Cisco Catalyst SD-WAN Control Components and Device Management Guide, Releases 26.x and Later

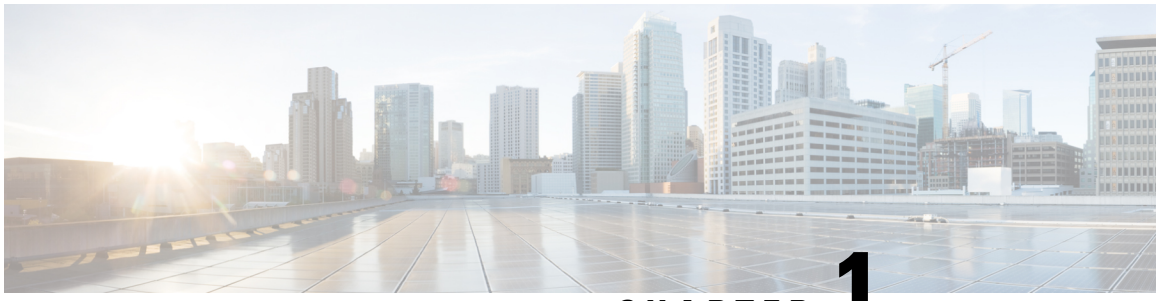
First Published: 2026-04-20

Last Modified: 2026-04-20

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 4 **Basic Settings for Cisco SD-WAN Manager** 67



CHAPTER 1

System Logging

Feature history for system logging

This shows the history of the system logging feature.

Table 1: Feature history

Feature Name	Release Information	Description
Ability to Send Syslog Messages over TLS	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature allows you to transport syslog messages to external configured hosts by establishing a Transport Layer Security (TLS) connection. Using the TLS protocol enables the content of syslog messages to remain confidential, secure, and untampered or unaltered during each hop.

Feature Name	Release Information	Description
Remote Logging Over TCP and TLS in Cisco Catalyst SD-WAN Control Components	Cisco Catalyst SD-WAN Control Components Release 20.13.1	The feature allows remote logging of syslog messages through TCP and TLS. This feature is now available on Cisco Catalyst SD-WAN Control Components (Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Manager) in addition to Cisco IOS XE Catalyst SD-WAN devices.

System logging

System logging is a process that

- records a text log of system events using a mechanism similar to the UNIX syslog command,
- allows devices to send log messages with configurable priority levels to UNIX-style syslog services, and
- supports secure transmission over the Transport Layer Security (TLS) protocol.

Priority levels

Log messages have levels that indicate their priority. These are the same as for standard UNIX commands. You can configure the priority of syslog messages.

Security

Cisco IOS XE Catalyst SD-WAN devices send syslog messages to syslog servers on configured external hosts using TCP and UDP. When the devices send the syslog messages, the messages might transit several hops to reach the output destination. The intermediate networks during the hops might not be trustworthy, be in a different domain, or have a different security level. Therefore, Cisco IOS XE Catalyst SD-WAN devices support sending secure syslog messages over TLS as described in RFC 5425. To secure the syslog message content from potential tampering, the TLS protocol is used for certificate exchange, mutual authentication, and ciphers negotiation.

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

Benefits of using TLS

- Message confidentiality

  Confidentiality of message content where each TLS session begins with a handshake between the Cisco IOS XE Catalyst SD-WAN device and the syslog server. The Cisco IOS XE Catalyst SD-WAN device and syslog server agree on the specific security key and the encryption algorithms to be used for that session. The TLS session opposes any disclosure of the contents of the syslog message.

- Message integrity

  Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.

- Authentication

Mutual authentication between the Cisco IOS XE Catalyst SD-WAN device and syslog server ensures that the syslog server accepts log messages only from authorized clients through certificate exchange.

System log files

System log (syslog) messages that are at or above the default or configured priority value are recorded in a number of files in the `/var/log` directory on the local device of the syslog server. The log files contain these items.

Table 2: Log files

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

Unused log files

Cisco Catalyst SD-WAN does not use these standard Linux files, which are available in the `/var/log` directory:

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

System log formats

Syslog messages begin with a percent sign (%) and come in these formats:

- Sequence and timestamp

  sequence-number:timestamp: %*facility-severity-MENEMONIC*:*description (hostname-n)*

- Format based on RFC5424

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

  The optional fields such as *hostname*, *appname*, *procId*, *msgId*, and *structured-data* are specified with a -.

Table 3: Field descriptions

Field	Description
facility	Sets the logging facility to a value other than 20, which UNIX systems expect.
severity	Importance or severity of the message, 0 to 7. A lower number indicates a greater severity of the system condition.
msg or description	Text string that describes the condition of the syslog server. This portion of the syslog message sometimes includes IP addresses, interface names, port numbers, or usernames. In syslog message formats based on RFC5424, the description is: *%facility-severity-MENEMONIC:description*

Examples

This system logging message includes a priority value, sequence number, and timestamp:

*<45>10: polaris-user1: *Jun 21 10:76:84.100: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down*

This RFC5424-format message has a priority value, version of syslog protocol specification, and timestamp:

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

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

System log message levels

Each system log (syslog) message has a severity, or priority, level. A lower severity number means a higher severity. The default priority value is 6 (informational). By default, all syslog messages are recorded.

Table 4: System log message severity levels

Severity level	Name	Description
0	Emergency	System is unusable.
1	Alert	System in a state that requires immediate action.
2	Critical	Serious condition.
3	Error	Error condition that does not fully impair system usability.
4	Warning	Minor error condition.
5	Notice	Normal operation, but with a significant condition requiring notice.
6	Informational	Routine condition (default).
7	Debug	Debug messages.

Sending system log messages to a server, using TLS

Transport layer security (TLS) is a networking protocol that provides secure communication through a network.

Benefits of using TLS for sending syslog messages

The benefits of using TLS for sending syslog messages are:

- Confidentiality

  Confidentiality of message content where each TLS session begins with a handshake between the Cisco IOS XE Catalyst SD-WAN device and the syslog server. The Cisco IOS XE Catalyst SD-WAN device and syslog server agree on the specific security key and the encryption algorithms to be used for that session. The TLS session opposes any disclosure of the contents of the syslog message.

- Integrity-checking

  Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.

- Mutual authentication

  Mutual authentication between the Cisco IOS XE Catalyst SD-WAN device and syslog server ensures that the syslog server accepts log messages only from authorized clients through certificate exchange.

Authentication type

- **Server**

  With server authentication, edge devices verify the identity of the syslog server. If the syslog server and the certificate are legitimate entities, the device establishes a TLS connection with the server.

  As part of server authentication, the syslog server shares its public certificate with the devices.

  See the prerequisite in the "Before you begin" section of this procedure.

  With this option, all information about TLS profiles, except the trustpoint information, is saved.

- **Mutual**

  With mutual authentication, edge devices and the syslog server authenticate each other at the same time.

  Devices require root or identity certificates for mutual authentication of the TLS session.

  With this option, a trustpoint, such as SYSLOG-SIGNING-CA certificate, is saved on the device. This enables SD-WAN Manager to install the certificate from the edge device.

Restrictions for system logging

Disabling system logging to disk

Disabling system logging to disk (`no system logging disk enable`) does not disable `vsyslog`.

Storage restrictions

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

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

Repeating or identical messages

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

Maximum length

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

The maximum length of a log message for Cisco SD-WAN Manager audit logs is 1024 bytes. The longer messages are truncated into smaller fragments and each of these fragments are indicated by an identifier. The identifiers are

- fragment 1/2
- fragment 2/2

and so on.

For example, a long audit log message when truncated into smaller fragments appears as:

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

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

AAA authentication and Netconf CLI access

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

Configure system logging

Use one of these methods to configure system logging:

- Configuration group
- Feature template
- CLI commands

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Configure system logging using a configuration group

System logging is the process of keeping a text log of system events.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Follow these steps to configure system logging for a device, using a configuration group:

Procedure

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

Step 2 Create and configure a Logging feature in a System profile.

a) Enter the disk information.

Table 5: 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

b) Enter the TLS Profile information.

Table 6: 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**.

Field	Description
Cipher Suite List	Choose groups of cipher suites (encryption algorithm) based on the TLS version. 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)

c) Enter the server information.

Table 7: 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: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
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 these: • **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, these fields appear: **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: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
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 these: • **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.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure system logging using a template

System log (syslog) messages are a text log of system events.

On Cisco IOS XE Catalyst SD-WAN devices, you can save system log messages locally or to a remote server.

Before you begin

Follow these steps to configure system logging for a device, using a feature template.

Procedure

Step 1 Create a System Logging feature template.

See Create a System Logging feature template, on page 12.

Step 2 Choose whether to save system log messages locally or to a syslog server. If saving messages to a server, choose whether to use the Transport Layer Security (TLS) protocol.

Configure a device to save system log messages to a server, using TLS, on page 13

a) If you choose to save syslog messages locally, do this:

Configure a device to save system log messages locally, on page 12

b) If you choose to save syslog messages to a syslog server, without using TLS, do this:

c) If you choose to save syslog messages to a syslog server, using TLS, with authentication by the server, do this:

d) If you choose to save syslog messages to a syslog server, using TLS, with mutual authentication by the edge device and the server, do this:

Create a System Logging feature template

System log (syslog) messages are a text log of system events.

Procedure

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

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

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

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

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

The Cisco logging template form displays fields for naming the template and defining the logging parameters. Click a tab or the plus sign (+) to view additional fields.

When you first open a feature template, SD-WAN Manager sets the scope to default, for parameters that have a default value. The default setting or value appears next to each parameter. To change the default or enter a value, select a different option from the scope drop-down list to the left of the parameter field.

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

The name may contain up to 128 alphanumeric characters.

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

The description may contain up to 2048 alphanumeric characters.

Configure a device to save system log messages locally

System log (syslog) messages are a text log of system events.

You can save system log messages locally or to an external server. This procedure configures a device to save system messages locally.

Before you begin

Follow these steps to configure a device to save system log messages to a local drive.

Procedure

Step 1 In a System Logging template, in the **Disk** section, configure these parameters:

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

Step 2 To save the feature template, click **Save**.

Configure a device to save system log messages to a server, using TLS

System log (syslog) messages are a text log of system events.

You can send system log messages to an external server over a Transport Layer Security (TLS) connection.

For the TLS connection, there are two methods of authentication, configured by the **Authentication Type** parameter.

- Server authentication: Authentication by the server.
- Mutual authentication: Authentication by both the device and the server.

See Sending system log messages to a server, using TLS, on page 5.

Before you begin

For the server authentication option, edge devices must have a root certificate authority (CA) preinstalled, which you configure using cryptographic module CLIs. See Install root CA on Cisco IOS XE Catalyst SD-WAN device.

Follow these steps to configure the TLS parameters for saving syslog messages to an external server over a TLS connection.

Procedure

Step 1 In a System Logging template, in the **TLS** section, click **New Profile**.

Step 2 Configure these parameters:

Field	Description
Profile Name	Enter the TLS profile name.
TLS Version	Choose TLS versions v1.1 or v1.2.
Authentication Type	Choose the authentication type: • **Server** With server authentication, edge devices verify the identity of the syslog server. If the syslog server and the certificate are legitimate entities, the device establishes a TLS connection with the server. As part of server authentication, the syslog server shares its public certificate with the devices. See the prerequisite in the "Before you begin" section of this procedure. With this option, all information about TLS profiles, except the trustpoint information, is saved. • **Mutual** With mutual authentication, edge devices and the syslog server authenticate each other at the same time. Devices require root or identity certificates for mutual authentication of the TLS session. With this option, a trustpoint, such as SYSLOG-SIGNING-CA certificate, is saved on the device. This enables SD-WAN Manager to install the certificate from the edge device.
Ciphersuites	Choose cipher suites (encryption algorithms) based on the TLS version.

Step 3 To save the feature template, click **Save**.

Configure a device to save system log messages to a server

System log (syslog) messages are a text log of system events.

Before you begin

Follow these steps to configure a device to save system log messages to a server.

Procedure

Step 1 Click **Server**.

Step 2 Click **Add New Server**, and configure these parameters:

Field	Description
Hostname/IP Address	Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages. To add another syslog server, click **+**. To delete a syslog server, click  .
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. VPN ID Range: 0 to 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 of syslog servers is ignored. If you configure multiple syslog servers, the source interface must be same for all of them.
Priority	Choose a severity of the syslog message to be saved. The severity indicates the seriousness of the event that generated the syslog message. See System log message levels, on page 5.
TLS	For Cisco IOS XE Catalyst SD-WAN devices, click **On** to enable syslog over TLS.
Custom Profile	For Cisco IOS XE Catalyst SD-WAN devices, click **On** to enable choosing a TLS profile, or click **Off** to disable choosing a TLS profile.
TLS Profile	For Cisco IOS XE Catalyst SD-WAN devices, choose a TLS profile that you have created for server or mutual authentication in IPv4 or IPv6 server configuration.

Step 3 To save the feature template, click **Save**.

Configure system logging using CLI commands

You can save event notification system log (syslog) messages locally or to a remote server. These event notification logs are converted to system log files and exported to the syslog server. You can then retrieve system log information from the syslog server.

- Configure system logging, saved locally, using CLI commands, on page 16
- Configure system logging, saved remotely, using CLI commands, on page 17

Configure system logging, saved locally, using CLI commands

System logging is the process of keeping a text log of system events.

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

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

Before you begin

Follow these steps to configure system logging for a device, saving syslog messages locally, using CLI commands:

Procedure

Step 1 Log syslog messages to a drive.

logging disk

Step 2 Enable logging to a drive.

enable

Step 3 Specify the size of syslog files in megabytes (MB).

By default, the syslog files are 10 MB. You can configure the size of syslog files to be 1 to 20 MB.

file size *size*

Step 4 Rotate syslog files on an hourly basis based on the size of the file.

By default, 10 syslog files are created. You can configure the rotate command to be a number from 1 through 10.

file rotate *number*

Example

```
Device(config-system)# logging disk
Device(config-logging-disk)# enable
Device(config-logging-disk)# file size 3
Device(config-logging-disk)# file rotate 3
```

Configure system logging, saved remotely, using CLI commands

System logging is the process of keeping a text log of system events.

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

Before you begin

Follow these steps to configure system logging for a device, saving syslog messages a remote server, using CLI commands:

Procedure

Step 1 Log syslog messages to a remote host or syslog server.

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

logging server

Step 2 If using a VPN, specify the VPN ID of the syslog server.

vpn *vpn-id*

Step 3 (Optional) Specify the source interface to reach the syslog server.

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

source interface *interface*

Step 4 Specify the severity of the syslog message to be saved.

The default priority value is "informational" and by default, all syslog messages are recorded. See the logging server command reference documentation for priority values.

priority *alert*

Example

```
Device(config-system)# logging server 192.168.0.1
Device(config-server-192.168.0.1)# source interface eth0
Device(config-server-192.168.0.1)# priority notice
```

Install a root certificate on a device for mutual authentication

To configure Cisco IOS XE Catalyst SD-WAN devices with Transport Layer Security (TLS) syslog protocol, the devices must have root or identity certificates for mutual authentication of TLS session. You can either use a third-party Certificate Authority (CA) to get public key infrastructure (PKI) services, or Microsoft Active

Directory Certificate Services (AD CS). AD CS allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your requirement.

Before you begin

Follow these steps to install a root certificate on a device for mutual authentication.

Procedure

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

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

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

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

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

Step 6 If you want to generate a certificate signing request (CSR), check the **Set CSR Properties** check box.

Step 7 Click **Close**.

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

Install a root certificate authority on a syslog server for server authentication

This procedure sets up the syslog-ng server tool on a server using Linux. The tool supports TLS.

The details of setting up a server, and installing the syslog-ng tool are beyond the scope of this documentation. The basic information provided here is for reference, and is subject to change.

Before you begin

Follow these steps to install a root certificate authority on a syslog server for server authentication.

Procedure

Step 1 On the Linux server, install the syslog-ng package.

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

Step 2 In the directory of the syslog-ng tool, create directories to store root certificates.

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

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

Step 3 Copy the contents of the `cacert.pem` file when installing root certificate on a device.

Install a root certificate authority on a device for server authentication, using CLI commands

Before you begin

Generate an encoded CA certificate on the syslog server. This is required in one of the steps. For instructions, see Install a root certificate authority on a syslog server for server authentication, on page 18.

Follow these steps to install a root certificate authority on a device, for server authentication.

Procedure

Step 1 To configure a public key infrastructure (PKI) trustpoint for a certificate authority, use these commands on a device, for authorizing and revocation of certificates in PKI.

a) Enable privileged EXEC mode.

```
enable
```

b) Enter configuration mode.

```
config-transaction
```

c) Declare the trustpoint and a given name and enter CA-trustpoint configuration mode. Specify the enrollment parameters and fingerprint for the CA. Obtain the fingerprint from the fingerprint.txt.

```
crypto pki trustpoint name
```

Example:

```
Device(config)# crypto pki authenticate PROXY-SIGNING-CA
        enrollment url bootflash:
        revocation-check none
        rsakeypair PROXY-SIGNING-CA 2048
        subject-name cn=proxy-signing-cert
        fqdn none
        fingerprint 54F371C8EE2BFB06E2C2D0944245C288FBB07163
```

d) If the authentication in the previous step fails, contact the PKI team for assistance.

