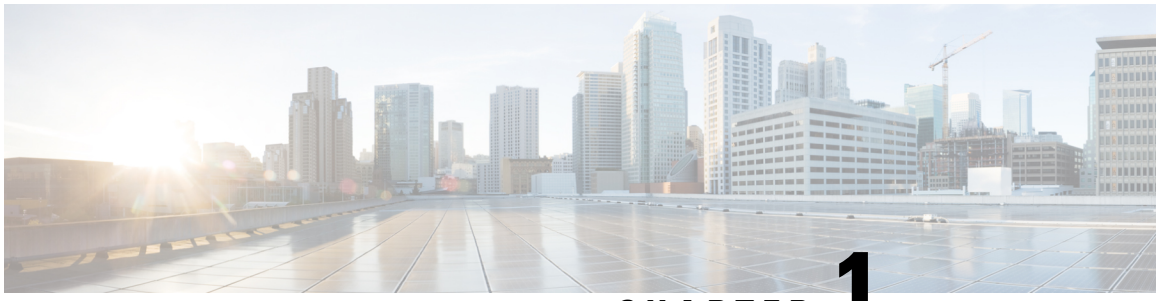
First Published: 2024-04-30

Last Modified: 2024-04-30

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

PART I

New or Changed Features in Configuration Groups



CHAPTER 1

New or Changed Features in Configuration Groups

Configuration Groups provide a simple, reusable, and structured approach for the configurations in Cisco Catalyst SD-WAN Manager. Configuration groups are used to provision SD-Routing devices.

This table provides release and related information for the features explained in this book. These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature History

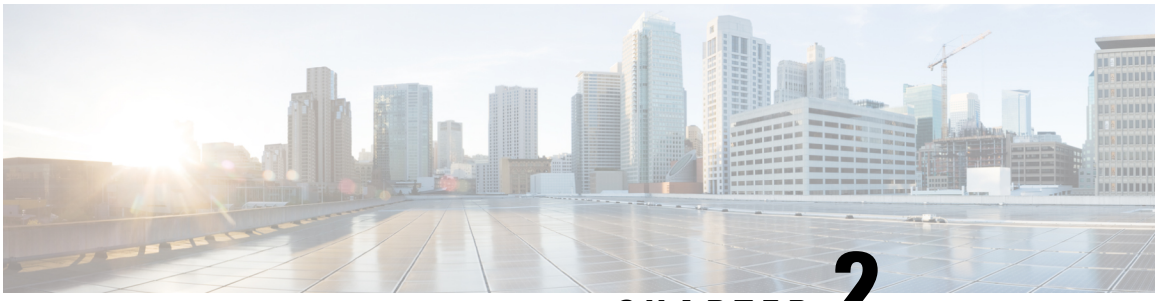
Feature Name	Release Information	Description
Classic CLI	Cisco IOS XE 17.15.1a	This feature provides support for including Cisco IOS XE CLI configuration commands that do not have an associated yang model. When used with the current configuration group, Classic CLI provides a robust provisioning mechanism for SD-Routing devices from Cisco SD-WAN Manager.

Feature Name	Release Information	Description
Configuration Groups and Feature Profiles (Phase III)	Cisco IOS XE 17.15.1a	The following enhancements are introduced in the Configuration Group feature. **Service Profile** • DMVPN • Ethernet Interface • BGP Routing • IPSec • OSPF Routing • OSPFv3 IPv4 Routing • OSPFv3 IPv6 Routing • EIGRP **Transport Profile** • Ethernet Interface • BGP Routing • IPSec • OSPF Routing • OSPFv3 IPv4 Routing • OSPFv3 IPv6 Routing

Feature Name	Release Information	Description
Configuration Groups and Feature Profiles (Phase II)	Cisco IOS XE 17.14.1a	The following enhancements are introduced in the Configuration Group feature. **Service Profile** • ACL IPV4 • ACL IPv6 • Route Policy • VRF • Object Tracker • Object Tracker Group • DHCP Server **Transport Profile** • Transport VPN • Management VPN • ACL IPv4 • ACL IPv6 • Route Policy • VRF • Object Tracker • Object Tracker Group
Configuration Groups and Feature Profiles (Phase I)	Cisco IOS XE 17.13.1a	This release introduces support for the following features in the System Profile: • AAA • Banner • Global • Logging • NTP • SNMP • Flexible Port Speed • CA Certificate
Configuration Group and Feature Profiles	Cisco IOS XE Release 17.13.1a	Configuration Group and Configuration Group Workflow features are introduced.

PART II

Provision SD-Routing Devices Using Configuration Groups



CHAPTER 2

Overview of Configuration Groups for SD-Routing devices

Cisco Catalyst SD-WAN Manager simplifies the provisioning of SD-Routing devices by using Configuration Groups, which provide a structured, reusable approach for creating and applying device-specific configurations. After onboarding a device, the Manager provisions it with the required configurations, streamlining this provisioning process.

Key components of Configuration Groups

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 Manager. 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 - Features are the individual capabilities you want to share across different configuration groups.

To learn more about the different types of feature and feature profiles, along with examples, see, Building Blocks for Profile-based Configuration Groups

Methods to create Configuration Groups

The Configuration Group menu in Cisco Catalyst SD-WAN Manager provides building blocks to assemble configurations for SD-Routing devices. There are two types of Configuration Group, namely, CLI Configuration Group and Profile-based Configuration Group.

Release 17.15.1a/20.15.1 introduces support for including Cisco IOS XE CLI configurations that do not have an associated YANG model, through the Classic CLI feature. The Classic CLI feature, when combined with the current configuration group offers a robust provisioning mechanism for your SD-Routing devices.

For New Devices

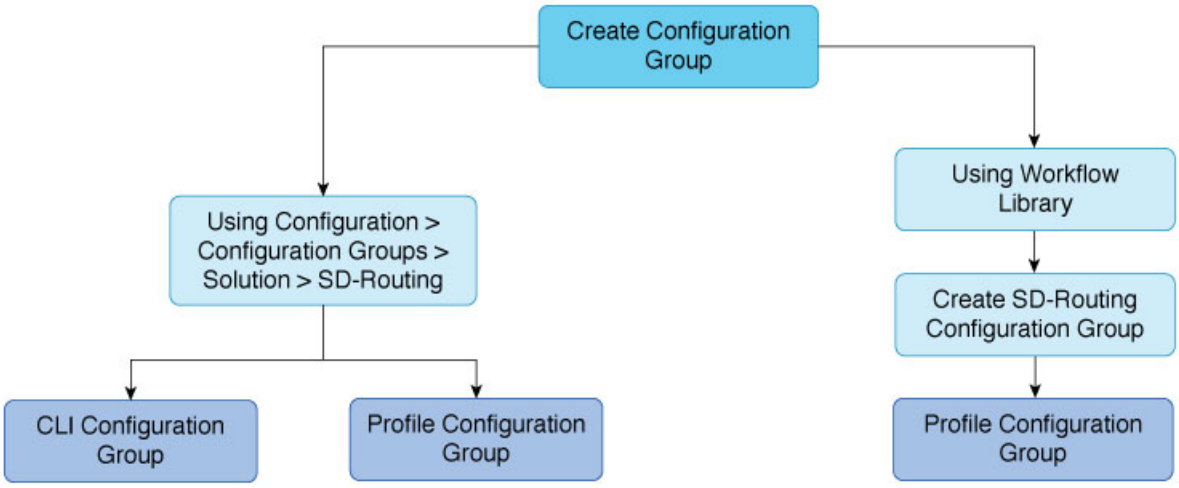
New devices can use profile-based configuration groups for easier setup, allowing you to define your configuration intent using profile building blocks in the UI. This approach integrates with feature profiles and CLI Add-On profiles for comprehensive configuration management and also supports Classic CLI. Alternatively, you can use CLI configuration group as it eliminates the need to map all existing configurations to feature profiles.

For Existing Devices

CLI configuration group is the preferred choice for existing devices as it provides faster configuration and supports Classic CLI. Alternatively, you can also use the profile-based configuration group which provides integration with feature profiles and CLI Add-On profiles for comprehensive configuration management.

Both these Configuration Group Types can be used for existing and new devices. While each method has its strengths, it's important to consider their practical applications and benefits to ensure optimal configuration.

Cisco Catalyst SD-WAN Manager provides multiple ways to create configuration groups



1 Create SD-Routing Configuration Groups using Configuration Group menu, on page 10
2 Create a SD-Routing Configuration Group using the Workflow Library, on page 23
3 Create Configuration Groups using CLI Configuration Group, on page 11
4 Create Configuration Groups using Profile Configuration Group, on page 13
5 Create Configuration Groups using Profile Configuration Group, on page 13

- Prerequisites for using Configuration Groups, on page 8
- Supported devices for Configuration Groups, on page 9
- Create SD-Routing Configuration Groups using Configuration Group menu, on page 10
- Associate and deploy the Configuration Group to an SD-Routing device, on page 15
- Disassociate a device from Configuration Group, on page 22
- Create a SD-Routing Configuration Group using the Workflow Library, on page 23
- Deploy SD-Routing devices using the Deploy Configuration Group Workflow, on page 23
- Release a console, on page 24

Prerequisites for using Configuration Groups

- Cisco SD-Routing devices should be on a minimum software version of Cisco IOS XE Release 17.15.1a to use configuration groups in Cisco SD-WAN Manager. The minimum software version for SD-WAN Manager should be 20.15.1.
- Cisco SD-WAN Manager version should be equal to or greater than the edge version.

  Releases 17.x refers to IOS-XE on the Routers and releases 20.x refers to the SD-WAN Manager.

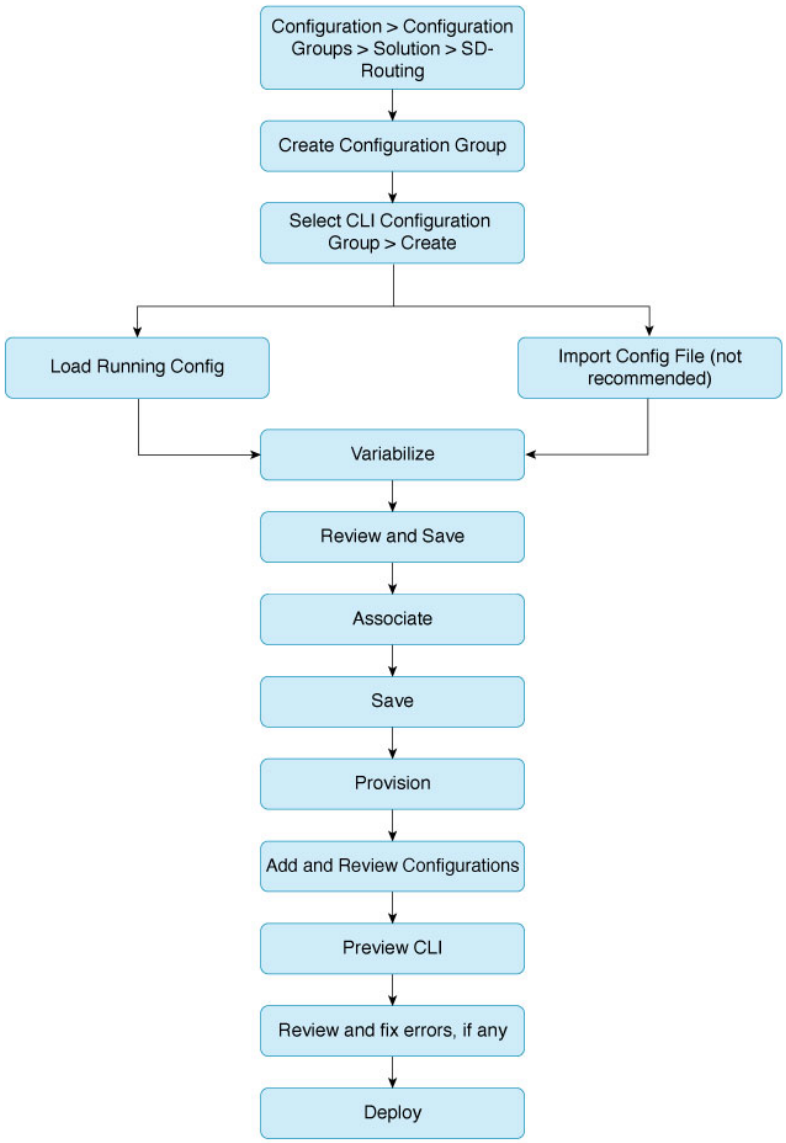
Supported devices for Configuration Groups

Configuration Group provisioning is supported on the following platforms.

- Cisco Catalyst 8000V Series Edge Platforms, Cisco Catalyst 8200 Series Edge Platforms, Cisco Catalyst 8300 Series Edge Platforms, Cisco Catalyst 8500 Series Edge Platforms.
- Cisco 1000 Series Integrated Services Routers. However, ISR1100-4G/6G and ISR1100X-4G/6G do not support SD-Routing mode.
- Cisco Catalyst IR1100 Rugged Series Routers, Cisco Catalyst IR1800 Rugged Series Routers, Cisco Catalyst IR8140 Heavy Duty Router and Cisco Catalyst IR8300 Rugged Series Router.