For information about syslog configuration, see Cisco SD-WAN IOS XE TLS Syslog Configuration on syslog-ng Server.

e) Configure the level to which a certificate chain is processed on all certificates.

```
chain-validation [{stop | continue}[parent-trustpoint]]
```

Example:

```
Device(ca-trustpoint)# chain-validation stop
```

f) Optionally, check the revocation status of a certificate.

```
revocation-check method
```

Example:

```
Device(ca-trustpoint)# revocation-check none
```

g) Return to global configuration mode.

exit

Example:

```
Device(ca-trustpoint)# exit
```

Step 2 Authenticate the root CA.

This is necessary before installing the server's root certificate.

crypto pki authenticate

Example:

```
Device(config)# crypto pki authenticate root
```

Step 3 Copy the block of text containing the base 64 encoded CA certificate from the syslog server, and paste it at the prompt.

The prerequisites section refers to the instructions for generating the encoded CA certificate on the syslog server.

Example:

An example encoded CA certificate:

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswCQYD
VQQGEwJJTjESMBAGA1UECAwJS2FybmF0YWthMRIwEAYDVQQHDAlCYW5nYWxvcmUx
...
+3RcM0VqjScIOZhp97dqfBlHEdqUE/QfKlBt12KU+0sj8yJJC+cuKlHQj5JGmGLI
Y6r7bMcn99Y6Rw==
-----END CERTIFICATE-----
```

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

The root CA certificate from the syslog server is installed on a device, enabling server authentication.

```
crypto pki trustpoint PROXY-SIGNING-CA
    enrollment url bootflash:
    revocation-check none
    rsakeypair PROXY-SIGNING-CA 2048
    subject-name cn=proxy-signing-cert
    fqdn none
    fingerprint 54F3...7163  >> The fingerprint configured was obtained from the
fingerprint.txt file.
commit
```

```
crypto pki authenticate PROXY-SIGNING-CA
Reading file from bootflash:PROXY-SIGNING-CA.ca
Certificate has the following attributes:
Fingerprint MD5: 7A97B30B ... 66488DCF
Fingerprint SHA1: 21E0F09B ... D39A268A
Trustpoint Fingerprint: 21E0F09B ... D39A268A
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
```

View system logs

System logging records a text log of system events.

Before you begin

In SD-WAN Manager, in **Administration** > **Settings**, enable **Data Stream**.

View device-specific system log (syslog) files in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

In Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.

Step 2 Select a device.

Step 3 Click **Troubleshooting**.

Step 4 In the **Logs** section, click **Debug Log**.

Step 5 From **Log Files**, select the name of a log file to view the log information.

Viewing system log information using CLI commands

You can use these CLI commands to view system log (log) information.

Viewing system log settings

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

```
Host(config-server-192.168.0.1)# show logging
System logging
    server 192.168.0.1
    source interface eth0
    exit
!
!
```

Viewing system log files

To view the contents of the system log file, use the **show log** command.

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

Create a certificate signing request and install feature certificates

This procedure validates and authenticates devices and the syslog server.

Procedure

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

Step 2 From **Certificates**, select a device.

a) Generate a feature certificate signing request (CSR).

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

b) View and download the feature CSR.

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Step 4 Import the certificate into Cisco IOS XE Catalyst SD-WAN devices.

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

SD-WAN Manager uses the signed certificate and installs it on devices.

After the feature certificate installation is successful, options are available in SD-WAN Manager to revoke or view a feature certificate.

Verifying the trustpoint configuration on a device

Display the contents of a syslog file to verify the trustpoint configuration.

Verifying server authentication

Example:

```
Cisco XE SD-WAN# show crypto pki trustpoints status
crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  subject-name CN=CSR-cbc47d9d-..._vManage Root CA
```

Verifying mutual authentication

Example:

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

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  rsakeypair SYSLOG-SIGNING-CA 2048
  subject-name CN=CSR-cbc47d9d-..._vManage Root CA
```

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

Example:

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

Trustpoint SYSLOG-SIGNING-CA:

 Issuing CA certificate not configured.

State:

Keys generated ..... No

 Issuing CA authenticated ..... No

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

Remote logging over TCP and TLS

Remote logging refers to saving system log information on a remote server.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, remote logging of syslog messages can include TCP and TLS transport methods, in addition to UDP. This applies to SD-WAN Control Component.

The default transport type for remote logging is UDP. But you can optionally select TCP or TLS as the transport method for remote logging.

Benefits of remote logging over TCP and TLS

These are benefits of remote logging over TCP and TLS.

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

Configure remote logging over TCP using CLI commands

Before you begin

Follow these steps to configure remote logging over TCP using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a remote server with transport type TCP.

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

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

Configure remote logging over TLS using CLI commands

Before you begin

Follow these steps to configure remote logging over TLS using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use these steps to install, list, and uninstall the certificate authority (CA) certificate from the syslog server.

a) Install a certificate.

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

b) List all installed certificates.

```
show logging cacert
```

c) Uninstall a certificate if necesseary.

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

Step 3 Create a TLS profile.

```
system
 logging
 tls-profile profile-name
```

```
  tls-version TLSv1.2
  ciphersuite ciphersuite1 ciphersuite2
```

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

Step 4 Attach a TLS profile to a remote logging server.