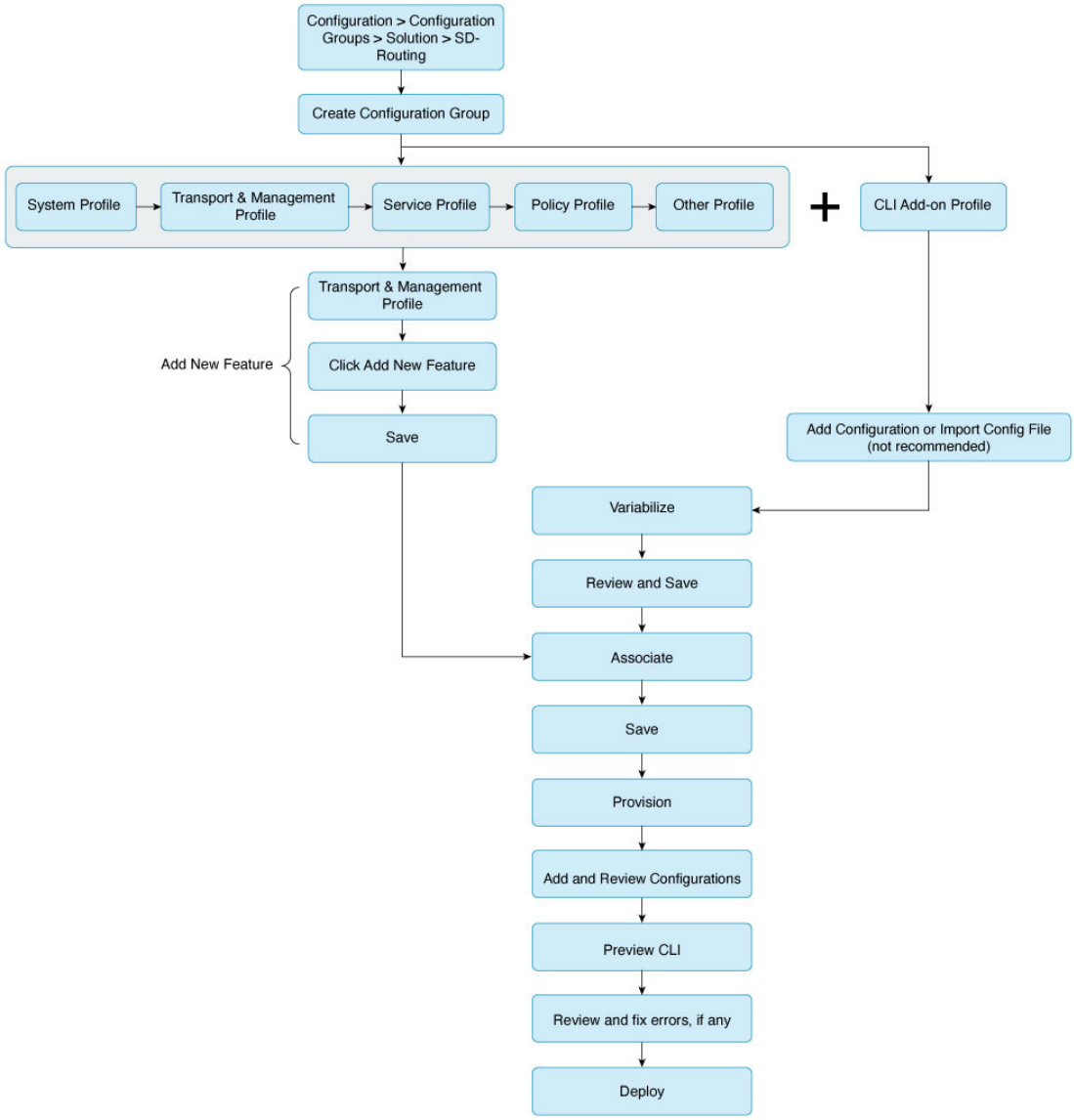
Create SD-Routing Configuration Groups using Configuration Group menu

Workflow to create SD-Routing Configuration Groups using CLI Configurations Group



1 Create Configuration Groups using CLI Configuration Group, on page 11

Workflow to create SD-Routing Configuration Groups using Profile Based Configuration Group



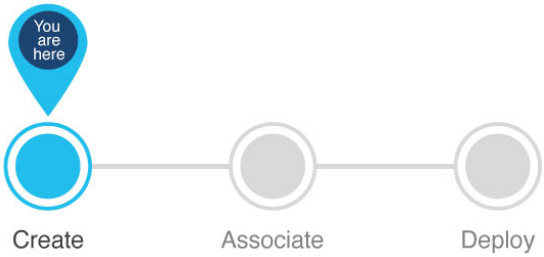
1 Create Configuration Groups using Profile Configuration Group, on page 13

Create Configuration Groups using CLI Configuration Group

The **Configuration Groups** menu on Cisco Catalyst SD-WAN Manager provides a user friendly method to create configuration groups for SD-Routing devices. After onboarding existing SD-Routing devices into Cisco SD-WAN Manager, use the **CLI Configuration Group** to load the device's running configurations, modify and deploy the configurations to these devices.

To create a CLI configuration group for SD-Routing devices, perform the outlined procedure.

The progress bar is a visual indication of the steps that you are expected to complete in the module before you move on to the next configuration step.



Before you begin

Ensure that you have an understanding of the configurations needed for your deployment.

Procedure

Step 1 From Cisco SD-WAN Manager main menu, go to **Configuration** > **Configuration Groups** and select **Solution** as SD-Routing.

Step 2 Click **Create Configuration Group**.

Step 3 Add a name and description, select the checkbox **CLI Configuration Group** and click **Create**.

Step 4 On the **CLI** pane, select a device from the drop-down list and load the running configuration from a reachable device. If your device has configurations that do not have an associated YANG model, a prompt suggests including those configurations. Click **Yes** to proceed. If you click **No**, Classic CLI will not be added.

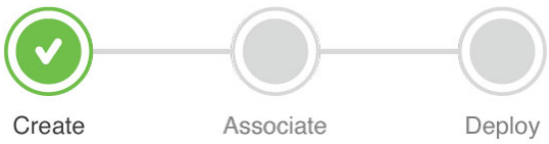
Alternatively, you can import a configuration file from an existing device by clicking **Action** in the top-right corner of the CLI pane and selecting **Import Config File**. Note, this method is not recommended as you will not be notified if your device has configurations that do not have an associated YANG model.

Step 5 You can use a single configuration across multiple devices of the same device models. To convert an actual configuration value to a variable, select the value and click **Action** > **Create Variable**. Enter the variable name and click **Create Variable.** You can also type the variable name directly, in the format {{variable-name}}. For example,{{hostname}}.

Note, Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.

Step 6 On the **Classic CLI** pane, review these configurations and click **Save** to create the Configuration Group.

This successfully concludes the creation of Configuration Group.



What to do next

Associate and deploy the Configuration Group to an SD-Routing device, on page 15

Create Configuration Groups using Profile Configuration Group

The **Configuration Groups** menu on Cisco Catalyst SD-WAN Manager provides a user friendly method to create configuration groups for SD-Routing devices. The building blocks: feature profiles, features and subfeatures, can be quickly assembled to create the configuration group and deployed to provision the SD-Routing devices.

The term **Profile Configuration Group** is used to distinguish between configuration group types. However, in the Cisco Catalyst SD-WAN Manager interface, it is labeled as Configuration Group. To create a profile-based configuration group for SD-Routing devices, perform the outlined procedure.

To create a profile based configuration group for SD-Routing devices, perform the outlined procedure.

Before you begin

Ensure that you have an understanding of the configurations needed for your deployment.

Procedure

Step 1 From Cisco SD-WAN Manager main menu, go to **Configuration** > **Configuration Groups** and select **Solution** as SD-Routing.

Step 2 Click **Create Configuration Group**.

Step 3 Add a name and description, and click **Create**.

Step 4 Createthe required feature profile(s). The available profiles are **System Profile**, **Transport & Management Profile**, **CLI Add-on Profile**, **Service Profile** and **Policy Profile**.

Step 5 Add features tothese feature profiles. To know how to add features, refer to Add a Feature to a Feature Profile. To know more about the different types of features and feature profiles, along with examples, see, Building Blocks for Profile-based Configuration Groups

Step 6 Createa **CLI Add-on Profile** to add device configurations that are not available through other configuration group features. You can add these commands in the **CLI Configuration** area or click **Action** > **Import Config File** to import a configuration and save the configurations.

Step 7 (Optional) If you want to add configurations that do not have associated YANG models, click **Action** and select the **Classic CLI** pane and enter the configurations.

Step 8 You can use a single configuration across multiple devices of the same device models. To convert an actual configuration value to a variable, select the value and click **Action** > **Create Variable**. Enter the variable name and click **Create Variable.** You can also type the variable name directly, in the format {{variable-name}} . For example, {{hostname}}.

Note, Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.

Step 9 Review these configurations and click **Save** to create the configuration group

What to do next

Associate and deploy the Configuration Group to an SD-Routing device, on page 15

Add a Feature to a Feature Profile

Before you begin

You should have created a profile based configuration group earlier.

Procedure

Step 1 From **Cisco Catalyst SD-WAN Manager**, select the **SD-Routing configuration group** and click the **down arrow** on the right.

Step 2 Select the feature profile and edit using the **Pencil icon**.

Step 3 Click **Add New Feature** and choose a feature from the drop-down list.

Step 4 Enter a name and description for the feature.

Step 5 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. Select your preference as described in the table.

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.

Step 6 Add features as required.

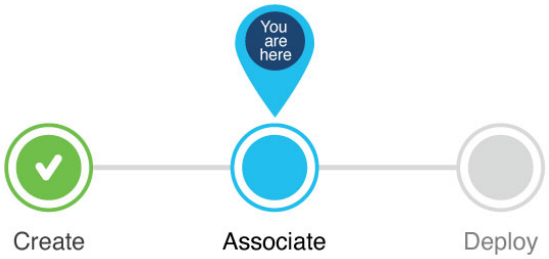
Step 7 Click **Save** to add the feature to the Feature profile.

What to do next

Associate and deploy the Configuration Group to an SD-Routing device, on page 15

Associate and deploy the Configuration Group to an SD-Routing device

This task involves reviewing configurations in the configuration group, associating the device with the configuration group, and provisioning one or more SD-Routing devices.



Before you begin

Ensure that the configuration group you select is a SD-Routing configuration group. For details on how to create Configuration Group, refer, Create SD-Routing Configuration Groups Using Configuration Group Menu

Procedure

Step 1 From Cisco SD-WAN Manager, select the **Configuration Group** created earlier.

Step 2 Click **+ Add** and select the devices from the list. Click **Save** to attach the configuration group to the selected devices.

Step 3 To provision the configuration changes, click **Deploy**.

Step 4 Select the device on which you prefer to provision the configuration changes. Click **Next**

Step 5 Add and review device configurations. Edit the table to include the variable values per device, for example, System IP and Site IDs. Alternatively, you can export the table as a CSV file, manually edit the variables in the file, and then re-import it. Once the configurations are updated, click **Next** to proceed.

Step 6 To preview deviceconfiguration changes, click **Preview CLI**.

If there are discrepancies in the syntax of the device configuration, a Config Group Validation Error message appears in the top-left corner of the preview screen, highlighting the issue.

Validation errors can be classified as:

Table 2: Error types

Error Type	resU nitA

Syntax Error
Following is an example output of a syntax error caused by an invalid command.
`Config Group validation error:`
`Configuration validation failed with error: --------^syntax error:`
`expecting log - Error:login on-success logs`
Following is an example output of a syntax error caused by an incorrect value.
`[2-Apr-2025 15:27:27 UTC] Failed to deploy device with Config Group`
`- sd_routing, ip address syntax error: "10.1.15.16.abcd" is not a valid`
`value.`
`Error: ip address 10.1.15.16.abcd 255.255.255.0`
Following is an example output of a syntax error caused by an unknown command.
`Config Group validation error:`
`Configuration validation failed with error:`
`syntax error: unknown command`
`Error abcd`	

Error Type	

Error Type	
Unknown Error	

a) Once the corrections are made, go back to the Deploy Configuration Group workflow, click **Deploy** to provision the configuration changes on the device and review the changes again.
b) Select the device to review the configuration changes on the **CLI** pane and on the **Classic CLI** pane either inline or side by side. The configurations that are removed are highlighted in red and the new configuration is highlighted in green. The **Classic CLI** pane also shows Cisco IOS XE CLI commands that do not have associated YANG models, submitted as part of configuration commands.

Step 7 Click **Deploy** to proceed with deployment.

This concludes the workflow of Creating, Associating and Deploying a Configuration Group.

Deployment status

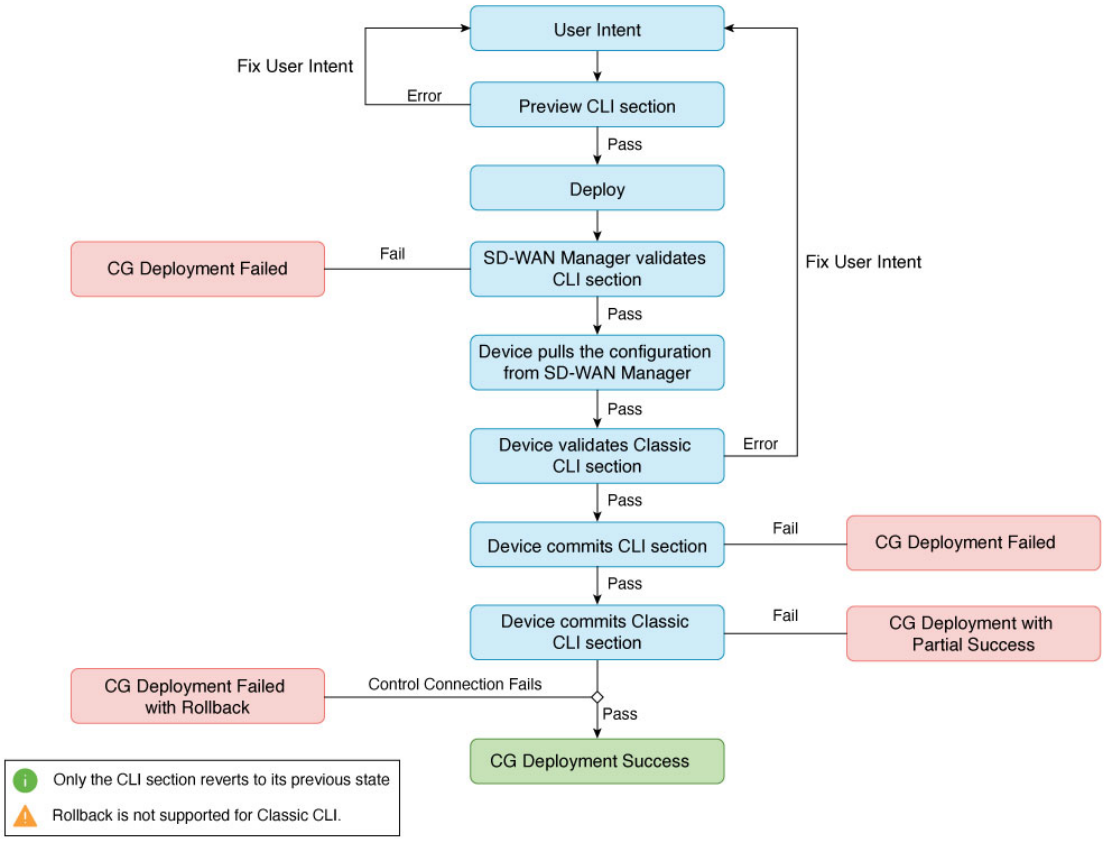
Once the deployment is complete, click **View deployment status** to view the status of the device provisioning. The Device Group pane provides the following information:

Table 3: Deployment status

Parameters	Description
Status	Indicates the deployment status.
Chassis Number	Specifies the Chassis number of the devices.
Hostname	Specifies the name of the host(s).
Message	Describes the status.
Start Time	Date and time at which you started the deployment.
System IP	Displays the system IP of the devices.
Action	Displays an **ellipsis (…)**, which, when clicked, opens a menu providing you with detailed information about the logs.

Use the Device Group pane to review the deployment status and click on **Action** > **Ellipsis (…)** to view the detailed logs on the deployment status.

This workflow illustrates the various deployment statuses.



This table provided outlines the different deployment statuses and the recommended user actions for each scenario.

Status	Description	User Action
Successful	The deployment was successful, and the device is fully configured.	-

Partial success	The associated YANG configuration was committed, but Classic CLI failed at the device end.
	Following is an example output of Partial Success.
	
	`2-Apr-2025 15:43:40 UTC] Deploying device with Config Group sd_routing`
	`[2-Apr-2025 15:43:41 UTC] Generating configuration`
	`[2-Apr-2025 15:43:41 UTC) Checking and creating device in Manager`
	`[2-Apr-2025 15:43:47 UTC] Device is online`
	`[2-Apr-2025 15:43:47 UTC] Updating device configuration in Manager`
	`[2-Apr-2025 15:43:47 UTC] Sending configuration to device`
	`[2-Apr-2025 15:43:52 UTC] Successfully notified device to pull configuration`
	`[2-Apr-2025 15:43:52 UTC] Device has pulled the configuration`
	`[2-Apr-2025 15:44:07 UTC] Device: Error:lOS command parser failed, FailedCommand:abcd, CommandErrorPosition:2, ParserModeContext:line aux O, ParserOutput:`
	`[2-Apr-2025 15:44:07 UTC] Config Group deployment completed with partial success.`
	`IOS add-on CLI config failed on the device`
		Select **Action** > **ellipsis** (…) to view detailed log information about the issue. Then go back to the configuration group page to correct the error and then deploy the device again.

Status	Description	User Action

Failure	The associated YANG configuration failed. The entire transaction was aborted, and no configuration was committed.
	Following is an example output of Failure.
	`[2-Apr-2025 15:33:40 UTC) Deploying device with Config Group sd_routing`
	`[2-Apr-2025 15:33:41 UTC] Generating configuration`
	`[2-Apr-2025 15:33:41 UTC] Checking and creating device in Manager`
	`[2-Apr-2025 15:33:47 UTC] Device is online`
	`[2-Apr-2025 15:33:47 UTC] Updating device configuration in Manager`
	`[2-Apr-2025 15:33:47 UTC] Sending configuration to device`
	`[2-Apr-2025 15:33:52 UTC] Successfully notified device to pull configuration`
	`[2-Apr-2025 15:33:53 UTC] Device has pulled the configuration`
	`[2-Apr-2025 15:33:58 UTC] Device: Validation failure, YANG CLIs found, content:`
	`fogin on-success log subscriber templating`
	`[2-Apr-2025 15:33:58 UTC] Failed to deploy Config Group`
		Select **Action** > **ellipsis** (…) to view detailed log information about the issue. Then go back to the configuration group page to correct the error and if there is a Valid IOS XE CLI without an associated YANG model then move the configuration to the Classic CLI pane. Then deploy the device again.

Status	Description	User Action

Rollback	The Control Connection failed causing a rollback to its previous working state. Only the CLI section reverts to its previous state, rollback for Classic CLI is not supported. To retain the previous device configurations, you need to correct these manually using SD-WAN Manager.
	Note, the system will wait for 5 minutes to re-establish the control connection; if the connection is not restored within this time, a rollback will occur.
	Following is an example output of Rollback.
	`12-Apr-2025 16:05:12 UTCJ Device has pulled the configuration`
	`[2-Apr-2025 16:10:44 UTC] Device: Control connections affected by config`
	`Current Date and time is 2025-04-02 16:10:27.446127`
	`Personality is SD-Routing vdaemon`
	`Checking Mandatory System Configs`
	`system-ip organization-name sp-organization-name root-ca-chain-status certificate-status certificate-validity number-active-wan-interfaces token`
	`dns-name/Validator Checking CDB`
	`name configured org-name configured sys-ip configured`
	`Checking WAN interfaces`
	`wan intf GigabitEthernet1`
	`PASS`
	`PASS`
	`PASS`
	`PASS`
	`PASS PASS`
	`PASS`
	`PASS`
	`PASS`
	`FAIL`
	`WAN interface GigabitEthernet1 is down due to which control connection could not be established! Mandatory configs missing`
	`[2-Apr-2025 16:10:44 UTC] Failed to attach configuration`
		Select **Action** > **ellipsis** (…) to view detailed log information about the issue. Then go back to the configuration group page to correct the error and then deploy the device again.
		For any unknown issues, get in touch with Cisco Technical Assistance (TAC) team.

Disassociate a device from Configuration Group

When moving a device to a different Configuration Group, you must first disassociate it from its current group. Follow these steps to disassociate a device from the Configuration Group.

Procedure

Step 1 From **Cisco Catalyst SD-WAN** Manager, choose **Configuration** > **Configuration Groups.**

Step 2 Select the preferred **SD-Routing configuration group** from the list.

Step 3 Click +**Add** adjacent to Associated field.

Step 4 Uncheck the devices to disassociate the devices from the Configuration group.

Step 5 Click **Save**.

Create a SD-Routing Configuration Group using the Workflow Library

The **Create SD-Routing Config** workflow available in the **Workflow Library** is a simplified workflow that guides you in creating a configuration group for SD-Routing devices. This is an alternative way to quickly create a configuration group.

Procedure

Step 1 From Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library** > **Create SD-Routing Config**.

Step 2 Enter a name and optionally a description and click to create a SD-Routing configuration group.

Step 3 Select the configuration group and add any additional profiles that you need. For more information refer to Create Configuration Groups using Profile Configuration Group, on page 13

What to do next

Associate and deploy the Configuration Group to an SD-Routing device, on page 15

Deploy SD-Routing devices using the Deploy Configuration Group Workflow

Before you begin

You should have created an SD-Routing Configuration Group and associated one or more devices with the configuration group.