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

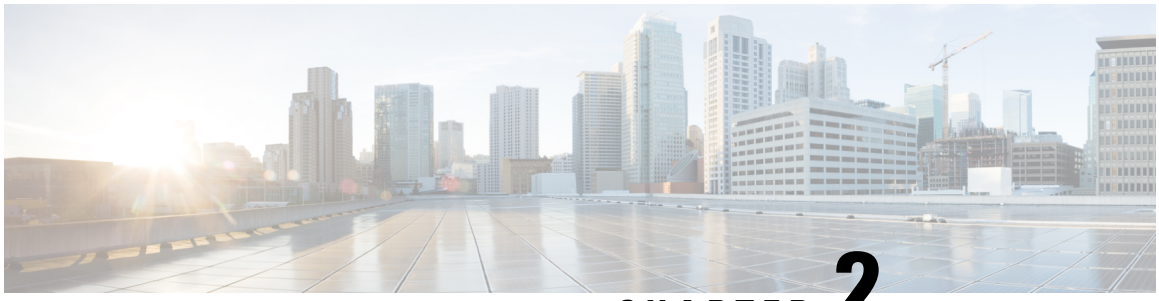
```
system
logging
  disk
   enable
  !
  tls-profile profile1
   version     TLSv1.2
   ciphersuite ECDHE-ECDSA-AES128-SHA256 AES256-GCM-SHA384 PSK-AES256-GCM-SHA384
PSK-AES128-GCM-SHA256 AES256-SHA256
  exit
  server 10.0.1.55
   source interface 10.1.1.12
   transport   tls
   tls-profile profile1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

Verifying remote logging over TCP and TLS

View the installed certificates to verify that remote logging is possible over TCP and TLS.

The **show logging cacert** command shows installed certificates.

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



CHAPTER 2

Device Tagging

Device tagging

Table 8: Feature History

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

Device tagging

Device tags are labels that

- help you group, describe, and locate devices more effectively, and
- enable adding devices to configuration groups using tag-based rules.

  For information about creating rules, refer to the information about adding devices to a configuration group using rules, in Using Configuration Groups in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

You can assign multiple tags to a single device.

Single-tenant and multitenant support

You can use device tagging in both the single-tenant and multitenant deployments.

Restrictions for device tagging

Maximum number of tags

In Cisco vManage Release 20.11.1 and earlier:

- Use a maximum of 25 tags per Cisco SD-WAN Manager instance.
- Use a maximum of 25 tags per device.

Permitted characters

In Cisco vManage Release 20.11.1 and earlier:

- Maximum characters in a tag: 25
- Permitted characters: Only alphanumeric characters, hyphens (–), and underscores (_).
- Cannot contain space or any other special characters.
- Tag name is case-sensitive.

Maximum tag rules per configuration group

Cisco vManage Release 20.11.1 and earlier: You can add only one tag rule to a configuration group.

Add device tags

Device tags are labels that help you group, describe, locate, or perform actions on devices efficiently.

You can add multiple tags to a device and you can delete unwanted tags from a device. You can also add device tags to devices using the Quick Connect workflow. Refer to the Quick Connect Workflow section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Follow these steps to add a tag to a device.

Procedure

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

Step 2 Click **WAN edge list** and choose a device.

Step 3 Click **Add tags**.

Step 4 Choose a tag from the list of existing tags or click **Create new tag**.

In Cisco vManage Release 20.11.1 and earlier, this was called **Add new tag**.

Step 5 Click **Apply**.

The specified tag is added to the device.

Delete device tags

You can delete only those tags that are not added to a device or are not a part of a tag rule.

Follow these steps to delete device tags from a device.

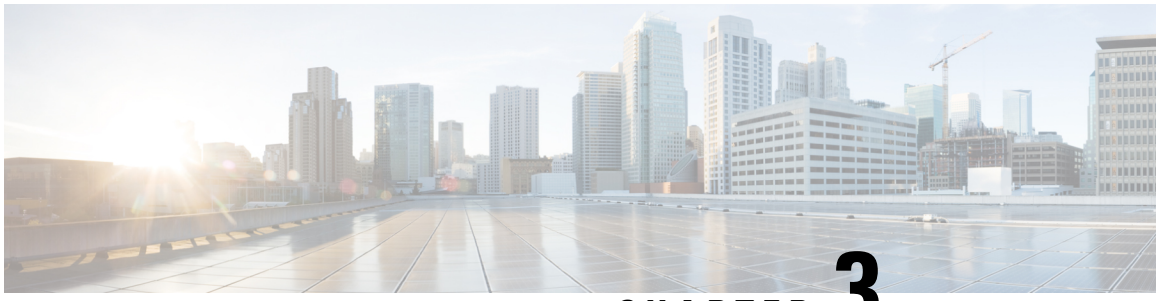
Procedure

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

Step 2 Choose the tags that you want to delete.

Step 3 Click **Delete tags**.

Step 4 Click **Yes** to confirm.



CHAPTER 3

Configure Devices

Feature history for configure devices

Table 9: Feature history

Feature name	Release information	Description
Support for Draft Mode in Device Template	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to save the device template configuration changes in Cisco SD-WAN Manager, and then apply these configuration changes to multiple Cisco IOS XE Catalyst SD-WAN devices later. The ability to save configuration changes simplifies generating larger device template configurations and applying them to devices.
Retrieve Last Edited Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to review the last edited configuration when a configuration push to the device fails. A copy of the last edited configuration is saved and can be retrieved to allow edits to the configuration before the next push.

Feature name	Release information	Description
Default Device Templates	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	A default device template provides basic information that you can use to bring up devices in a deployment quickly. This feature is supported on the Cisco Cloud Services Router 1000V Series, Cisco C1111-8PLTELA Integrated Services Routers, and Cisco 4331 Integrated Services Routers.
Remove Certificate SUDI requirement	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to use a subject SUDI serial number instead of a certificate serial number to add a device to a Cisco Catalyst SD-WAN overlay network.
Create a UCS-E Template	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template.

Configure devices in Cisco SD-WAN

You can use Cisco SD-WAN Manager to create and store configurations for all devices; the Cisco SD-WAN Manager systems themselves, Cisco SD-WAN Controllers, Cisco SD-WAN Validator, and routers. When the devices start up, they contact SD-WAN Manager, which then downloads the device configuration to them. (A device starting up first contacts the SD-WAN Validator, which validates the device and sends it the IP address of SD-WAN Manager.)

The general procedure for creating configurations for all devices is the same. This section provides a high-level description of the configuration procedure and describes the prerequisite steps you must complete before creating configurations and configuring devices in the overlay network.

Types of templates

There are two types of templates:

- Feature templates
- Device templates

Feature templates

Feature templates are the building blocks of complete configuration for a device. For each feature that you can enable on a device, Cisco SD-WAN Manager provides a template form that you fill out. The form allows you to set the values for all configurable parameters for that feature.

Because device configurations vary for different device types and the different types of routers, feature templates are specific to the type of device.

Some features are mandatory for device operation, so creating templates for these features is required. Also for the same feature, you can create multiple templates for the same device type.

Special Characters in Feature Template

In releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you enter **<** or **>** special characters in a SD-WAN Manager feature template definition or description, SD-WAN Manager generates a 500 exception error while attempting to preview a SD-WAN Manager feature template.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you enter **<** or **>** special characters in a SD-WAN Manager feature template definition or description, the special characters are converted to their HTML equivalents, **<** and **>**.

This applies to all feature templates. You no longer receive a 500 exception error when previewing a SD-WAN Manager feature template.

Device templates

Device templates contain the complete operational configuration for a device and are created by consolidating feature templates.

- Each device template is specific to a device type.
- If multiple devices of the same type share the same configuration, you can use the same template for all of them. Differences between devices are handled using configuration variables.
- If devices of the same type have different configurations, you create separate templates.

CLI-based device templates

You can create a device template by entering a CLI-style configuration directly in SD-WAN Manager by

- Uploading a text file with the configuration
- Copying and pasting configuration text
- Typing the configuration directly into SD-WAN Manager

From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, you can review your last edited configuration when your latest configuration is not being pushed to the device. For more information, see Edit a device template when a push fails.

From Cisco vManage Release 20.5.1, device variable page shows text area instead of text input field to configure CLI device template for the ease of configuration.

Template variables

Within a feature template, some configuration commands and options are identical across all device types, while others are variable, changing from device to device. Examples of variable parameters include:

- Device system IP address
- Geographic latitude and longitude

- Timezone
- Overlay network site identifier

When you attach a device template to a device, you are prompted to enter the actual values for these variables. You can provide these values in two ways:

1. Manually: Type the values for each variable for each device.
2. Bulk upload: Upload an excel file in CSV format containing the values for all devices.

Use variable values in configuration templates

In an overlay network, multiple devices of the same type might have similar configurations. This often happens with routers in different stores or branch locations that provide identical services but have unique hostnames, IP addresses, GPS locations, and site-specific properties such as BGP neighbors. It also applies to redundant controllers like Cisco SD-WAN Controllers and Cisco SD-WAN Manager systems, where each controller has its own hostname and IP address.

To simplify configuration, create a single configuration template with both static and variable values. Static values remain common across all devices, while variable values apply to individual devices. You provide the variable values when attaching a device to the configuration template.

You can configure variable values in a feature template in two ways:

- Set the parameter scope to Device Specific:

  For a parameter, select **Device Specific** to mark it as a variable. Each variable has a unique key. When you select **Device Specific**, the Enter Key box appears with a default key. You can use the default key, or you can change it by typing a new string and then moving the cursor out of the Enter Key box.

- Mark a group of parameters as optional:

  For some features in some feature configuration templates, you can mark the entire feature as optional. To mark the feature in this way, click Mark as Optional Row in a section of a feature configuration template. The variable parameters are then dimmed, and you cannot configure values for them in the feature configuration template.

Enter device-specific values for the variables when attaching the device to the configuration using one of these methods:

- From a file: When you are attaching a template to a device, you load a file to SD-WAN Manager. This is an Excel file in CSV format that lists all the variables and defines the variable's value for each device.
- Manually: When you attach a device template to a device, the SD-WAN Manager prompts you for the values for each of device-specific parameters, and you type in the value for each parameter.

Cisco Catalyst SD-WAN supports up to 500 variables in a single template push operation.

Use a file for variable parameters

To load device-specific variable values, create a template variables file in Excel CSV format. This file lists all the variables in your device configurations and defines their values. Create the file offline, and then import it into the SD-WAN Manager server when you attach a device configuration to one or more devices in the overlay network.

We recommend creating a template variables CSV file if your overlay network includes more than a few Cisco IOS XE Catalyst SD-WAN devices.

CSV file format

File description

The CSV file is an Excel spreadsheet with one column for each variable required to configure a device. The header row lists the variable names (one variable per column), and each subsequent row represents a device and defines its variable values.

Spreadsheet options

You can create one spreadsheet for all devices in the overlay network: Cisco IOS XE Catalyst SD-WAN devices, SD-WAN Manager systems, SD-WAN Controller, and SD-WAN Validators, or create a separate spreadsheet for each device type. The system identifies the device type by its serial number.

In the spreadsheet, specify values only for the required variables for each device type and device. If a variable does not need a value, leave the corresponding cell blank.

Make the first three columns in the spreadsheet these items, and arrange them in the order shown:

Column	Column heading	Description
1	csv-deviceId	Serial number of the device (used to uniquely identify the device). For Cisco IOS XE Catalyst SD-WAN devices, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.
2	csv-deviceIP	System IP address of the device (used to populate the **system ip address** command).
3	csv-host-name	Hostname of the device (used to populate the **system hostname** command).

Use unique variable keys from the Enter Key box of a feature configuration template as the headings for the remaining columns. You can arrange these columns in any order.

Generate a skeleton CSV file

To have SD-WAN Manager generate a skeleton CSV file:

You create a template variables CSV file manually using the format described in the previous section, or let SD-WAN Manager generate a skeleton CSV file containing all required columns and headings. The generated CSV file includes one row for each Cisco device type and column headings for all variables required by the feature templates in the device configuration. The column headings use the key strings that identify device-specific parameters. Then fill each row with values for the corresponding variables.

Procedure

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

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

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

Step 3 Create the required feature templates for one Cisco IOS XE Catalyst SD-WAN device router, one Cisco Catalyst SD-WAN Controller, one Cisco SD-WAN Manager system, and one Cisco Catalyst SD-WAN Validator.inf

In each feature template:

- For fields that have default values, verify that you want to use that value for all devices. If you do not want to use the default, change the scope to **Global** or **Device-specific**.
- For fields that apply to all devices, select the **Global** icon next to the field and set the desired global values.
- For fields that are device specific, select the **Device-specific** icon next to the field and leave the field blank.

Step 4 For each Cisco device type, create a device template.

Step 5 From the SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 6 Click **Device Templates**, and select the desired device template from the template list table.

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

Step 7 Click **…**, and click **Export CSV**.

Step 8 Repeat Steps 7 and 8 for each device template.

Edit the exported CSV file to include at least the device serial number, system IP address, and hostname for each device in the overlay network. Then enter values for the desired device-specific variables. Ensure that variable names do not include forward slashes (/), backslashes (), or parentheses (( )).

If needed, combine multiple CSV files into a single file.

Import a CSV file

To import the CSV file containing device-specific variable values when you attach a device template to the Viptela device.

Procedure

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

Step 2 Click **Device Templates**.

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

Step 3 For the desired template, click **...**, and select **Attach Devices**.

Step 4 In the **Attach Devices** dialog box, select the desired devices in **Available Devices** and click the arrow to move them to **Selected Devices**.

Step 5 Click **Attach**.

Step 6 Click the Up arrow. The Upload CSV File box displays.

Step 7 Choose the CSV file to upload, and click **Upload**.

During the attachment process, click Import file to load the Excel file. If SD-WAN Manager detects duplicate system IP addresses for devices in the overlay network, it shows a warning message or pop-up. Correct the system IP addresses to remove any duplicates before continuing to attach device templates to Viptela devices.

Manually enter values for device-specific variables and for optional rows

To manually enter values for device-specific variables or for variables in optional rows when you attach the template to a device:

When you attach a device template that includes device-specific parameters, SD-WAN Manager prompts you to enter the parameter values. When you attach a device template that includes device-specific parameters, SD-WAN Manager prompts you to enter the parameter values. However, this method does not scale well for larger networks.

When many devices share the same configuration except for a few parameters, you can specify those parameters as optional rows in the feature configuration template. When you select **Optional Row**, the feature template automatically marks those parameters as device-specific and dims them so you cannot modify them in the template. You do not have to individually mark the parameters as device specific. When you attach the device template to a device, SD-WAN Manager prompts you to enter the values for those parameters.

Using optional rows to enter device-specific values is useful when a group of many Cisco IOS XE Catalyst SD-WAN devices provide identical services at their branch or site, but individual routers have their own hostname, IP address, GPS location, and other site or store properties, such as BGP neighbors.

Optional rows are available for some parameters in some feature configuration templates. To treat a parameter or set of parameters as an optional row, click the **Mark as Optional Row** box. For these types of parameters, the feature configuration template has a table listing all the configured parameters. The Optional column indicates which are optional rows

Procedure

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

Step 2 Click **Device Templates**, and select the desired device template.

Step 3 Click **…**, and click **Attach Devices**.

The **Attach Devices** dialog box opens.

Step 4 Choose one or more devices from **Available Devices** and move them to **Selected Devices**.

Step 5 Click **Attach**.

Step 6 In the **Chassis Number** list, select the desired device.

Step 7 Click **…**, and click **Edit Device Template**. The **Update Device Template** dialog box opens.

Step 8 Enter values for the optional parameters. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.

Step 9 Click **Update**.

Step 10 Click **Next**.

If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.

You need to shut down the OMP on the device, before changing the system-ip on the device.

Step 11 In the left pane, select the device. The right pane displays the device configuration and the **Config Preview** tab in the upper right corner is selected.

Step 12 Click **Config Diff** to preview the differences between this configuration and the configuration currently running on the device, if applicable. To edit the variable values entered in the previous screen, click **Back**.

Step 13 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed. Click the **right angle bracket** to the left of the row to display details of the push operation.

Configure and manage device templates

Create a device template

A device template defines a device's complete operational configuration.

It consists of multiple feature templates, each defining the configuration for a specific Cisco Catalyst SD-WAN software feature.

- Some feature templates are mandatory (marked with an asterisk *), while others are optional.
- Each mandatory feature template and some optional ones include a factory-default template.

You can either use the factory-default template `Factory_Default_feature-name_Template` or create a custom feature template.

- Create a device template from feature templates
- Create a device template after building custom feature templates

Create a device template from feature templates

Use these steps to create a device template from feature templates.

Procedure

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

Step 2 Click **Device Templates**.

Step 3 Click the **Create Template** drop-down and select **From Feature Template**.

Step 4 From the **Device Model** drop-down, select the device type for which you wish to create the template.

a. All feature templates for that device type appear.

b. Required templates are marked with *, and optional ones are not.

c. Factory-default templates are preselected.

Step 5 In the **Template Name** field, enter a name using letters, digits (0–9), hyphens (-), or underscores (_).

No spaces or special characters allowed.

Step 6 In the **Description** field, enter a description.

Spaces and any characters allowed

Step 7 To view a factory-default configuration, select a feature template and click **View Template**.

Click **Cancel** to return to the previous screen.

Step 8 To create a **custom template** for a feature:

a) Select the desired factory-default feature template and click **Create Template**.
b) In the **Template Name** and **Description** fields, provide details (same naming rules apply).
c) Configure each parameter as needed.
d) Click tabs or **(+)** to expand additional fields.

Step 9 When you first open a feature template, parameters with default values show a check mark under the **Default** scope. You can change the scope for each parameter:

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

To make an entire parameter group device-specific, select **Mark as Optional Row**. These parameters are grayed out in the feature template and filled later when attaching the device.

Step 10 Click **Save** after configuring each feature template.

Step 11 Repeat steps 6 through 9 for each additional software feature you want to include.

Step 12 Click **Create**.

- The new device template appears in the Device Template table.
- The Feature Templates column shows how many feature templates it includes.

- The Type column displays Feature, indicating it was created from feature templates.

Create a device template after building custom feature templates

To create device templates after building custom feature templates.

Procedure

Step 1 Click **Feature** > **Add Template**.

Step 2 From **Select Devices**, choose the device type.

You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.

Step 3 Select the **feature template**.

The template form is displayed.

This form contains fields for naming the template and fields for defining the required parameters. If the feature has optional parameters, then the template form shows a plus sign (+) after the required parameters.

Step 4 In the **Template Name** field, enter a name for the device template.

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

Step 5 In the **Description** field, enter a description for the device template.

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

Step 6 For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down list of each parameter's value box.

Click the plus sign (+) from the required parameters to set the values of optional parameters.

Step 7 Click **Save** .

Step 8 Repeat Steps 2 to 7 for each additional feature template you wish to create.

Step 9 Click **Device**.

Step 10 Click the **Create Template** drop-down list and select **From Feature Template**.

Step 11 From the **Device Model** drop-down list, select the type of device for which you wish to create the device template.

SD-WAN Manager displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (*). The remaining templates are optional.

Step 12 Repeat step 4 and 5.

Step 13 To view the factory-default configuration for a feature template, select the desired feature template and click **View Template**.

Step 14 Factory default configuration.

a) Click **Cancel** to return to the **Configuration Template** screen.

The new device template is displayed in the **Device Template** table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

b) To modify a factory-default configuration, choose a different feature template you created from the drop-down.

Repeat this step for each factory-default feature template you wish to modify.

Step 15 Click **Create**

The new configuration template is displayed in the Device Template table.

The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Create a device CLI template

To create a device template by entering a CLI text-style configuration directly on the SD-WAN Manager.

Procedure

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

Step 2 Click **Device Templates**.

Step 3 Click the **Create Template** drop-down list and select **CLI Template**.

Step 4 From the **Device** Type drop-down list, select the type of device for which you wish to create the template.

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

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

Step 6 In the **Description** field, enter a description for the device template.

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

Step 7 In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

Step 8 To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.

Step 9 Click **Add**. The new device template is displayed in the Device Template table.

The **Feature Templates** column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Default device templates

A default device template includes the basic information needed to bring up devices in a deployment. It allows you to quickly provision devices with the minimum details required for them to operate in your network.

You cannot directly edit or update a default device template, but you can copy it and then edit the copied version.

Procedure

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

Step 2 Click **Device Templates**.

Step 3 From the **Template Type** drop-down list, select **Default**.

A list of default device templates displays.

Step 4 Perform any of these actions:

- To attach a default device template to devices, click **...**, and select **Attach Devices**.

  In the **Attach Devices** dialog box, select the devices that you want attach, and then click **Attach**.

- To view the configuration settings for a default device template, click **...**, and choose **View**.

- To copy a default device template, click **...**, and choose **View**.

  In the **Template Copy** dialog box, enter a unique name and a description for the copy that you are creating, and then click **Copy**.

  The copied version becomes a feature template that you can edit.

- To create an Excel file in CSV format that contains device-specific settings from a device template, click **...**, and choose **Export CSV**. Use the dialog box that displays to open or save the CSV file.

  You can use this CSV file as a reference for device-specific settings when you create other device templates.

Change variable values for a device

When you create a configuration from device configuration templates that contain variables, SD-WAN Manager automatically populates those variables with actual values when you attach the templates to devices. To enable this, create an Excel file listing the variable values for each device and save it in CSV format. You can also manually enter the variable values.

After you push the configuration to a device, you can change the value assigned to any variable.

Procedure

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

Step 2 Click **Device Templates**, and choose the desired device template.

Step 3 Click **...**, and click **Change Device Values**.

The screen displays a table of all the devices that are attached to that device template.

Step 4 For the desired device, click **...**, and click **Edit Device Template**.

Step 5 In the **Update Device Template** dialog box, enter values for the items in the variable list.

Step 6 Click **Update**.

Step 7 Click **Next**.

Step 8 Click **Configure Devices** to push the configuration to the device.

The Status column displays if the configuration was successfully pushed or not. Click the right angle bracket to display the details of the push operation.

Change the device rollback timer

By default, when you attach a configuration template to a Cisco IOS XE Catalyst SD-WAN device, the router rolls back to the previous configuration if it fails to start successfully within 5 minutes. For configurations created from the CLI, you can change the device's rollback timer.

Procedure

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

Step 2 Click **Device Templates**, and choose a device template.

Step 3 Click **…**, and click **Change Device Values**.

The right pane displays the device's configuration, and the **Config Preview** tab is selected.

Step 4 In the left pane, click the name of a device.

Step 5 Click **Configure Device Rollback Timer**. The **Configure Device Rollback Time** pop up page is displayed.

Step 6 From the **Devices** drop-down list, select a device.

Step 7 Enable or disable the rollback timer.

- To enable the rollback timer, in the **Set Rollback slider** drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.
- To disable the rollback timer, click **Enable Rollback slider**. When you disable the timer, the **Password** field dialog box appears.

  Enter the password that you used to log in to SD-WAN Manager.
- In the **Device Rollback Time** slider, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.
- To exclude a device from the rollback timer setting, click **Add Exception** and select the devices to exclude.

Step 8 The table of the **Configure Device Rollback Time** dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the **Trash** icon of the device name.

Step 9 Click **Save**.

Step 10 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed. Click **(+)** to display details of the push operation.

Edit a device template when a push fails

If the configuration push to a device fails, you can review the last edited configuration to identify any issues that caused the failure.

See Retrieve last edited configuration.

Retrieve last edited configuration

Before you begin

To review your last edited configuration, a device template must be attached to a device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.

Step 2 Click **Device Templates** and choose a device template.

Step 3 Click **...**, and choose **Edit**.

The **CLI Configuration** box displays the current running configuration on the device.

Step 4 Click **Load Last Attempted Config** to view the last edited configuration.

Step 5 Click **Config Diff** to view the differences in the current configuration versus the last edited configuration. The **Config Diff** option is available when you modify the configuration or when you click **Load Last Attempted Config**.

Step 6 Click **Config Preview**.

Load Last Attempted Config and the **Config Diff** option is available only when the configuration is not being pushed to the device.

Step 7 Click **Update**.

Step 8 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed. Click > to view the details of the push operation.

Determine why a device rejects a template

To determine why the device rejected the template.

When you attach a template to a device using the screen, the device might reject the template. One reason that this may occur is because the device template contains incorrect variable values. When a device rejects a template, it reverts to the previous configuration.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.
Step 2 Click **Device Templates** and select the desired template.
Step 3 Locate the device. The **Template Status** column indicates why the device rejected the template.

Preview device configuration and view configuration differences

Use these steps for a configuration that you have created using the CLI.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
Step 2 Click **Device Templates**, and choose the desired device template.
Step 3 Click **...**, and click **Change Device Values**.

The right pane displays the device's configuration, and **Config Preview** is selected.

Step 4 Click the name of a device.
Step 5 Click **Config Diff** to view the differences between the current configuration and the one running on the device.
Step 6 Click **Back** to edit the variable values you entered on the previous screen.
Step 7 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed.

Click the right angle bracket to display details of the push operation.

Export a variables-spreadsheet in CSV format for a template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.
Step 2 Click **Device Templates** and select the desired template.
Step 3 Click **…**, and click **Export CSV**.

Edit a device template

Procedure

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

Step 2 Click **Device Templates** or **Feature Templates** and select a template..

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

Step 3 Click **…**, and click **Edit**.

You cannot change the name of a device or feature template when that is attached to a device.

You can edit templates simultaneously from one or more Cisco SD-WAN Manager servers. For simultaneous template edit operations, the following rules apply:

- You cannot edit the same device or feature template simultaneously.
- When you are editing a device template, all other feature templates attached to that device template are locked and you cannot perform any edit operations on them.
- When you are editing a feature template that is attached to a device template, that device template as well as all other feature templates attached to it are locked and you cannot perform any edit operations on them.

Delete a template

Deleting a template does not remove the associated configuration from devices.

Procedure

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

Step 2 Click **Device Templates** or **Feature Templates** and select a template..

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

Step 3 Click **…**, and click **Delete**.

Step 4 To confirm the deletion of the template, click **OK**.

Copy a template

Procedure

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

Step 2 Click **Device Templates** or **Feature Templates** and select a template..

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

Step 3 Click **…**, and click **Copy**.

Step 4 Enter a new template name and description.

Step 5 Click **Copy**.

Edit a CLI device template

Procedure

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

Step 2 Click **Device Templates** and select a template..

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

Step 3 Click **…**, and click **Edit**.

Step 4 Under **Device CLI Template**, edit the template.

Step 5 Click **Update**.

View a template

Use these steps to view a template.

Procedure

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

Step 2 Click **Device Templates** or **Feature Templates**, and select a template you wish to view.

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

Step 3 Click **…**, and then click **View**.

View device templates attached to a feature template

Use these steps to view a template device templates attached to a feature template.

Procedure

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

Step 2 Click **Feature Templates**, and select a template you wish to view.

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

Step 3 Click **…**, and click **Show Attached Device Templates**.

Step 4 **Device Templates** dailog box opens, displaying the names of the device templates to which the feature template is attached.

View devices attached to a device template

Procedure

Step 1 For a device template that you created from feature templates:

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

b) Click **Device Templates**, and select a template you wish to view.

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

c) Click **Device Templates**, and select a template you wish to view.

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

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

e) From **Attach Devices**, click **Attached Devices**.

Step 2 For a device template that you created from a CLI template:

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

b) Click **Device Templates**, and select a template you wish to view.

c) Click **…**, and then click **Show Attached Devices**.

Attach templates to devices

Attach and detach a device template

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

You need to recreate the feature templates, as the templates created prior to Cisco vManage Release 20.5.1 fail when attached to the device.

Parallel operations

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

You can perform the following template operations in parallel:

- Attach device templates to devices
- Detach device templates from devices
- Change variable values for device templates that have devices attached to them

Configuration deployment behavior

If the device being configured is present and operational on the network, the configuration is sent to the device immediately and takes effect immediately.

If the device has not yet joined the network, the pushing of the configuration to the device is scheduled. When the device joins the network, SD-WAN Manager pushes the configuration immediately after it learns that the device is present in the network.

Rules for template operations

The rules below apply for template operations:

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

Attach a device template to devices

Use these steps to attach a device template to one or more devices.

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

Procedure

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

Step 2 Click **Device Templates** and select the desired template.

Step 3 Click **…**, and click **Attach Devices**.

The **Attach Devices** dialog box opens with the **Select Devices** tab.

Step 4 Select devices.

a) In the **Available Devices** column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
b) Click the arrow pointing right to move the device to the **Selected Devices** column on the right.
c) Click **Attach**.

Step 5 Enter variable values.

If the template contains variables, enter the missing values for each device:

- Manually: Enter values in the table or click **…** and **Edit Device Template**.

  When using optional rows, leave a parameter blank if not required.

- Import File: Click **Import File** to upload a CSV file listing all variables and their values.

- Click **Update**, then **Next**.

  If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.

Step 6 Preview configuration.

a) In the left pane, select a device to preview its configuration.

   The right pane displays the **Config Preview** tab.

b) To view differences with the running configuration, click the **Config Diff** tab.
c) Click **Back** to edit variables if needed.

Step 7 Click **Configure Device Rollback Timer**.

The **Configure Device Rollback Time** dialog box appears.

a) Select a device from the **Devices** drop-down list.
b) Enable timer: Drag the Set Rollback slider left (gray → green).
c) Disable timer: Click the slider; enter your Cisco SD-WAN Manager password when prompted.
d) Set interval: Drag the Device Rollback Time slider to choose a time (default 5 minutes; range 6–15 minutes).
e) Add Exception: Click **Add Exception** to exclude devices.
f) The bottom table lists devices and their rollback times. Click the Trash icon to delete an entry.
g) Click **Save**.

Step 8 Click **Configure Devices** to push the configuration to all selected devices.

The Status column shows whether the configuration was successfully pushed. Click the right angle bracket (>) to view detailed push operation results.

Configuration prerequisites

Security prerequisistes

- Before configuring any device in the network, ensure that the device is validated and authenticated so that SD-WAN Manager, Cisco SD-WAN Controllers, and SD-WAN Validators recognize it as authorized in the overlay network.
- A signed certificate must be installed on SD-WAN Manager, Cisco SD-WAN Controllers, and SD-WAN Validators to validate and authenticate them in the overlay network.
- Obtain an authorized serial number file from Cisco, which lists the serial and chassis numbers for all routers permitted in your network. Upload this serial number file to SD-WAN Manager to validate and authenticate the routers.

Variables spreadsheet

Feature templates often include variables. To ensure SD-WAN Manager populates these variables with actual values when attaching a device template to a device, create an Excel spreadsheet containing the variable values for each device, and save it in CSV format.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be the following, in this order:

- csv-deviceId—Serial number of the device (used to uniquely identify the device). For routers, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.
- csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).
- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network—Cisco Catalyst SD-WAN Controllers, SD-WAN Validators, and routers. You do not need to specify values for all variables for all devices.SD-WAN Validator

Device configuration workflow

Devices in the overlay network that are managed by SD-WAN Manager must be configured from SD-WAN Manager.

Procedure

Step 1 Create feature templates.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**, and click **Add Templates**.

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

Step 2 Create device templates.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**, and click **Create Templates**.

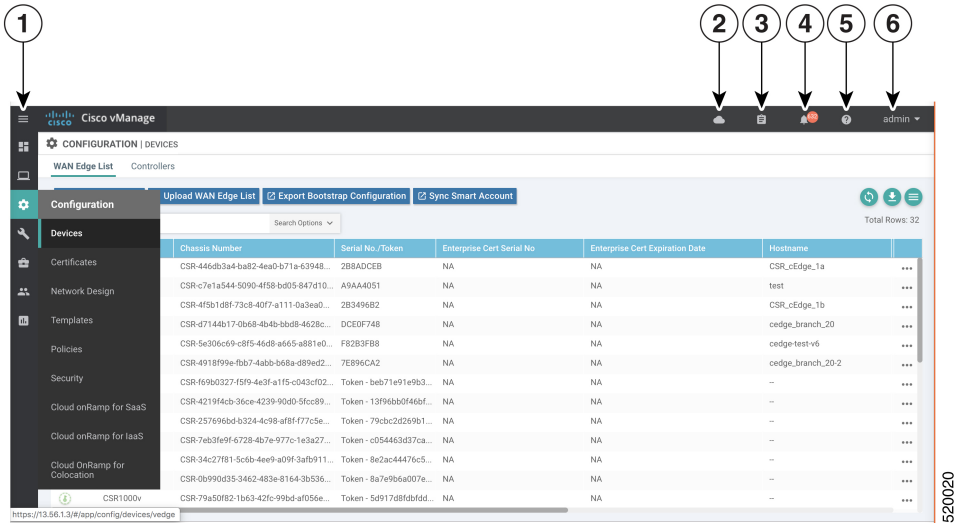
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 Attach device templates to individual devices.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**, and choose a template.
c) Click **…**, and select **Attach Devices**.

Configure and manage devices using SD-WAN Manager

Use the **Devices** screen to add and delete devices, toggle the mode of a device between CLI and SD-WAN Manager, upload the WAN edge serial number file, export bootstrap configuration and, and perform other device-related tasks.



1	Menu
2	CloudExpress
3	Tasks
4	Alarms
5	Help
6	User Profile

Change configuration modes

A device can be in either of these configuration modes:

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

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

Procedure

Step 1 Follow these steps to toggle a router from Cisco SD-WAN Manager mode to CLI mode.

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

- The **Config Lock** (Provision Device) option appears only if a template is attached to the device or if a configuration group is deployed to the device.
- Starting from Cisco IOS XE SD-WAN Release 17.11.1a, click the **...** icon adjacent to the device that you want to change fromCisco SD-WAN Manager mode to the CLI mode and click **Config Lock** (Provision Device).

Step 2 Follow these steps to toggle a controller device from Cisco SD-WAN Manager mode to CLI mode:

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
b) Click **Controllers**, and select a device.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

c) Click the **Change Mode** drop-down list.
d) Select **CLI mode** and then select the device type. The **Change Mode - CLI** window opens.
e) From the **Manager mode** pane, select the device and click the right arrow to move the device to the **CLI mode** pane.
f) Click **Update to CLI Mode**.

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

Upload WAN edge router authorized serial number file

To upload the WAN edge router authorized serial number file to SD-WAN Manager and then download it to controllers in the network

- The WAN eEdge router authorized serial number file contains, as applicable, the subject SUDI serial number, the chassis number, and the certificate serial numbers of all valid Cisco IOS XE Catalyst SD-WAN devices in the overlay network.
- You retrieve a serial number file from the Cisco Plug-and-Play (PnP) portal and upload it to SD-WAN Manager. (For more information about Cisco PnP, see Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products.)
- From SD-WAN Manager, you send the file to the controllers in the network. This file is required to allow the Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational.

Procedure

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

Step 2 Click **WAN Edge List**, and click **Upload WAN Edge List**.

The Quick Connect workflow opens, enabling you to upload the serial number file. Refer information about the Quick Connect workflow in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Step 3 (This step applies only for releases earlier than Cisco Catalyst SD-WAN Manager Release 20.14.1) Under the **Upload WAN Edge List** screen:

a) Click **Choose File** and select the WAN edge router authorized serial number file you received from Cisco PnP.

b) To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the **Validate the uploaded vEdge List and send to controllers** check box is selected. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > WAN Edge List.

a) Click **Upload**.

A list of routers in the network is displayed in the router table, with details about each router.

What to do next

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

Upload WAN edge router serial numbers from Cisco Smart Account

To upload the WAN edge router authorized serial numbers from a Cisco Smart account to SD-WAN Manager and then download it to all the controllers in the overlay network:

- To allow Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational, Cisco Catalyst SD-WAN requires chassis numbers of all valid Cisco IOS XE Catalyst SD-WAN devices in the overlay network.

  In addition, certificate serial numbers, subject SUDI serial numbers, or both numbers are required for all devices.

Procedure

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

Step 2 Click **WAN Edge List**, and click **Sync Smart Account**.

Step 3 In the **Sync Smart Account** window:s

a) Enter the **Username** and **Password** for your Smart account.

b) To automatically validate the routers and send their chassis and serial numbers to the controllers, check the **Validate the Uploaded WAN Edge List and Send to Controllers** check box. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > **WAN Edge List** .

c) Click **Sync**

A list of routers in the network is displayed in the router table, with details about each router.

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

Export device data in CSV format

In an overlay network, you might deploy multiple devices of the same type that share identical or nearly identical configurations.

- Example 1: In a network with redundant SD-WAN Controllers, you must configure each controller with identical policies.
- Example 2: In a network with Cisco IOS XE Catalyst SD-WAN devices at multiple sites, each device provides identical services at each site.

Using templates for identical configurations

As these devices have essentially identical configurations:

- You can create one set of feature templates.
- You can consolidate them into one device template.
- You can use this single device template to configure all devices.

To assign unique values per device, you can:

- Create an Excel file in CSV format.
- List all the variables.
- Define each device-specific variable value for every device.
- Load this file when you attach the device template to the devices.

How to export data in CSV format

The Export icon lets you create and download device data in a CSV file. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

SD-WAN Manager downloads all data from the device table to an Excel file in CSV format.

View a device's running configuration

Running configuration is configuration information that SD-WAN Manager obtains from the memory of a device. This information can be useful for troubleshooting.

Use these steps to view a device's running configuration:

Procedure

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

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **…**, and click **Running Configuration**.

View a device's local configuration

Local configuration refers to the configuration that the SD-WAN Manager stores for a device.This information helps troubleshoot issues or determine how to access a device when it is not reachable from SD-WAN Manager.

To view a device's local configuration created using Configuration ► Templates:

Procedure

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

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **...**, and click **Local Configuration**.

Copy router configuration

Copy the configuration from the old router to the new router.

When you are replacing one router at a site with another router, you copy the old router's configuration to the new router. Then you remove the old router from the network and add the new one.

Procedure

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

Step 2 Mark the new Cisco IOS XE Catalyst SD-WAN device as invalid.

Step 3 From the Cisco SD-WAN Manager, choose **Configuration** > **Devices**.

Step 4 Under **WAN Edge List,** select the old router.

Step 5 Click **…**, and click **Copy Configuration**.

Step 6 In the **Copy Configuration** window, select the new router.

Step 7 To confirm the copy of the configuration, click **Update**.

After you have copied the configuration to the new router, you can add the new router to the network. First, delete the old router from the network, as described below. Then add the new router to the network:

Step 8 From the Cisco SD-WAN Manager, choose **Configuration** > **Certificates**.

Mark the new router as valid.

Step 9 Click **Send to Controller**.

Delete a WAN edge router

Delete a router to remove it from your deployment. This action also removes the following items associated with the router from the WAN Edge router serial number list:

- Chassis number
- Certificate serial number
- Subject SUDI serial number

Deleting a router also permanently removes the router configuration from SD-WAN Manager.

Procedure

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

Step 2 Mark the WAN Edge router as invalid.

Step 3 From the SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 4 Click **WAN Edge List,** and select the router.

Step 5 Click **...**, and click **Delete WAN Edge**.

Step 6 To confirm deletion of the device, click **OK**.

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

Step 8 Click **Send to Controller.**

Decommission a cloud router

Decommissioning a cloud router (such as a C8000v) removes the device's serial number from SD-WAN Manager and generates a new token for the device.

- The Decommission WAN Edge feature applies only to cloud WAN edge devices and retains the cloud WAN Edge's UUID generated on the PnP Portal.
- Physical devices do not support the Decommission WAN Edge functionality.

Procedure

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

Step 2 Click **WAN Edge List**, and select a cloud router.

Step 3 Click **…**, and click **Decommission WAN Edge**.

Step 4 To confirm the decommissioning of the router, click **OK**.

Note
From Cisco Catalyst SD-WAN Manager Release 20.15.1, the process to decommision a WAN edge router has been modified. The scenarios below highlight the updates.

Table 10: Updates to deleting a WAN edge router

Scenario	Action
Decommision a compromised device	Click **Delete WAN Edge**
Device is reachable	Perform a mandatory **configuration unlock** before proceeding with the decommissioning process.
Device is unreachable	The device will be unlocked after certain time when the device is unreachable. If you no longer have the device onboarded, with no Cisco SD-WAN Manager visibility, you can hold the power button for 5–10 seconds for a config reset, or 10-20 seconds for a software reset. If you have console/terminal access, you can run the **request config reset** command. Reuse of UUID is only possible after decommissioning a device. In this case, the **Decommission** option is not available since the device is offline.

View log of template activities

The template activity log records details about creating, editing, and deleting configuration templates, as well as the status of attaching templates to devices. This information helps in troubleshooting.

Procedure

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

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **…**, and click **Template Log**.

View status of device bring up

You can view the status of operations that bring a router or controller online in the overlay network. This helps you monitor and track their progress effectively.

Procedure

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

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **…**, and click **Device Bring Up**.

Add a Cisco SD-WAN Validator

A Cisco SD-WAN Validator automatically orchestrates connectivity between Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager. If any Cisco IOS XE Catalyst SD-WAN device or SD-WAN Controller is behind a NAT, the SD-WAN Validator also serves as an initial NAT-traversal orchestrator.

Procedure

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

Step 2 Click **Controllers**.

Step 3 Click **Add Validator**.

Step 4 In the **Add Validator** window:

a) Enter **Validator Management IP Address** of the SD-WAN Validator.

b) Enter the **Username** and **Password** to access the SD-WAN Validator.

c) To allow the certificate-generation process to occur automatically, check the **Generate CSR** check box.

d) Click **Add**.

Step 5 Repeat Steps 2, 3 and 4 to add additional SD-WAN Validators.

The new SD-WAN Validator is added to the list of controllers in the Controllers screen.

Configure Cisco SD-WAN Controllers

Add an SD-WAN Controller

After the SD-WAN Validator authenticates Cisco IOS XE Catalyst SD-WAN devices, the SD-WAN Validator provides Cisco IOS XE Catalyst SD-WAN device information that they need to connect to the SD-WAN Controller. A SD-WAN Controller controls the flow of data traffic throughout the network via data and app-route policies.

Procedure

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

Step 2 Click **Controllers**.

Step 3 Click **Add Controller**.

Step 4 In the **Add Controller** window:

a) Enter the system IP address of the Cisco Catalyst SD-WAN Controller.
b) Enter the **username** and **password** to access the SD-WAN Controller.
c) Select the protocol to use for control-plane connections. The default is DTLS. The DTLS (Datagram Transport Layer Security) protocol is designed to provide security for UDP communications.
d) If you select TLS, enter the port number to use for TLS connections. The default is 23456.
e) The TLS (Transport Socket Layer) protocol that provides communications security over a network.
f) Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
g) Click **Add**.

Step 5 Repeat Steps 2, 3 and 4 to add additional SD-WAN Controllers. Cisco SD-WAN Manager can support up to 20 SD-WAN Controllers in the network.

The new SD-WAN Controller is added to the list of controllers in the Controllers screen.

Edit SD-WAN Controller details

You can edit controller details to update the controller's IP address and login credentials.

Procedure

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

Step 2 Click **Controllers**, and select the controller.

Step 3 Click **…**, and click **Edit**.

Step 4 In the **Edit** window, edit the IP address and the login credentials.

Step 5 Click **Save**.

Delete an SD-WAN Controller

Deleting a controller removes it from the overlay. Delete the controller when you replace it or no longer need it in your network.

Procedure

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

Step 2 Click **Controllers**, and select the controller.

Step 3 Click **…**, and click **Invalidate**.

Step 4 To confirm the removal of the device and all its control connections, click **OK**.

Configure reverse proxy on SD-WAN Controllers

To configure reverse proxy on an individual SD-WAN Manager and SD-WAN Controller:

Procedure

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

Step 2 Click **Controllers**, and select the controller.

Step 3 Click **…**, and click **Add Reverse Proxy**.

The **Add Reverse Proxy** dialog box is displayed.

Step 4 Configure the private IP address and port number for the device.

The private IP address is the IP address of the transport interface in VPN 0. The default port number is 12346. This is the port used to establish the connections that handle control and traffic in the overlay network.

Step 5 Configure the proxy IP address and port number for the device, to create the mapping between the private and public IP addresses and port numbers.

Step 6 If the SD-WAN Manager NMS or SD-WAN Controller has multiple cores, repeat Steps 5 and 6 for each core.

Step 7 Click **Add**.

To enable reverse proxy in the overlay network, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Proxy** > **Reverse Proxy**. Now enable **Reverse Proxy** and click **Save**.

Configure UCSE using a configuration group

Use these steps to configure UCSE using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

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

Step 2 Create and configure a UCSE feature in Other profile.

a) Configure parameter scope.

Table 11: Parameter

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.

b) Configure options for the UCSE feature.

Table 12: Settings

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.

c) Configure basic settings.

Table 13: 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.

d) Configure IMC.

Table 14: 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.

e) Configure advanced settings.

Table 15: Advanced Configuration

Field	Description
Interface Name*	Specify the name of the interface.
Layer	Specify the layer details necessary for traffic exchange between different VLANs.
UCSE Interface VPN	Specify the details of the UCS-E interface VPN.
IPv4 Address	Provide the UCS-E management port address.

What to do next

See Deploy a configuration group.

Create a UCS-E Template

For more information about the Cisco Unified Computing System (UCS) E-Series Servers, see the Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Hardware Installation Guide.

Procedure

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

Step 2 Click **Feature Templates**.

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

Step 3 Click **Add Template**.

Step 4 Select a Cisco IOS XE Catalyst SD-WAN device from the list.

Step 5 From the **Other Templates** section, click **UCSE**.

The UCSE Feature template opens. The top of the form contains fields for naming the template, and the bottom contains fields for configuring the Integrated Management Controller (IMC).

Step 6 In the **Template Name** field, enter a name for the template.

The name can be up to 128 characters and can contain only alphanumeric characters.

Step 7 In the **Description** field, enter a description of the template.

The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 8 Configure bay and slot for template

Click the Basic Configuration tab to configure the bay and the slot for the template.

Parameter name	Description
Bay	Specify the number for the SAS drive bays.
Slot	Specify the slot numbers for the mezzanine adapters

Step 9 Configure IMC.

Click the **IMC** tab to configure the IMC parameters for the template.

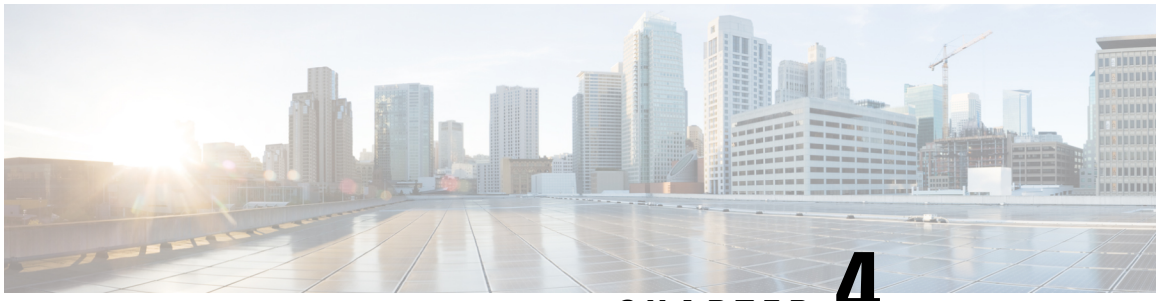
Parameter name	Description

Access port	Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN.
	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
	The type of port, GE or TE, depends on the hardware model.
	For example:
	`Router(config-ucse)# imc access-port shared-lom ?`
	`GE1 GE1`
	`TE2 TE2`
	`TE3 TE3`
	`console Console`
	`failover Failover`
	Some hardware models have GE ports whereas some have TE ports.
	Depending on the hardware module, the appropriate port (GE or TE) needs to be configured. Otherwise you will get an error.
	• You can obtain the UCS-E module hardware model type by using the following commands:
	show inventory
	show platform
	• Failover - sub-option under Shared.
	For example:
	`Router(config)#ucse subslot 1/0`
	`Router(config-ucse)#imc access-port ?`
	`MGMT MGMT Interface`
	`shared-lom Shared LOMRouter(config-ucse)#imc access-port shared-lom ?`
	`GE1 GE1`
	`TE2 TE2`
	`TE3 TE3`
	`console Console`
	`failover Failover`

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.

Parameter name	Description
Assign priority	Assign the priority.

Parameter scope	Scope description
Global (indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices.
Device specific (indicated by a host icon)	Use a device-specific value for the parameter. 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.
Default	When Default is selected, this field is not enabled.



CHAPTER 4

Basic Settings for Cisco SD-WAN Manager

Basic system settings

Basic system settings are a set of parameters that enable the Cisco Catalyst SD-WAN fabric to function. They include

- device properties such as name and IP address
- network time configuration
- user access to devices
- system logging, and
- network interface parameters.

Device and SD-WAN Control Component properties

Device and SD-WAN Control Component properties, together called host properties, are the parameters that Cisco Catalyst SD-WAN uses to construct a view of the network topology. They include:

- Device system IP address:

  This provides a fixed location of the device in the overlay network. This address is independent of any of the interfaces and interface IP addresses on the device. The system IP address is one of the four components of the Transport Location (TLOC) property of each device.

- IP address of the SD-WAN Validator for the network domain, or a domain name system (DNS) name that resolves to one or more IP addresses for SD-WAN Validator:

  An SD-WAN Validator automatically orchestrates the process of bringing up the overlay network, admitting a new device into the overlay, and providing the introductions that allow the device and SD-WAN Controllers to locate each other.

- Domain identifier and the site identifier:

  These system-wide host properties are required on all devices, except for the SD-WAN Validators, to allow the Cisco Catalyst SD-WAN software to construct a view of the topology

Configure the host properties. Refer to the information about the overlay network bring-up process in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Time and NTP

Network Time Protocol (NTP), is a networking protocol for synchronizing the clocks of devices throughout a network. It ensures that the time on all participating components of the network is accurate and synchronized.

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

User authentication and access with AAA, RADIUS, and TACACS+

Authentication, authorization, and accounting (AAA) is a framework for controlling access to resources. It includes:

- Authentication: Verifying the identity of a user or device seeking access.
- Authorization: Authorizing access to the resources a user is permitted to use, based on predefined policies and privileges.
- Accounting: Tracking and logging user activities within the network.

In Cisco Catalyst SD-WAN, AAA, in combination with RADIUS and Terminal Access Controller Access-Control System (TACACS+) user authentication, controls which users are allowed access to devices, and what operations they are authorized to perform after they are logged in or connected to the devices.

The Cisco Catalyst SD-WAN implementation of AAA includes:

- Authentication: Users log in with a username and a password. A local device can authenticate users or authentication can be performed by a remote device, either a RADIUS server or a TACACS+ server, or both in a sequence.
- Authorization: Authorization is implemented using role-based access. Access is based on groups that are configured on the devices. A user can be a member of one or more groups. User-defined groups are considered when performing authorization, that is, the Cisco Catalyst SD-WAN software uses group names received from RADIUS or TACACS+ servers to check the authorization level of a user. Each group is assigned privileges that authorize the group members to perform specific functions on the corresponding device. These privileges correspond to specific hierarchies of the configuration commands and the corresponding hierarchies of operational commands that members of the group are allowed to view or modify.
- Accounting: From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, accounting generates a record of commands that a user executes on a device. Accounting is performed by a TACACS+ server.

Authentication for WANs and WLANs

Wide area networks (WAN) and wireless local area networks (WLAN) are two types of networks primarily differentiated by geographical reach and connectivity methods.

- Geographical reach: Extensive for WAN; limited for WLAN, such as a single building.
- Connectivity: Combination of wired and wireless technologies for WAN; wireless for WLAN.

Authentication methods differ for WAN and WLAN.

Authentication for wired networks

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

IEEE 802.1X authentication requires three components:

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

Authentication for wireless networks

For wireless LANs (WLANs), routers can run IEEE 802.11i to prevent unauthorized network devices from gaining access to the WLANs. IEEE 802.11i implements Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) to provide authentication and encryption for devices that want to connect to a WLAN. WPA authenticates individual users on the WLAN using a username and a password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2–compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher. Authentication is done by either using preshared keys or through RADIUS authentication.

Network segmentation

Network segmentation is the division of a network into smaller, isolated logical segments.

Segmentation is a fundamental part of enhancing security, improving network performance, and simplifying manageability. The core idea is to restrict communication between different parts of the network.

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

Network interface properties

A network interface is the component that enables a device in a network to connect to other devices, to send and receive data. There are numerous interface properties relevant to a Cisco Catalyst SD-WAN fabric.

VPN

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

Devices use VRFs in place of VPNs. When you configure a device in SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

The fabric has these types of VPNs and VRFs:

- VPN 0: Transport VPN:

  Carries control traffic using the configured WAN transport interfaces. Initially, VPN 0 contains all the interfaces on a device except for the management interface, and all the interfaces are disabled. This is the global VRF in Cisco IOS XE Catalyst SD-WAN software.

- VPN 512: Management VPN:

  Carries out-of-band network management traffic among the devices in the fabric. The interface used for management traffic is in VPN 512.

  - On devices, VPN 512 is configured by default and enabled. On devices, the management VPN is converted to VRF Mgmt-Intf.
  - On SD-WAN Control Components, VPN 512 is not configured by default.

Other properties

For each network interface, you can configure a number of interface-specific properties, such as

- DHCP clients and servers
- VRRP
- interface MTU and speed, and
- Point-to-Point Protocol over Ethernet (PPPoE).

At a high level, for an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

Management and monitoring options

Management interfaces enable you to manage and monitor devices in the Cisco Catalyst SD-WAN fabric, allowing you to collect information from the devices in an out-of-band fashion and to perform operations on the devices, such as configuring and rebooting them.

These are the available management interfaces:

- CLI
- IP Flow Information Export (IPFIX)
- REST API
- SNMP
- System logging (syslog) messages
- Cisco SD-WAN Manager

CLI through SSH

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

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

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

IPFIX

The IP Flow Information Export (IPFIX) protocol, also called cflowd, is a tool for

- monitoring the traffic flowing through devices in the Cisco Catalyst SD-WAN fabric, and
- exporting information about the traffic to a flow collector.

cflowd version

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

Aggregating information

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

Devices do not cache any of the records that are exported to a collector.

For a list of elements exported by IPFIX, refer to the information about traffic flow monitoring with Cflowd in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

Enabling the collection of traffic flow information

To enable the collection of traffic flow information, you must create data policies that identify the traffic of interest, and then direct that traffic to a Cflowd collector. Refer to the information about traffic flow monitoring with Cflowd in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

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

REST API

The Cisco Catalyst SD-WAN representational state transfer (REST) application programming interface (API) is a programmatic interface for controlling, configuring, and monitoring the devices in the network.

You can access the REST API through Cisco SD-WAN Manager.

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

SNMP

The Simple Network Management Protocol (SNMP) is an internet standard protocol that allows you to manage all the devices in the Cisco Catalyst SD-WAN network.

SNMP version

Cisco Catalyst SD-WAN supports supports SNMP v2c.

For SNMPv3, the PDU type for notifications is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

Configuring SNMP

You can configure:

- Properties for a device, such as device name, location, contact, and community, to enable the device to be monitored by a network management system.
- SNMP servers to receive SNMP trap messages.
- SNMP traps and trap groups. SNMP traps are messages that devices send to indicate an event or problem.

SNMP management information base

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

System log messages

System log (syslog) messages are records of events on a device that form a chronological log of the device status for auditing, debugging problems, and so on.

System logging operations use a mechanism similar to the UNIX **syslog** command to record system-wide, high-level operations that occur on the devices in the Cisco Catalyst SD-WAN network.

The log levels (priorities) of the messages are the same as those in standard UNIX commands. You can configure the priority of the syslog messages to log.

You can configure logging to store the syslog files locally on the device or to send them to a remote host.

Cisco SD-WAN Manager

Cisco SD-WAN Manager is a centralized network management system that

- allows configuration and management of the devices in the Cisco Catalyst SD-WAN fabric, and
- provides a dashboard displaying the operations of the entire network and of individual devices in the network.

Three or more Cisco SD-WAN Manager servers are consolidated into a Cisco SD-WAN Manager cluster to

- provide scalability and management support for up to 6,000 devices
- distribute Cisco SD-WAN Manager functions across multiple devices, and
- provide redundancy of network management operations.

Enforce a software version on devices

If you are using the Cisco Catalyst SD-WAN hosted service, you can enforce a version of the Cisco Catalyst SD-WAN software to run on a router when it first joins the overlay network.

To ensure that templates are in sync after an upgrade that enforces a software version, make sure of these before you perform the upgrade:

- The bootflash and flash on the router must have enough free space to support the upgrade
- The version of the SD-WAN image that is on the device before the upgrade must be a lower version than the enforced SD-WAN version you specify in the procedure in this section
- For ZTP enforcement feature to start, initial onboarding has to be done through PNP/ZTP workflow.

Before you begin

- Ensure that the bootflash and flash on the router have enough free space to support the upgrade.
- Ensure that the version of the SD-WAN image that is on the device before the upgrade is a lower version than the version of the software image you are enforcing with this procedure.

- For ZTP enforcement feature to start, initial onboarding has to be done through the Plug-and-Play/ZTP workflow.

Follow these steps to enforce a specific software version to run a device when it first joins the fabric.

Procedure

Step 1 Ensure that the software image for the desired device software version is present in the Cisco SD-WAN Manager software image repository:

a) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

The **Software Repository** page opens and displays a table of software images. If the desired software image is present in the repository, continue with Step 2.

b) If you need to add a software image, click **Add New Software**.

c) Select the location from which to download the software images, either Cisco SD-WAN Manager, Remote Server, or Remote Server - Cisco SD-WAN Manager.

d) Select an x86-based or a MIPS-based software image.

e) To place the image in the repository, click **Add**.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 3 Click **Enforce Software Version (ZTP)**.

If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, locate **Enforce Software Version (ZTP)** and click **Edit**.

Step 4 For a specific platform, enable enforcing the software version.

Step 5 Do one of these:

- Use an image on a local server:
  - **a.** In the **Image Location** field, choose **Local Server**.
  - **b.** In the **Version/Image Name** field, choose an image.
- Use an image on a remote server:
  - **a.** In the **Image Location** field, choose **Remote Server**.
  - **b.** In the **Remote Server Name** field, choose a server.
  - **c.** In the **Image Filename** field, choose an image.

Step 6 Click **Save**.

Configure a login page banner using a configuration group

You can configure the banner text for login pages.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Follow these steps to configure a login page banner.

Procedure

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

Step 2 Create and configure a Banner feature in a System profile.

Table 16: Banner Basic Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Login	Enter the text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type \n.
Message of the Day	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.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure a login page banner, using templates

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

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

Before you begin

Follow these steps to configure a login page banner.

Procedure

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

Step 2 Click **Feature Templates**, click **Add Template**, and select an appropriate device model.

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

Step 3 Select **Cisco Banner** from the list of templates.

Step 4 Configure these parameters:

Table 17: Configuring a banner:

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

Step 5 To save the feature template, click **Save.**

Configure a login page banner, using CLI commands

Before you begin

Perform these steps to configure a login banner using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use the **banner** command to configure a login page banner.

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

Create a custom banner

Before you begin

Follow these steps to create a custom banner that is displayed when you log in to Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **Banner**.

Step 3 Enable the **Configure a login banner for the Cisco Catalyst SD-WAN Manager system** control.

Step 4 In **Banner Info**, enter the text string for the login banner or click **Select a File** to download a file that contains the text string.

Step 5 Click **Save**.

Configure device statistics collection

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

An update in Cisco Catalyst SD-WAN Manager Release 20.16.1 improves the performance of statistics processing, with faster performance and better scalability.

By default, devices enable collecting statistics groups such as Aggregated SAIE and AppHosting.

To delete previously collected data from the statistics database, use the REST API provided in the Cisco Developer Documentation.

Before you begin

Perform these steps to configure device statistics.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **Statistics Database Configuration**.

For Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Statistics Setting** and **Edit**.

Step 3 For each statistics group, enable or disable as desired.

To collect statistics exclusively for Cisco SD-WAN Analytics, select the **Analytics only** option for the group.

To enable or disable for specific devices in the network, select the **Custom** option for the group and specify the devices.

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

Configure the time interval for collecting device statistics

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

Before you begin

Perform these steps to configure device statistics.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 To modify the time interval at which device statistics are collected, click **Statistics Configuration**.

Step 3 Enter the required **Collection Interval** in minutes.

Range: 5 to 180 minutes

Default: 30 minutes

From Cisco Catalyst SD-WAN Manager Release 20.9.6, SD-WAN Manager collects device statistics files at a higher frequency, independent of the configured collection intervals.

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

Configure the SD-WAN Manager server maintenance window

Before you begin

Perform these steps to set or cancel the start and end times and the duration of the maintenance window for the Cisco SD-WAN Manager server.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Maintenance Window**.

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

To cancel the maintenance window, click **Cancel**.

Step 3 Click the **Start Date** and **Start Time** drop-down list. Select the date and time when the **Maintenance Window** will start.

Step 4 Click the **End Date** and **EndTime** drop-down list. Select the date and time when the **Maintenance Window** will end.

Step 5 Click **Save**. The start and end times and the duration of the maintenance window are displayed in the **Maintenance Window** bar.

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

Configure device basic settings using a configuration group

Before you begin

Perform these steps to configure basic parameters for devices.

Procedure

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

Step 2 Create and configure a Basic feature in a System profile.

a. Configure basic settings.

Table 18: Basic Settings

Field	Description
Time Zone	Choose the time zone to use on the device.
Device Groups	Enter the names of one or more groups to which the device belongs, separated by commas.
Location	Enter a description of the location of the device. It can be up to 128 characters.
Description	Enter any additional descriptive information about the device.
Console Baud Rate(bps)	Choose the baud rate of the console connection on the router. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps). Default: 9600
Overlay ID	Specifies the overlay ID of a device in the Cisco Catalyst SD-WAN overlay network. Range: 0 - 4294967295 ($2^{32} – 1$) Default: 1
Controller Group	List the Cisco Catalyst SD-WAN Controller groups to which the router belongs.
Max OMP Sessions	Set the maximum number of OMP sessions that a router can establish to a Cisco SD-WAN Controller. Range: 1 through 100

b. Configure controller settings.

c. Configure GPS.

Table 19: 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.

d. Configure track settings.

Table 20: 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.

e. Configure advanced settings.

Table 21: 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

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure device basic system settings using templates

Create a Cisco System feature template to configure device system settings.

You can create a Cisco System feature template directly or through a device template.

Before you begin

Follow these steps to create a Cisco System feature template.

Procedure

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

Step 2 Select **Feature Templates**.

Step 3 Click **Add Template**.

Step 4 Select a platform.

Step 5 Click **Cisco System**.

Step 6 According to your needs, configure one or more of these sections.

a) To configure system-wide functionality on a Cisco Catalyst SD-WAN device, select the **Basic Configuration** tab and configure these parameters.

Table 22:

Field	Description
Site ID (on routers, Cisco SD-WAN Manager instances, and Cisco SD-WAN Controller)	Identifier of the site in the SD-WAN fabric domain where the device resides, such as a branch, campus, or data center. The site ID must be the same for all devices at the same site. Range: 1 through 4,294,967,295 (2^{32} – 1, or hexadecimal 0x100000000 – 1)
System IP	System IP address for the Cisco Catalyst SD-WAN device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0.
Timezone	Timezone to use on the device.
Hostname	Name for the device. Maximum 32 characters.
Location	Description of the location of the device. Maximum 128 characters.
Device Groups	Names of one or more groups to which the device belongs, separated by commas.
Controller Groups	SD-WAN Controller groups to which the router belongs.
Description	Additional descriptive information about the device.
Console Baud Rate	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 (from Cisco vManage Release 20.3.1)
Maximum OMP Sessions	Maximum number of OMP sessions that a router can establish to a Cisco Catalyst SD-WAN Controller. Range: 0 through 100 Default: 2

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

Table 23:

Field	Description
Latitude	Latitude of the device, in the format *decimal-degrees*.
Longitude	Longitude of the device, in the format *decimal-degrees*.

c) To track the status of transport interfaces that connect to the internet (Network Address Translation Direct Internet Access (NAT DIA),

- click **Tracker** and **New Endpoint Tracker**, or
- click **Tracker Group** and **New Endpoint Tracker Group**.

Then configure these parameters.

Table 24:

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Tracker Type	Choose an interface, static route.
Threshold	How long to wait for the probe to return a response before declaring that the transport interface is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Interval	How often probes are sent to determine the status of the transport interface. Range: 10 to 600 seconds Default: 60 seconds (1 minute)
Multiplier	Number of times to resend probes before declaring that the transport interface is down. Range: 1 to 10 Default: 3
Tracker Type	Interface or static route.
Endpoint Type	IP address or DNS name.
Endpoint IP or Endpoint DNS Name	Endpoint IP. or DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.

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

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

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

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

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

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

For more information on NAT DIA tracker for Cisco IOS XE Catalyst SD-WAN devices, refer to NAT DIA Tracker in the *Cisco Catalyst SD-WAN NAT Configuration Guide*.

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

To monitor endpoint trackers, see Monitor NAT DIA endpoint trackers, on page 86.

d) To configure additional system parameters, click **Advanced** and configure these parameters:

Field	Description
Control Session Policer Rate	Maximum rate of DTLS control session traffic, to police the flow of control traffic. Range: 1 to 65535 pps Default: 300 pps
Port Hopping	Click **On** to enable port hopping, or click **Off** to disable it. When a 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 devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. To disable port hopping on an individual TLOC (tunnel interface), use the VPN Interface Ethernet configuration template. Default: Enabled on routers. Disabled on Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Controller hosts.
Port Offset	Number by which to offset the base port number. Configure this option when multiple devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. Range: 0 to 19
Track Transport	**On** : Regularly check whether the DTLS connection between the device and a Cisco Catalyst SD-WAN Validator is up. **Off**: Disable checking. Default: Enabled
Track Interface	Tag string to include in routes associated with a network that is connected to a non-operational interface. Range: 1 to 4,294,967,295

Field	Description
Gateway Tracking	**On** : Enable tracking of default gateway. **Off**: Disable tracking. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the device's route table. Default: Enabled
Collect Admin Tech on Reboot	**On** : Collect admin-tech information when the device reboots. **Off**: Disable collection.
Idle CLI Timeout in minutes	How long to wait, when the CLI is inactive, to log out the user. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires. Default: CLI session does not time out.

Monitor NAT DIA endpoint trackers

Monitor the NAT DIA endpoint tracker configuration.

Configure NAT DIA endpoint trackers using Configure device basic settings using a configuration group, on page 80 or Configure device basic system settings using templates, on page 82.

Before you begin

Follow these steps to monitor the NAT DIA endpoint tracker configuration.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Select a device from the list of devices.

Step 3 Click **Real Time**.

Step 4 From the **Device Options** drop-down list, choose **Endpoint Tracker Info**.

Configure global system settings using a configuration group

Before you begin

Perform these steps to configure basic parameters for devices.

Procedure

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

Step 2 Create and configure a Global feature in a System profile.

a) Configure services.

Table 25: 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).
Specify interface for source address	Enter the address of the source interface in all HTTPS client connections.

b) Configure NAT64.

Table 26: 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)

c) Configure authentication.

Table 27: Authentication

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

d) Configure SSH.

Table 28: SSH Version

Field	Description
SSH Version	Choose the SSH version. Default: Disabled

e) Configure other settings.

Table 29: 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.
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.

Field	Description
(optional) **Interface statistics per minute**	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Choose the time interval for interface statistics data collection: • **1 minute** • **5 minutes** (default)

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure global system settings using templates

Configure global system settings using templates.

From Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x, you can use the Global Settings template to configure device global parameters such as:

- Services such as HTTP and Telnet
- NAT64 time-outs
- HTTP authentication mode
- TCP keepalive
- TCP and UDP small servers
- Console logging
- IP source routing
- VTY line logging
- SNMP IFINDEX persistence
- BOOTP server

Before you begin

Follow these steps to configure global system settings.

Procedure

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

Step 2 Click **Feature Templates**.

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

Step 3 Click **Add Template**.

Step 4 Select a device type.

Step 5 Create a Global Settings template.

Step 6 Enter a name and description.

Step 7 Configure these parameters according to your requirements.

a) Configure services.

Field	Description
HTTP Server	Enable or disable HTTP server.
HTTPS Server	Enable or disable secure HTTPS server.
Passive FTP	Enable or disable passive FTP.
IP Domain-Lookup	Enable or disable domain name server (DNS) lookup.
Arp Proxy	Enable or disable proxy ARP.
RSH/RCP	Enable or disable remote shell (RSH) and remote copy (RCP) on the device.
Telnet (Outbound)	Enable or disable outbound telnet.
CDP	Enable or disable Cisco Discovery Protocol (CDP). From Cisco IOS XE SD-WAN Release 17.3.1, CDP on interfaces is enabled when the **cdp run** command is executed globally on Cisco ASR 1000 series devices.

b) Configure NAT64.

Field	Description
UDP Timeout	NAT64 translation timeout for UDP Range: 1 to 65536 (seconds) Default: 300 seconds (5 minutes) **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default UDP Timeout value for NAT64 has changed to 300 seconds (5 minutes).
TCP Timeout	NAT64 translation timeout for TCP Range: 1 to 65536 (seconds) Default: 3600 seconds (1 hour) **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default TCP Timeout value for NAT64 has been changed to 3600 seconds (1 hour).

c) Configure authentication.

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

d) Configure SSH.

Field	Description
SSH version	Specify an SSH version. Default value: Version 2

e) Configure 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.
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.

Configure global system settings using CLI commands

Configure global system settings using CLI commands in a CLI add-on profile or CLI add-on template.

These CLI instructions are not comprehensive.

Before you begin

Perform these steps to configure global system settings using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enable or disable services.

Enable services:

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

Note
From Cisco IOS XE SD-WAN Release 17.3.1, CDP on interfaces is enabled when the **cdp run** command is executed globally on Cisco ASR 1000 series devices.

Enable outbound Telnet:

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

Disable services:

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

Disable outbound Telnet:

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

Step 3 Enable or disable other settings.

Enable:

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