Procedure

Step 1 From Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Deploy Configuration Group** workflow.

Step 3 Follow the instructions provided in the workflow.

Release a console

When you push configurations to a device using a Configuration Group, the device console locks, blocking any other actions through the terminal. To make the console available for pushing configurations directly through the terminal, you release it from the SD-WAN Manager. Follow these steps to release a console from a Configuration Group.

Procedure

Step 1 From **Cisco Catalyst SD-WAN Manager**, choose **Configuration** > **Devices** > **WAN Edges.**

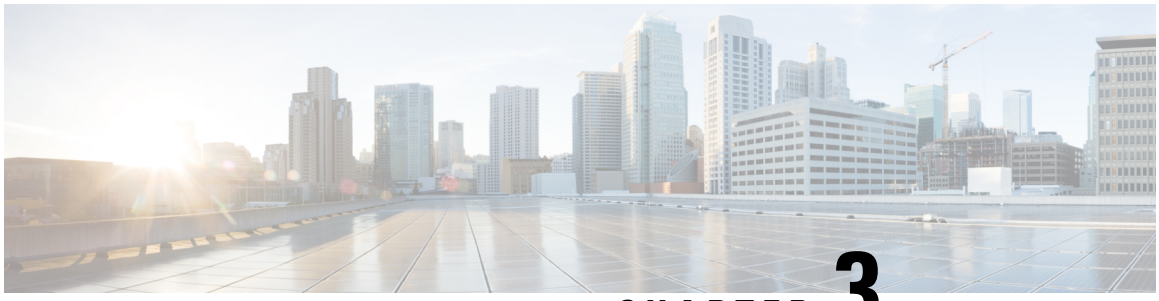
Step 2 Click **…** adjacent to the configuration group name.

Step 3 Select **Config Unlock.**

Step 4 Click **Yes** in the Config Unlock dialogue box to release the console.

PART III

Building Blocks for Profile-based Configuration Groups



CHAPTER 3

System Profile

AAA

The authentication, authorization, and accounting (AAA) feature helps authenticate users logging in to the Cisco SD-Routing device, 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
Add AAA User	
Name	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. 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.

Field	Description
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	
SSH RSA Key	Choose **ssh-rsa**.

Radius

Field	Description
Add Radius Server	
IP Address (v4 or v6)	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
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 SD-Routing 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	
IP Address (v4 or v6)	Enter the IP address of the TACACS+ server host.
Authentication 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 [second]	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 SD-Routing device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.

Accounting

Field	Description
Add Accounting Rule	
Rule Id	Enter the accounting rule ID.
Method	Specifies the accounting method list. Choose one of the following: • **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.
Start Stop	Enable this option to if you want the system to send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.

Field	Description
Groups	Choose a previously configured TACACS group. The parameters that this accounting rule defines are used by the TACACS servers that are associated with this group.

Authorization

Field	Description
Console	Enable this option to perform authorization for console access commands.
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.
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.
Group(s)	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.

802.1x

Field	Description
Authentication Param	Enable authentication parameters.
Accounting Param	Enable accounting parameters

Authentication and Authorization Order

Field	Description
Server Auth Order	Select **local**.

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
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.
Message of the Day	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.

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.
Cisco Discovery Protocol (CDP)	Enable or disable Cisco Discovery Protocol (CDP).
Link Layer Discovery Protocol (LLDP)	Enable or disable Link Layer Discovery Protocol (LLDP).
HTTP Client Source Interface	Enter the address of the source interface in all HTTPS client connections.

NAT

Field	Description
NAT 64 UDP Timeout	Specify the NAT64 translation timeout for UDP. Range: 1 to 536870 (seconds) Default: 300 seconds (5 minutes)
NAT 64 TCP Timeout	Specify the NAT64 translation timeout for TCP. Range: 1 to 536870 (seconds) Default: 3600 seconds (1 hour)
NAT TCP Timeout	Specify when NAT translations over TCP sessions time out Range: 1 through 8947 minutes Default: 3600 seconds (1 hour)
NAT 64 UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 300 seconds (5 minutes)

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.

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.

Field	Description
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	
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.
VRF	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.
Severity	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	
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.
VRF	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.

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 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.
VRF to reach NTP Server*	Enter the VRF name used to reach the NTP server, can be up to 32 alphanumeric characters

Field	Description
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 SD-Routing 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.

Advanced

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`.

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 SD-Routing devices.

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

SNMP

Table 4: Advanced

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 SD-Routing 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

Table 5: Basic

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 SD-Routing device 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.

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.

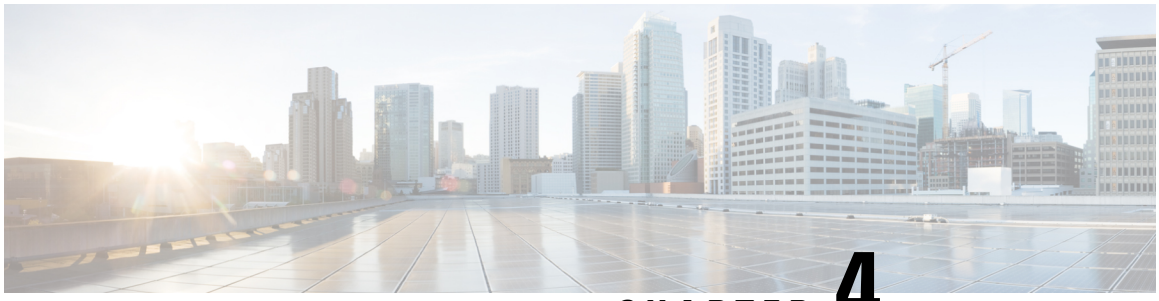
For more information about the Cisco Catalyst 8500-12X4QC platform's port options in each of its bays, see the C8500-12X4QC product overview in the *Cisco Catalyst 8500 Series Edge Platforms Data Sheet*.

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.
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.



CHAPTER 4

Transport and Management Profile

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.

Transport VRF

The Transport VRF feature helps you configure the VRF for WAN.

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
VRF	Enter the identifier of the VRF.
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 VRF.
Secondary DNS Address (IPv4)	Enter the IP address of a secondary IPv4 DNS server in this VRF.
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IP address of the primary IPv6 DNS server in this VRF.
Secondary DNS Address (IPv6)	Enter the IP address of a secondary IPv6 DNS server in this VRF.

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 VRF.
Subnet Mask*	Enter the subnet mask.

Field	Description

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 VRF.

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.

ACL IPv4

The following table describe the options for configuring the ACL IPv4 feature.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.

Field	Description
Standard	Standard ACLs control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL.
Extended	Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL.
Add ACL Sequence	Sequential collection of permit and deny conditions that apply to an IP packet
Import ACL Sequence	Import an ACL sequence into the device
Drop or Accept	Action to perform if match exists or not.
Edit ACL Sequence	
ACL Sequence Name	Enter a name for the ACL Sequence.
Source Address	Source address of IP packets
Source Address Host	A single source address host
Action Type	The default value is accept
Accept Actions	Select log from the drop-down list to log messages about packets that are permitted or denied by a standard IP access list.

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.

Management VRF

The following table describes the options for configuring the Management VRF 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.

DNS

Field	Description
Add DNS	
Primary DNS Address (IPv4)	Enter the IPv4 address of the primary DNS server in this VPN.

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	
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 VRF.
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 VRF.

Field	Description
Next Hop/Null 0	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.

Object Tracker

Use the Tracker feature to track the status of the tracker endpoints

The following table describes the options for configuring the Object Tracker feature.

Basic Settings

Parameter Name	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Description	Enter a description for the Object Tracker
Object Tracker ID	Name of the object tracker
Interface Name	Enter the global or device-specific tracker interface name. For example, Gigabitethernet1 or Gigabitethernet2
Interface Track Type	Duration to wait for the probe to return a response before declaring that the transport interface is down. Range: 100 through 1000 milliseconds. Default: 300 milliseconds . The options are: • Line-protocol • Ip-routing • Ipv6-routing
Route IP	Route IP prefix of the network
Route IP Mask	Subnet mask of the network

Parameter Name	Description
VRF Name	VRF name to be used as the basis to track route reachability
Delay Up (Seconds)	Sets delay of from 0 to 180 seconds before communication of up status of the tracked object or list of objects
Delay Down (Seconds)	Sets delay of from 0 to 180 seconds before communication of down status of the tracked object or list of objects

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.
Delay Up (Seconds)	Sets delay of from 0 to 180 seconds before communication of up status of the tracked object or list of objects
Delay Down (Seconds)	Sets delay of from 0 to 180 seconds before communication of down status of the tracked object or list of objects

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 • Interface • OSPF Tag
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • AS Path • Community • Local Preference • Metric • Metric Type • Next Hop • Origin • OSPF Tag • Weight

VRF

DNS

The following table describes the options for configuring the Management VRF feature.

Field	Description
VRF Name	Enter a name for the VRF.
RD	Specify a route distinguisher for the VRF or use the system default. A route distinguisher helps distinguish the distinct virtual private network routes of customers who connect to the provide
DNS	
IP Address	Enter the IP address of the primary DNS server in this VRF This IP address is used for resolving the Cisco SD-WAN Validator hostname

Host Mapping

Field	Description
Add New Host Mapping	
Hostname	Enter the hostname of the DNS server. The limit is 128 characters.
List of IP	Enter 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, to configure the VRF.
Subnet Mask	Enter the subnet mask for the prefix or the IP address. You can also choose a subnet mask from the drop-down list.

Field	Description
Gateway	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** , the following fields are displayed : • **Address**: Specify the next-hop IPv4 address. • **Administrative distance**: Specify the administrative distance for the route. • **Object Tracker/Object Tracker Group**: Object tracking is a mechanism for tracking an object to take any client action on another object as configured by the client. You can identify each tracked object by a unique name that is specified by the track parameter. Select an object from the drop-down list. • **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. • **Administrative distance:** Specify the administrative distance for the route. • **dhcp** • **Administrative distance**: Enter the administrative distance for the route. • **Interface**: Click **Add** and specify the following details: • **Interface Name**: Specify a valid interface or choose a value from the drop-down list. • **Add Next Hop**: • **Address**: Specify the next-hop IPv4 address. • **Administrative distance**: Specify the administrative distance for the route.
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 VRF.

Field	Description

Gateway	Choose one of the following options to configure the Next Hop to reach the static route:
	• **Next Hop**: Select this option and click **Add**,the following fields are displayed :
	  • **Address**: Specify the next-hop IPv4 address.
	  • **Administrative distance**: Specify the administrative distance for the 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.
	  • **Administrative distance:** Specify the administrative distance for the route.
	• **Interface**: Click **Add** and specify the following details:
	  • **Interface Name**:Specify a valid interface or choose a value from the drop-down list.
	  • **Next Hop**:
	  • **Address**: Specify the next-hop IPv4 address.
	  • **Administrative distance**: Specify the administrative distance for the route.

NAT

NAT	
NAT Enable	Use the toggle button to enable NAT
Add NAT Interfaces	Add interfaces that are facing the Interne the internal servers
Static NAT	Add a static NAT mapping
Static NAT Subnet	Define the subnet for the NAT mapping
NAT Port Forward	Define NAT port forwarding rules
Dynamic NAT	Define Dynamic NAT rules.

Route Leak

Route leak from Global VRF

Route Protocol	Choose a protocol from the available options to leak routes from global VRF to the service VRF that you are configuring.
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in VRF)	
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 VRF	
Route Protocol	Choose a protocol from the available options to leak routes from the service VRF that you are configuring to the global VRF.
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in global VRF)	
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 VRF(s)	
Source VRF	Enter a value of the source VRF.
Route Protocol	Choose a protocol from the available options to leak routes from the source service VRF to the service VRF that you are configuring.
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in Service VRF)	
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.

Ethernet Interface

This feature helps you configure Ethernet Interface in the VRF.

The following table describes the options for configuring the Ethernet Interface feature.

Field	Description
Type	Choose a VRF from the drop-down list
Associated VRF	Choose a VRF

Basic Configuration

Field	Description
Shutdown	Enable or disable the interface.
Control Connection	Select on to enable control connections on the tunnel.
Bind Interface	Enter the name of a physical interface to bind to a loopback 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 VRF 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
IPv4 Settings	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

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**.

BFD

Field	Description
Enable BFD	Enable this option to detect link failures

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.

ACL

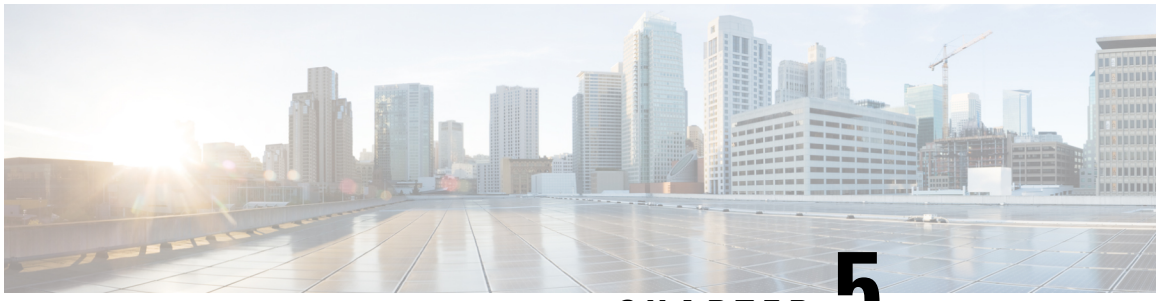
Field	Description
ACL IPv4 Ingress	Enter the name of an IPv4 access list to packets being received on the interface
ACL IPv4 Egress	Enter the name of an IPv4 access list to packets being transmitted on the interface
ACL IPv6 Ingress	Enter the name of an IPv6 access list to packets being received on the interface
ACL IPv6 Egress	Enter the name of an IPv6 access list to packets being transmitted on the interface

Advanced

Field	Description
Duplex	Specify whether the interface runs in full-duplex or half-duplex mode. Default: full

Field	Description
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 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

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.