```
    snmp-server ifindex persist
    ip bootp server
```

Disable:

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

Step 4 Configure NAT64.

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

Step 5 Configure authentication.

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

Configure NTP servers using a configuration group

Configuring network time for your network includes these tasks:

1. Configure NTP servers and parameters as described in this procedure.
2. Configure the timezone in a System profile, in a Basic feature.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Perform these steps to configure NTP servers and parameters.

Procedure

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

Step 2 Create and configure an NTP feature in a System profile.

a) Configure a server.

Table 30: Server

Field	Description
Add Server	

Field	Description
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: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
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.

b) Configure authentication.

Table 31: 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**.

c) Configure advanced parameters.

Table 32: 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.
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 Interface	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`**.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure NTP servers and parameters using templates

Configure network time protocol (NTP) servers using a Cisco NTP feature template.

You can create a Cisco NTP feature template directly or through a device template.

Configuring network time for your network includes these tasks:

1. Configure NTP servers and parameters as described in this procedure.
2. Configure the timezone in a System template.

Before you begin

Perform these steps to configure NTP servers and parameters.

Procedure

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

Step 2 Select **Feature Templates**.

Step 3 Click **Add Template**.

Step 4 Select a platform.

Step 5 Click **Cisco NTP**.

Step 6 To add an NTP server:

a) Click **Server**.

b) Click **New Server**, and configure these parameters.

Table 33: NTP server parameters

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

c) You can click **Add** to add another server.
d) Click **Save**.

Step 7 To configure the authentication keys used to authenticate NTP servers:

a) Click **Authentication**.
b) Click the **Authentication Key** tab.
c) Click **New Authentication Key**, and configure these parameters.

Table 34: NTP authentication key parameters

Field	Description
Authentication Key ID*	• Authentication Key: Enter an authentication key ID. Range: 1 to 65535 • Authentication Value: Enter either a cleartext key or an AES-encrypted key.
Authentication Value*	Enter an authentication key. For this key to be used, you must designate it as trusted. To associate a key with a server, enter the same value that you entered in the **Authentication Key ID** field under **Server**.

d) Click **Add**.

Step 8 To configure the trusted keys used to authenticate NTP servers:

a) Click **Authentication**.

b) Click the **Trusted Key** tab.

c) Configure these parameters.

Table 35: Trusted key parameters

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

Configure a router as an NTP primary using templates

Configure a router to operate as an NTP primary using templates.

You can configure one or more supported routers as an NTP primary router in a Cisco Catalyst SD-WAN deployment. A router that is configured in this way acts as the NTP server to which other nodes in the deployment synchronize their clocks.

Configuring a router as an NTP primary router is useful if you do not have an NTP server in your deployment.

To configure a router as an NTP primary router, create a template that includes configured parameters for the NTP primary router.

Before you begin

Follow these steps to configure a router to operate as an NTP primary.

Procedure

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

Step 2 Create a new Cisco NTP feature template or edit an existing one.

- To create a new Cisco NTP feature template, click **Feature Templates**, click **Add Template**, select the type of device to be the NTP primary router, and then select the **Cisco NTP** template in the **Basic Information** section.
- To update an existing Cisco NTP feature template, click **Feature Templates**, click **...** adjacent to a template, and select **Edit**.

Step 3 For a new template, enter a name and description.

Step 4 In the **Master** tab, perform these steps:

a) For the **Master** option, choose **Global** from the drop-down list, and then select **On**.

b) (Optional) In the **Stratum** field, enter the stratum value for the NTP primary router, which is the hierarchical distance of the router from its reference clock.

Range: 1 to 15

Default: 8

c) (Optional) In the **Source** field, enter the name of the exit interface for NTP communication.

If configured, the system sends NTP traffic to this interface.

Examples: **GigabitEthernet1**, **Loopback0**

Step 5 Click **Save** for a new template, or **Update** if updating an existing template.

Configure a router as an NTP primary using CLI commands

Configure NTP using CLI commands in a CLI add-on profile or CLI add-on template.

These CLI instructions are not comprehensive.

You can configure one or more supported routers as an NTP primary router in a Cisco Catalyst SD-WAN deployment. A router that is configured in this way acts as the NTP server to which other nodes in the deployment synchronize their clocks.

Configuring a router as an NTP primary router is useful if you do not have an NTP server in your deployment.

Before you begin

Perform these steps to configure NTP settings using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use **ntp master** to configure a device as primary.

Optionally, include a stratum value for the NTP primary router. The stratum value defines the hierarchical distance of the router from its reference clock. For *stratum-number*:

- Range: 1 to 15
- Default: 8

```
ntp master [stratum-number]
```

Step 3 (Optional) Use **ntp source** to configure an NTP source, which is an exit interface for NTP communication.

If configured, the system sends NTP traffic to this interface.

Examples for *source-interface*: **GigabitEthernet1**, **Loopback0**

```
ntp source source-interface
```

Configure NTP servers using CLI commands

Configure NTP servers using CLI commands in a CLI add-on profile or CLI add-on template.

Before you begin

Perform these steps to configure NTP servers.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enter system configuration mode.

```
system
```

Step 3 Enter NTP configuration mode.

```
ntp
```

Step 4 Enter keys configuration mode.

```
keys
```

Step 5 Configure an authentication type to use for an NTP server. Assign a key for the authentication type, and assign one of these authentication methods: MD5, CMAC-AES-128. Using multiple instances of the **authentication** command, you can configure authentication for multiple NTP servers.

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

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

Step 6 Designate an authentication type as trusted. Optionally, you can include multiple authentication key IDs.

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

Step 7 Exit keys configuration mode.

```
exit
```

Step 8 Configure an NTP server, including the VPN and version, and optionally an authentication key. You can configure multiple NTP servers.

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

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

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

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

Configure device time using CLI commands

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

Configure the time using CLI commands in a CLI add-on profile or CLI add-on template.

Before you begin

Perform these steps to configure the time on a device using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use **clock set** to set the time.

clock set *hh:mm:ss dd month yyyy*

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

Configure GPS using a configuration group

Before you begin

Perform these steps to configure GPS for devices.

Procedure

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

Step 2 Create and configure a GPS feature in a Transport and Management profile.

Step 3 Configure GPS.

Table 36: GPS

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2,048 characters and can contain only alphanumeric characters.
GPS	Click **On** to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: • **MS-based**: Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, cell tower data is used to enhance the quality and precision in determining location, which is useful when satellite signals are poor. • **Standalone**: Use satellite information when determining position.
NMEA	Click **On** to enable the use of NMEA streams to help with determining position. NMEA streams data from the router's cellular module to any marine device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address*	Enter the IP address of the router's interface that connects to the external device reading the NMEA.
Destination Address*	Enter the IP address of the external device's interface that's connected to router.
Destination Port*	Enter the number of the port to use to send NMEA data to the external device's interface.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure GPS using templates

Configure GPS using templates.

Note You can configure GPS using Cisco SD-WAN Manager from Cisco vManage Release 20.6.1, with devices running Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later.

Configuring GPS is a prerequisite for geofencing. Refer to Geofencing in the *Cisco Catalyst SD-WAN Location Services Configuration Guide*.

Before you begin

Follow these steps to configure GPS.

Procedure

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

Step 2 Create a new GPS feature template or edit an existing one.

- To create a new GPS feature template, click **Feature Templates**, click **Add Template**, select a device type, and select the **GPS** template.
- To update an existing GPS feature template, click **Feature Templates**, click **...** adjacent to a template, and select **Edit**.

Step 3 For a new template, enter a name and description.

Step 4 Configure the GPS parameters.

Parameter Name	Description
GPS	Click **On** to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: • **MS-based**: Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, a network data session is used to obtain the GPS satellite locations, resulting in a faster fix of location coordinates. • **Standalone**: Use satellite information when determining position. **Note** Standalone mode is currently not supported for geofencing.

Parameter Name	Description
NMEA	Click **On** to enable the use of NMEA streams to help in determining position. NMEA streams data from the router's 4G LTE Pluggable Interface Module (PIM) to any device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address	(Optional) Enter the IP address of the interface that connects to the router's PIM. **Note** This option is not used for configuring geofencing.
Destination Address	(Optional) Enter the IP address of the NMEA server. The NMEA server can be local or remote. **Note** This option is not used for configuring geofencing.
Destination Port	(Optional) Enter the number of the port to use to send NMEA data to the server. **Note** This option is not used for configuring geofencing.

Step 5 Click **Save** for a new template, or **Update** if updating an existing template.

Configure automatic bandwidth detection using templates

Configure automatic bandwidth detection using templates.

Also see Configure automatic bandwidth detection using CLI commands, on page 105.

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

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

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

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

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

The set of system defined public iPerf3 servers includes:

- iperf.scottlinux.com
- iperf.he.net
- bouygues.iperf.fr
- ping.online.net
- iperf.biznetnetworks.com

Before you begin

Configure automatic bandwidth detection.

Procedure

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

Step 2 Create a new Cisco VPN Interface Ethernet feature template or edit an existing one.

- To create a new Cisco VPN Interface Ethernet feature template, click **Feature Templates**, click **Add Template**, select a device type, and select the **Cisco VPN Interface Ethernet** template.
- To update an existing Cisco VPN Interface Ethernet feature template, click **Feature Templates**, click **...** adjacent to a template, and select **Edit**.

Step 3 For a new template, enter a name and description.

Step 4 Configure bandwidth detection.

Field	Description
Auto Detect Bandwidth	When enabled, the device detects the bandwidth.
Iperf Server	To use a private iPerf3 server for automatic bandwidth detection, enter the IPv4 address of the private server. To use a public iPerf3 server for automatic bandwidth detection, leave this field blank. The private iPerf3 server should run on port 5201, which is the default iPerf3 port.

Step 5 Ensure that the **allow-service all** command is configured for the tunnel interface.

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

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

Configure automatic bandwidth detection using CLI commands

Configure automatic bandwidth detection using CLI commands.

Also see Configure automatic bandwidth detection using templates, on page 103.

To disable auto-bandwidth-detect, use the no form of the command: **no auto-bandwidth-detect**.

Before you begin

Perform these steps to configure automatic bandwidth detection.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use the **auto-bandwidth-detect** command to enable automatic bandwidth detection.