CHAPTER 5

Service Profile

ACL IPv4

The following table describe the options for configuring the ACL IPv4 feature.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Standard	Standard ACLs control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL.
Extended	Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL.
Add ACL Sequence	Sequential collection of permit and deny conditions that apply to an IP packet
Import ACL Sequence	Import an ACL sequence into the device
Drop or Accept	Action to perform if match exists or not.
Edit ACL Sequence	
ACL Sequence Name	Enter a name for the ACL Sequence.
Source Address	Source address of IP packets
Source Address Host	A single source address host

Field	Description
Action Type	The default value is accept
Accept Actions	Select log from the drop-down list to log messages about packets that are permitted or denied by a standard IP access list.

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.

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	
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.

Object Tracker

Use the Tracker feature to track the status of the tracker endpoints

The following table describes the options for configuring the Object Tracker feature.

Basic Settings

Parameter Name	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Description	Enter a description for the Object Tracker
Object Tracker ID	Name of the object tracker

Parameter Name	Description
Interface Name	Enter the global or device-specific tracker interface name. For example, Gigabitethernet1 or Gigabitethernet2
Interface Track Type	Duration to wait for the probe to return a response before declaring that the transport interface is down. Range: 100 through 1000 milliseconds. Default: 300 milliseconds . The options are: • Line-protocol • Ip-routing • Ipv6-routing
Route IP	Route IP prefix of the network
Route IP Mask	Subnet mask of the network
VRF Name	VRF name to be used as the basis to track route reachability
Delay Up (Seconds)	Sets delay of from 0 to 180 seconds before communication of up status of the tracked object or list of objects
Delay Down (Seconds)	Sets delay of from 0 to 180 seconds before communication of down status of the tracked object or list of objects

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.

Parameter Name	Description
Delay Up (Seconds)	Sets delay of from 0 to 180 seconds before communication of up status of the tracked object or list of objects
Delay Down (Seconds)	Sets delay of from 0 to 180 seconds before communication of down status of the tracked object or list of objects

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 • Interface • 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 • Origin • OSPF Tag • Weight

VRF

DNS

The following table describes the options for configuring the Management VRF feature.

Field	Description
VRF Name	Enter a name for the VRF.
RD	Specify a route distinguisher for the VRF or use the system default. A route distinguisher helps distinguish the distinct virtual private network routes of customers who connect to the provide
DNS	
IP Address	Enter the IP address of the primary DNS server in this VRF This IP address is used for resolving the Cisco SD-WAN Validator hostname

Host Mapping

Field	Description
Add New Host Mapping	
Hostname	Enter the hostname of the DNS server. The limit is 128 characters.
List of IP	Enter 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, to configure the VRF.
Subnet Mask	Enter the subnet mask for the prefix or the IP address. You can also choose a subnet mask from the drop-down list.

Gateway	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** , the following fields are displayed :
	  • **Address**: Specify the next-hop IPv4 address.
	  • **Administrative distance**: Specify the administrative distance for the route.
	  • **Object Tracker/Object Tracker Group**:
	  Object tracking is a mechanism for tracking an object to take any client action on another object as configured by the client. You can identify each tracked object by a unique name that is specified by the track parameter.
	  Select an object from the drop-down list.
	• **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.
	  • **Administrative distance:** Specify the administrative distance for the route.
	• **dhcp**
	  • **Administrative distance**: Enter the administrative distance for the route.
	• **Interface**: Click **Add** and specify the following details:
	  • **Interface Name**: Specify a valid interface or choose a value from the drop-down list.
	  • **Add Next Hop**:
	  • **Address**: Specify the next-hop IPv4 address.
	  • **Administrative distance**: Specify the administrative distance for the route.

Field	Description
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 VRF.

Gateway	Choose one of the following options to configure the Next Hop to reach the static route:
	• **Next Hop**: Select this option and click **Add**,the following fields are displayed :
	  • **Address**: Specify the next-hop IPv4 address.
	  • **Administrative distance**: Specify the administrative distance for the 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.
	  • **Administrative distance:** Specify the administrative distance for the route.
	• **Interface**: Click **Add** and specify the following details:
	  • **Interface Name**:Specify a valid interface or choose a value from the drop-down list.
	  • **Next Hop**:
	  • **Address**: Specify the next-hop IPv4 address.
	  • **Administrative distance**: Specify the administrative distance for the route.

NAT

NAT	
NAT Enable	Use the toggle button to enable NAT
Add NAT Interfaces	Add interfaces that are facing the Internet an the internal servers
Static NAT	Add a static NAT mapping
Static NAT Subnet	Define the subnet for the NAT mapping
NAT Port Forward	Define NAT port forwarding rules
Dynamic NAT	Define Dynamic NAT rules.

Route Leak

Route leak from Global VRF	
Route Protocol	Choose a protocol from the available options to leak routes from global VRF to the service VRF that you are configuring.
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in VRF)	
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 VRF	
Route Protocol	Choose a protocol from the available options to leak routes from the service VRF that you are configuring to the global VRF.
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in global VRF)	
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 VRF(s)	
Source VRF	Enter a value of the source VRF.
Route Protocol	Choose a protocol from the available options to leak routes from the source service VRF to the service VRF that you are configuring.
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in Service VRF)	
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.

IPv4/IPv6 Static Route Service

IPv4/IPv6 Static Route

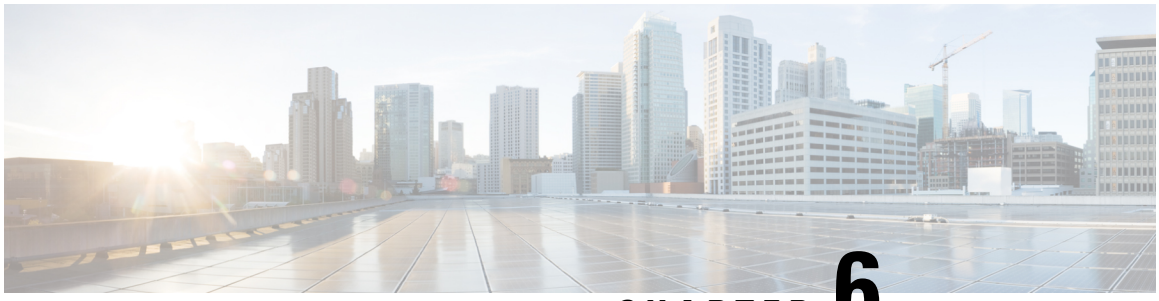
Field	Description
Add IPv4 Static Route	

Field	Description
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.

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.



CHAPTER 6

Policy Object Profile

The Policy Object feature profile enables you to attach policy configurations to a device.

The following table describes the options for configuring the policy profile.

Table 6:

Field	Description
Choose existing	Choose an existing profile from the Profiles table.
Create new	When you choose this option, the following fields appear: • Name: Enter a name for the profile. • Description: Enter a description of the profile. The description can contain any characters and spaces.