```
auto-bandwidth-detect
iperf-server ipv4-address
```

Step 3 Ensure that the **allow-service all** command is configured for the tunnel interface.

The example includes the **auto-bandwidth-detect**, **iperf-server**, and **allow-service all** commands.

```
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation gre
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
  auto-bandwidth-detect
  iperf-server 192.0.2.255
 exit
 appqoe
  no tcpopt enable
  no dreopt enable
```

Configure system logging using CLI commands

Configure system logging using CLI commands in a CLI add-on profile or CLI add-on template.

Before you begin

Perform these steps to configure system logging using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure system logging.

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

Connect to a device by SSH terminal

Establish an SSH session with a device.

Before you begin

Perform these steps to establish an SSH session with a device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.

Step 2 Select a device.

Step 3 Enter credentials to log in to the device.

You can execute CLI commands to monitor or configure the device.

Proxy server for SD-WAN Manager HTTP and HTTPS traffic with external servers

You can configure a proxy server to handle HTTP and HTTPS traffic between Cisco SD-WAN Manager and external servers.

Traffic

Here's some of the HTTP and HTTPS traffic SD-WAN Manager directs through a proxy, if configured:

- HTTPS connection for Symantec or Cisco automated certificate request or renewal
- REST API calls to URLs of these domains:

- cisco.com
- amazonaws.com
- microsoft.com
- office.com
- microsoftonline.com

Each 24 hours, SD-WAN Manager checks whether the proxy server is reachable. If the proxy server is unreachable, SD-WAN Manager raises an alarm: `HTTPS proxy server {IP} not reachable`

Benefits

Cisco SD-WAN Manager uses an HTTP or HTTPS connection to an external server for certain traffic, including:

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

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

Restrictions for a proxy server for HTTP and HTTPS traffic

These restrictions apply to using a proxy server for HTTP and HTTPS traffic between Cisco SD-WAN Manager and external servers.

Domain name resolution

When configured to communicate with external servers via an HTTP/HTTPS proxy server, SD-WAN Manager resolves fully qualified domain names (FQDNs) locally or through configured DNS servers, bypassing the proxy server.

SD-WAN Manager then sends the HTTP or HTTPS connections resulting from the resolution to the proxy server. DNS queries for the resolution of external server FQDNs must be successful before SD-WAN Manager can send the resulting connections to the proxy server for HTTP and HTTPS traffic.

SD-AVC container

There is no support for using the proxy server for traffic between the SD-AVC container, which operates as part of SD-WAN Manager, and external services.

Configure a proxy server for HTTP and HTTPS traffic

Configure a proxy server for HTTP and HTTPS traffic between Cisco SD-WAN Manager and external servers.

SD-WAN Manager verifies that the proxy server for HTTP and HTTPS traffic is reachable, and saves the server details in the configuration database. SD-WAN Manager then directs HTTP and HTTPS connections and REST API calls to external servers through the proxy server.

If the HTTP/HTTPS proxy server is not reachable, Cisco SD-WAN Manager displays an error message on the GUI indicating the reason for failure.

Before you begin

- SD-WAN Manager uses HTTPs connection to *www.cisco.com* (previously, TCP port 7 echo request was used) to validate reachability of the proxy server. Ensure that you configure your firewall and proxy server to allow the echo requests to make the destination host ports accessible.
- Enable out of band interface on single node using **Administration** > **Cluster Management** before configuring proxy server.

Perform these steps to configure a proxy server for HTTP and HTTPS traffic.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **HTTP/HTTPS Proxy**.

Step 3 For the **Enable HTTP/HTTPS Proxy** setting, click **Enabled**.

Step 4 Enter the **HTTP/HTTPS Proxy IP Address** and **Port** number.

For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. For releases from Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

Step 5 Enter a **Non Proxy Host/IP List** of IP addresses or hostnames to exclude from use with the proxy server.

Use the pipe (|) character to separate items in the list.

Step 6 Click **Save**.

Rate limit for bulk API requests

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

From Cisco vManage Release 20.10.1, send bulk API requests to the SD-WAN Manager cluster. SD-WAN Manager distributes the API requests among the clusters in the node. This distribution increases the rate limit to:

(rate-limit per node) * (number of nodes in the cluster)

This allows you to retrieve more data in a shorter duration compared to a bulk API request addressed to a single node. With the distribution, you need not send separate bulk API requests to two or more nodes in the cluster or collate the API responses.

Configure the rate limit for bulk API requests, using CLI commands

Configure the rate limit for bulk API requests.

Before you begin

Follow these steps to configure the rate limit for bulk API requests.

Procedure

Step 1 Log in to one of the Cisco SD-WAN Manager nodes in the SD-WAN Manager cluster and execute the **request nms server-proxy set ratelimit** command.

```
sdwan-manager# request nms server-proxy set ratelimit
```

Step 2 When prompted with this:

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

Enter **n**.

Step 3 When prompted with this:

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

Enter **y**.

Step 4 Enter the per-node rate limit in response to a prompt similar to this:

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

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

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

Step 5 Enter the unit time for which the rate limit applies in response to a prompt similar to this:

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

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

While SD-WAN Manager applies the rate limit to all the SD-WAN Manager instances in the cluster, the command line displays this message:

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

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

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

Step 6 Restart the server-proxy using the **request nms server-proxy restart** command.

```
sdwan-manager# request nms server-proxy restart
```

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

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

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

View the rate limit for bulk API requests

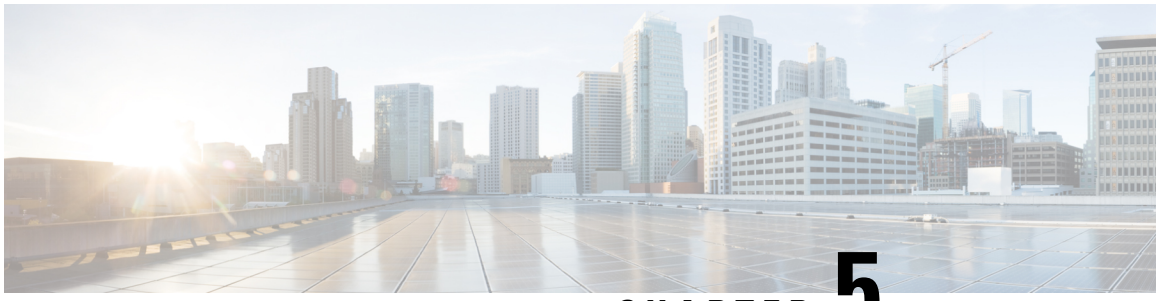
View the rate limit for bulk API requests.

Procedure

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

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

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



CHAPTER 5

Wireless Management

Feature history for wireless management

This table describes the developments of this feature, by release.

Table 37: Feature history

Feature Name	Release Information	Description
Wireless Management for ISR 1000 Series Routers with WiFi 5	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to configure wireless LAN settings on WiFi 5-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager. With Cisco SD-WAN Manager, you can automate the wireless LAN controller configuration and provide wireless connectivity without the need for another external controller to configure and manage the wireless settings on the routers.

Feature Name	Release Information	Description
Wireless Management for ISR 1000 Series Routers with WiFi 6	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables you to configure wireless LAN settings on WiFi 6-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager. The Embedded Wireless Controller on these routers facilitates wireless connectivity management without the need for an external controller.

Supported devices for wireless management

This section identifies Cisco device models that are compatible with wireless LAN management capabilities. It details the specific device models and the minimum software release versions required for wireless management on the Cisco ISR 1000 Series, assisting users in verifying their hardware for wireless deployments.

The following table displays a list of Cisco ISR 1000 Series routers that include the WLAN module.

Table 38: Cisco ISR 1000 Series Routers

Device Family	Device Name	Release Version
Cisco ISR 1000 Series Routers with WLAN module supporting WiFi 5	• C1101-4PLTEPW • C1109-4PLTE2PW • C1111-4PW • C1111-8PLTEEAW • C1111-8PW • C1112-8PLTEEAW • C1112-8PW • C1113-8PLTEEAW • C1113-8PMW • C1113-8PW • C1116-4PLTEEAW • C1116-4PW • C1117-4PLTEEAW • C1117-4PLTELAW • C1117-4PMLTEEAW • C1117-4PMW • C1117-4PW • C1121-8PLTEPW • C1121X-8PLTEPW	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1
Cisco ISR 1000 Series Routers with WLAN module supporting WiFi 6	• C1131X-8PLTEPW • C1131-8PLTEPW • C1131X-8PW • C1131-8PW	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1

Prerequisites for wireless management on Cisco ISR 1000 series routers

WLAN module VLAN association

Add the management interface of the Wireless LAN (WLAN) module to a specific VLAN in order to access servers such as DHCP and RADIUS.

DHCP server

Configure a DHCP server to assign the IP address for the access point.

SVI for WLAN controller

Configure a switch virtual interface (SVI) on the Cisco ISR 1000 Services Router for virtual WLAN controller management.

Restrictions for wireless management on Cisco ISR 1000 series routers

Single Cisco mobility express access point

Configure only one access point on the LAN side of the router when using Cisco Mobility Express. However, you can connect other external access points to the router that are not configured with Cisco Mobility Express.

Absence of other wireless controllers

Ensure that no other wireless controllers are accessible on the LAN side of the router.

Wireless management on ISR 1000 series routers

Wireless Management on Cisco ISR 1000 Series Routers is a capability that enables the configuration and management of wireless LAN settings, provisioned through a Wireless LAN (WLAN) module, and utilizing an embedded virtual wireless LAN controller. This feature provides wireless connectivity without the need for an external controller to manage the router's wireless settings.

This capability is implemented through:

- WLAN Module Provisioning: A WLAN module is provisioned on the Cisco ISR 1000 Series Routers to provide wireless connectivity
- Embedded Virtual Controllers (EWC): The WLAN module hosts a virtual wireless LAN controller.
- Cisco SD-WAN Manager Integration: Wireless settings are configured and managed using SD-WAN Manager.

Cisco Mobility Express

Cisco Mobility Express is a virtual wireless LAN controller installed in the WLAN module of WiFi 5-capable Cisco ISR 1000 Series Routers. It provides the interface where wireless settings for LAN access are available.

Embedded wireless controller

The Embedded Wireless Controller is a virtual wireless controller installed on the WLAN module of WiFi 6-capable C1131 Cisco IOS XE Catalyst SD-WAN devices. Similar to Cisco Mobility Express, the EWC provides the interface for wireless LAN access settings.

Configure wireless management on Cisco ISR 1000 series routers using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

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

Step 2 Create and configure a Wireless LAN feature in Service profile.

a) Configure the basic details for the wireless LAN.

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.

b) Configure ME IP address.

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.

c) Configure the Wi-Fi SSID details for setting up a wireless LAN.

Field	Description
Add SSID	

Field	Description
SSID Name*	Enter a name for the wireless SSID. It can be a string from 4 to 32 characters. The SSID must be unique.
Admin State*	Enable this option to indicate that the interface has been configured.
Broadcast SSID*	Enable this option if you want to broadcast the SSID. Disable this option if you do not want the SSID to be visible to all the wireless clients.
VLAN (Range 1-4094)*	Enter a VLAN ID for the wireless LAN traffic.
Radio Type	Choose one of the following radio types: • **2.4GHz** • **5GHz** • **All**
Security Type*	Choose a security type: • **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server. • **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase. • **Open**: Choose this option to allow access to the wireless network without authentication.
Passphrase*	This field is available if you choose **WPA2 Personal** as the security type. Set a pass phrase. This pass phrase provides users access to the wireless network.
QoS Profile	Choose a QoS profile.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure wireless management on ISR 1000 series routers

Use this procedure to configure and manage wireless settings on your Cisco ISR 1000 Series Routers using Cisco SD-WAN Manager. This task allows you to enable wireless LAN functionality directly on the router, leveraging its embedded wireless controller capabilities.

Wireless management on ISR 1000 Series Routers enables you to set up wireless LANs (WLANs) directly on the router, utilizing its embedded wireless controller. This eliminates the need for an external wireless LAN controller, simplifying network architecture and management.

Before you begin

- Ensure your Cisco ISR 1000 Series Router is a supported model with a WLAN module (WiFi 5 or WiFi 6 capable).
- Confirm that necessary network prerequisites, such as DHCP server availability and proper VLAN configuration for the WLAN module's management interface, are in place.

Follow these steps to configure wireless management using feature templates in Cisco SD-WAN Manager:

Procedure

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

Step 2 Click **Feature Templates**.

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

Step 3 Click **Add Template** to select an appropriate device model.

Step 4 In the left pane, from **Select Devices**, choose a Cisco ISR 1000 Series Router for which you are creating a template.

Step 5 Under **OTHER TEMPLATES**, click **ISR1K Wireless** to select it as the feature template.

Step 6 In the **Template Name** field, enter a name for the feature template.

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

Step 7 In the **Description** field, enter a description for the feature template.

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

Step 8 Enter the Wi-Fi SSID details for setting up a wireless LAN:

Parameter Name	Description
Wireless Network Name (SSID)	Enter a name for the wireless SSID. It can be a string from 4 to 32 characters. The SSID must be unique.
VLAN (Range 1-4094)	Enter a VLAN ID for the wireless LAN traffic.
Security Type	Choose a security type: • **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server. • **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase. • **Open**: Choose this option to allow access to the wireless network without authentication.

Parameter Name	Description
RADIUS Server IP	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the IP address of the RADIUS server.
Authentication Port	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the authentication port number of the RADIUS server.
Shared Secret	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the shared secret key of the RADIUS server.
Passphrase	(Optional) This field is available if you choose the **WPA2 Personal** option as the security type. Set a pass phrase. This pass phrase provides users with access to the wireless network.
Admin State	Choose an admin state.
Radio Type	Choose one of the following radio types: • **2.4GHz** • **5GHz** • **Both**
Broadcast SSID	Choose **On** to broadcast the SSID. Choose **Off** if you do not want the SSID to be visible to all the wireless clients.
QoS Profile	Choose a QoS profile.

Step 9 Enter the **General** details for the wireless LAN:

Parameter Name	Description
Country	Choose the country where the ISR is installed.
Username	Specify the username of Cisco Mobility Express. If you are using a C1131 Cisco IOS XE Catalyst SD-WAN device specify the username for the EWC.
Password	Specify the password for Cisco Mobility Express or the EWC.

Step 10 Enter the **Advanced** details for the wireless LAN:

Parameter Name	Description
Controller IP Address	**Note** For Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and Cisco vManage Release 20.6.1 and earlier releases, this field is displayed as **ME IP Address.** Specify the Management IP address of Cisco Mobility Express or EWC.
Subnet Mask	Specify the subnet mask for the Management IP address.
Default Gateway	Specify the default gateway address of Cisco Mobility Express or EWC.
2.4GHz Shutdown	Click **Yes** to shut down the 2.4 GHz radio type. Click **No** to not shut down this radio type.
5GHz Shutdown	Click **Yes** to shut down the 5 GHz radio type. Click **No** to not shut down this radio type.

Step 11 Click **Save** to save your wireless configuration.

After completing these steps, the wireless LAN settings are configured on your Cisco ISR 1000 Series Router via the feature template, enabling wireless connectivity.

What to do next

Deploy the configured feature template to the desired devices. For more information, see Deploy a Configuration Group.

Configure wireless management on Cisco ISR 1000 series routers using CLI commands

Use this procedure to apply Command Line Interface (CLI) templates to configure wireless LAN settings on your Cisco ISR 1000 series routers. This method allows for direct configuration using pre-defined command sets.

CLI templates are pre-configured sets of commands that simplify the deployment of wireless settings. They allow for precise control over radio profiles, WLAN SSIDs, and general wireless LAN parameters. By default, these commands are executed in global configuration mode.

Before you begin

Ensure you have console or SSH access to the Cisco ISR 1000 series router.

Follow these steps to configure wireless management settings using CLI templates:

Configure a WLAN profile using a CLI template

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

```
wlan-profile wlan-profile-sample-1
vlan-id 100
ssid sample-ssid-1
data-security personal
passphrase 0 Pass-Phrase-Sample123#
qos-type silver
wlan-profile wlan-profile-sample-2
vlan-id 200
ssid sample-ssid-2
data-security enterprise
aaa radius-server 10.2.3.4 auth-port 1812 shared-secret 0 EsrdT_23sss

qos-type gold
nobroadcast-ssid
```

Configure general WLAN settings using a CLI template

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

Here is the complete configuration example that shows that show how to configure and manage wireless settings on Cisco ISR 1000 Series Routers.

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto
```

```
wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

Procedure

Step 1 Access the router's command-line interface.

Log in to your Cisco ISR 1000 series router.

Step 2 Enter global configuration mode.

From privileged EXEC mode, enter configure terminal.

```
Router# configure
Router(config)#
```

Step 3 Configure the radio profiles.

Apply the necessary CLI commands to define the 2.4GHz and 5GHz radio settings, such as shutdown status, channel, and bandwidth.

```
radio-profile 24ghz
shutdown
exit
radio-profile 5ghz
no shutdown
```

Step 4 Configure the WLAN profiles.

Apply the CLI commands to define your wireless SSIDs, including VLAN IDs, security types (WPA2 Personal, WPA2 Enterprise, Open), passphrases, RADIUS server details, and QoS profiles.

```
wlan-profile wlan-profile-sample-1
vlan-id 100
ssid sample-ssid-1
data-security personal
passphrase 0 Pass-Phrase-Sample123#
qos-type silver
wlan-profile wlan-profile-sample-2
vlan-id 200
ssid sample-ssid-2
data-security enterprise
aaa radius-server 10.2.3.4 auth-port 1812 shared-secret 0 EsrdT_23sss

qos-type gold
nobroadcast-ssid
```

Step 5 Configure general wireless LAN settings.

Apply the CLI commands to set the country code, management IP address, default gateway, and management credentials for Cisco Mobility Express or the Embedded Wireless Controller (EWC).

```
wireless-lan country US
wireless-lan mgmt ip address10.16.1.100 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 0 sRe32dfst#asd
```

Step 6 Commit the configuration changes.

Here is the complete configuration example that shows that show how to configure and manage wireless settings on Cisco ISR 1000 Series Routers.

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

The wireless management settings are applied to your Cisco ISR 1000 series router using the specified CLI templates. The router's wireless module will now operate according to the configured radio and WLAN profiles.

This section provides a sample Command Line Interface (CLI) configuration for wireless management on Cisco ISR 1000 Series Routers. This example illustrates a complete setup, including WLAN profiles, radio settings, and general wireless LAN management parameters, serving as a factual representation for reference and implementation. Refer to Configuration example for wireless configuration on Cisco ISR 1000 series routers, on page 123.

What to do next

Monitor the wireless configuration to verify that the settings are active and functioning as expected. For verfication steps, refer to Monitor wireless configuration on Cisco ISR 1000 series routers, on page 123.

Monitor wireless configuration on Cisco ISR 1000 series routers

Use this procedure to monitor the wireless settings configured on your Cisco ISR 1000 series routers using Cisco SD-WAN Manager. This allows you to verify the operational status of your wireless LAN, including radio parameters, SSID information, and connected clients.

After configuring wireless management, it is essential to monitor the operational status to ensure that the settings have been applied correctly and the wireless network is functioning as expected. Cisco SD-WAN Manager provides real-time monitoring capabilities for this purpose.

Before you begin

- Wireless management must be configured and deployed on the Cisco ISR 1000 Series Router.
- You must have access to Cisco SD-WAN Manager with appropriate monitoring permissions.

Follow these steps to monitor the wireless configuration using Cisco SD-WAN Manager:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, navigate to **Monitor** > **Network**.

Step 2 Choose a router from the list of the routers.

Step 3 Click **Real Time** in the left pane.

Step 4 From the **Device Options** drop-down list, choose one of the following options:

Device Option	Description
Wireless Radio	Displays the radio parameters of the wireless LAN.
Wireless SSID	Displays information about the wireless SSID.
Wireless Clients	Displays information about the wireless clients in the wireless LAN.

Upon selecting a device option, the real-time data for the chosen wireless aspect (Radio, SSID, or Clients) is displayed, providing insight into the current state of the wireless configuration on the selected Cisco ISR 1000 Series Router.

Configuration example for wireless configuration on Cisco ISR 1000 series routers

This section provides a sample CLI configuration for wireless management on Cisco ISR 1000 series routers. This example illustrates a complete setup, including WLAN profiles, radio settings, and general wireless LAN management parameters, serving as a factual representation for reference and implementation.

Wireless configuration example

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

Troubleshooting wireless configuration on Cisco ISR 1000 series routers

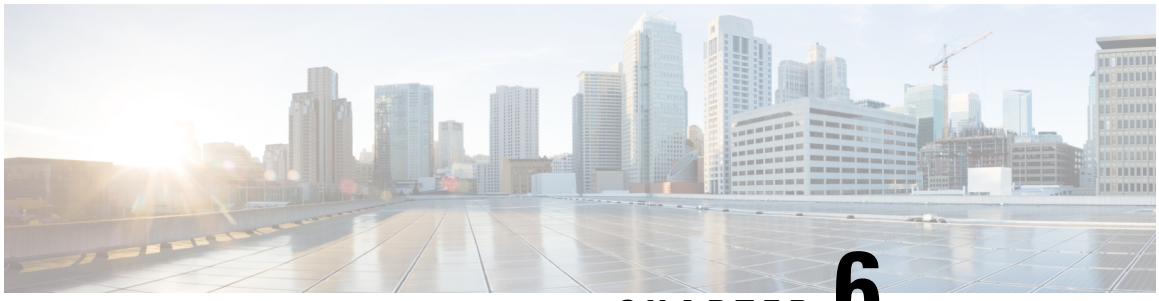
To ensure successful connection of an access point to the Cisco Mobility Express virtual controller or the Embedded Wireless Controller (EWC).

This guidance applies when a Cisco Mobility Express-enabled or EWC-enabled access point fails to establish a connection to the Cisco ISR 1000 Series Router's wireless controller.

The primary reason for this connectivity failure is the absence of an active DHCP server within the management VLAN that is assigned to the Wlan-GigabitEthernet interface. Without an IP address dynamically assigned by a DHCP server, the access point cannot communicate with the controller.

If a DHCP server is not configured in the appropriate VLAN, the access point will remain unable to connect to the wireless controller, thereby preventing wireless client connectivity through that access point.

- Configure a DHCP Server: Ensure a DHCP server is configured and active within the native VLAN of the WiFi module. This server must be capable of assigning IP addresses to the access points.
- Verify WLAN Module VLAN Configuration: Confirm that the management interface of the WLAN module is correctly assigned to a specific VLAN that has access to the DHCP server and other necessary network services (e.g., RADIUS).



CHAPTER 6

Cellular Gateway

Feature history for Cellular Gateway configuration

This table describes the developments of this feature, by release.

Table 39: Feature History

Feature Name	Release Information	Feature Description
Cellular Gateway Configuration	Cisco vManage Release 20.4.1 Cisco IOS XE Catalyst SD-WAN Release 17.4.1a (on devices)	This feature provides templates for configuring a supported cellular gateway as an IP pass-through device. This release supports the Cisco Cellular Gateway CG418-E and CG522-E.
Cellular Gateway Configuration Using a Configuration Group	Cisco Catalyst SD-WAN Manager Release 20.13.1 Cisco IOS CG Release 17.13.1	Added support for configuring cellular gateways using configuration groups. A new Create Cellular Gateway Group workflow creates a configuration group specifically for cellular gateways.

Cellular Gateways

A cellular gateway is a network device that

- provides wireless connectivity to a wide area network (WAN),
- functions as a bridge between cellular networks and enterprise LANs, and
- supports secure remote management and monitoring.

Secure Communication with Devices through a vmanage-admin Account

SD-WAN Manager communicates with devices, such as Cisco Catalyst Cellular Gateways, using a secure channel—either a datagram transport layer security (DTLS) tunnel or transport layer security (TLS) tunnel. Within this secure channel, it communicates with the devices or controllers using the NETCONF protocol, within an SSH session. It uses an internal-use-only passwordless "vmanage-admin" user account on the device or controller. The vmanage-admin account is created during the initial device setup. Cisco SD-WAN Manager uses this secure channel for monitoring, configuring, and managing devices.

As noted, the vmanage-admin user accounts do not have any password associated with them, so SD-WAN Manager uses a passwordless procedure to log in to the account. To accomplish this, SD-WAN Manager generates an asymmetric encryption public-private key pair. During deployment of a device, SD-WAN Manager copies the public key that it has generated to the device. It sends the public key using a proprietary protocol, within a secure channel—a DTLS or TLS tunnel.

The activity that SD-WAN Manager performs using the vmanage-admin account appears in syslog messages and in the output of certain show commands. The syslog messages are logged with the same level of detail as activities performed through any other user account. The level of syslog detail depends on the syslog configuration of the device.

Note SD-WAN Manager requires the vmanage-admin account on devices in order to monitor, configure, and manage the devices. Removing, disabling, or altering this account on a device would prevent Cisco SD-WAN Manager from performing these activities, and is not supported.

Supported Cellular Gateway devices

This sections provides information about the supported Cisco Catalyst Cellular Gateway models.

- CG418-E
- CG522-E

Configure a cellular gateway with a feature template

Configure a cellular gateway device using a feature template.

Use feature templates in SD-WAN Manager to standardize device configurations and enable efficient updates.

For information about using a configuration group, see Configure a Cellular Gateway using a Configuration Group in SD-WAN Manager, on page 129.

Follow these steps to configure a cellular gateway using a feature template.

Procedure

Step 1 Create a device template for Cisco Cellular Gateway CG418-E devices.

After you enter a description for the feature template, do this:

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**.

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

c) From the **Create Template** drop-down list choose **From Feature Template**.
d) From the **Device Model** drop-down list select the type of device for which you are creating the template.
e) Choose **Cellular Gateway** > **Cellular Gateway Platform** > **Create Template**. Then configure the Cellular Gateway Platform feature template as shown in this table.

Table 40: Cellular Gateway Platform Template Parameters

Parameter Name	Description
Basic Configuration Tab	
Time Zone	Choose the time zone to use for the device. The device uses this time zone for clock synchronization when NTP is configured.
Management Interface	Enter the IPv4 address of the management interface for accessing the device.
Admin-Password	Enter the admin user password for logging in to the device by using an SSH client or a console port.
NTP-Servers	Configure one or more NTP servers to which the device synchronizes its clock.
Cellular Configuration Tab	
IP-Src-Violation	Choose **v4 only**, **v6 only**, or **v4 and v6** to enable the IP source violation feature for the corresponding IP address types. Choose **None** if you do not want to enable this feature.
Auto-SIM	Choose **On** to enable the auto-SIM feature. When this feature is enabled, the device automatically detects the service provider to which SIMs in the device belong and automatically loads the appropriate firmware for that provider.
Primary SIM Slot	Choose the slot that contains the primary SIM card for the device. If the device loses service to this slot, it fails over to the secondary slot.
Failover-Timer (minutes)	Enter the number of minutes that the device waits before trying to communicate with the primary SIM slot after the device detects loss of service to this slot.
Max-Retry	Enter the number of consecutive unsuccessful attempts by the device to communicate with the primary SIM before failing over to the secondary slot

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

Table 41: Cellular Gateway Profile Template Parameters

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

Parameter Name	Description
Add	Click to add the profile your are configuring.
Advanced Configuration Tab	
Attach Profile	Choose the profile that the device uses to connect to the cellular network.
Cellular 1/1 Profile	Choose the profile that the device uses for data connectivity over the cellular network.

Step 2 Attach the device template to the device.

Configure a Cellular Gateway using a Configuration Group in SD-WAN Manager

Configure and manage cellular gateways using a configuration group in SD-WAN Manager.

Before you begin

Create a configuration group for Cisco Catalyst Cellular Gateways using **Workflows** > **Create Cellular Gateway Group**. On the **Configuration Groups** page, the resulting configuration group is labelled cellulargateway in the **Device Solution** column.

Follow these steps to configure a Cellular Gateway using a Configuration Group in SD-WAN Manager.

Procedure

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

Step 2 Click **…** adjacent to a configuration group for a Cellular Gateway and choose **Edit**.

- **AAA** feature:

Table 42: Local

Parameter Name	Description
Name	The account name is preset to **admin** and cannot be changed.
Password	Enter a password for login.

Table 43: TACACS

Parameter Name	Description
TACACS Configuration	Enable TACACS configuration. Click **Add TACACS** to add one or more TACACS servers.
Authentication	TACACS authentication option: • **tacacs_ascii**: Send authentication information in ASCII format. • **tacacs_pap**: Send authentication information using the password authentication protocol (PAP).
Timeout	Timeout for TACACS authentication. Range: 1 through 1000 seconds
TACACS	
IP Address	IP address of the TACACS server.
Auth Port	TCP port number to connect to the TACACS server. Default: 49
Secret Key	Encryption key for encrypting and decrypting traffic between the cellular gateway and the TACACS server. Configure the same key on the TACACS server.
Source Interface	Preconfigured as Cellular1/0, and cannot be changed. This is the only interface that the cellular gateway can use for communication with the TACACS server.
Priority	Priority level of the TACACS server. Zero is a default priority value and indicates the highest priority. If a cellular gateway is unable to establish a connection with the highest priority server, it attempts to connect to the server of the next highest priority. Range: 0 through 7

• **Cellular** feature:

Table 44: Cellular Settings

Parameter Name	Description
Primary Slot	Choose a SIM slot to designate it as primary. Range: 0, 1 Default: 0
SIM SLOT 0 Cellular Profile	

Parameter Name	Description
Profile Id	Profile ID. You can click **Add** to add multiple profiles.
Access Point Name	Access point name, from your service provider.
Authentication Method	Authentication method (**none**, **pap**, **chap**, **pap_or_chap**) indicated by your service provider.
Username	Username for authentication, as indicated by your service provider.
Password	Password for authentication, as indicated by your service provider.
Packet Data Network Type	Packet data network type (**IPv4**, **IPv6**, **IPv4v6**), as indicated by your service provider.
Attach Profile	Choose the attach profile from the defined profiles.
Data Profile	Choose the data profile from the defined profiles. You can use the same profile for the attach profile and data profile.
SIM SLOT 1 Cellular Profile	
See the fields described for SIM slot 0.	

- **Logging** feature:

Table 45: Disk

Parameter Name	Description
Disk File Rotate	Maximum number of log files to store locally. The device collects diagnostic monitor log files, which have a maximum size of 20 MB each, until the number of files reaches the rotate value. Then the device deletes the oldest file to make room for a new file. Range: 1 through 10
Disk File Size	Maximum file size for each log file that the device stores locally. After reaching the maximum size, the device creates a new log file, with a numerically sequenced filename. Range: 1 through 20 megabytes

Table 46: Servers

Parameter Name	Description
Server Name Type	Choose **ipv4** or **ipv6**, according to the server address type, or choose **dns** if you enter a server domain name in the **Server Name Value** field.
Server Name Value	IP address or domain name of the server.

Parameter Name	Description
Source IP	By default, this is the system IP address. You can choose the **Device Specific** option to specify per device.
Priority	Filter the type of log messages saved using one of the following priority options, listed from lowest to highest priority. Each priority option configures the device to save log messages of that priority and all higher priorities. For example, information is the lowest priority of message, so choosing **information** includes information log messages and all other log messages too. Choosing **error** excludes information, notice, and warn log messages, but includes error messages and all other log messages of higher priority (critical, alert, and emergency). From lowest to highest priority, the options are the following: • information • notice • warn • error • critical • alert • emergency

• **Network Protocol** feature:

Table 47: Basic Configuration

Parameter Name	Description
Passthrough	The cellular gateway operates in one of two modes: IP passthrough and NAT. In IP passthrough mode, the cellular gateway passes the public IP address assigned by the internet service provider (ISP) to a downstream device attached to the cellular gateway. Disabling the **Passthrough** option enables NAT, which gives the devices that are connected to the cellular gateway access to a DHCP server and to the local gateway. **Note** Enabling passthrough mode disables and hides the other fields in the **Basic Configuration** section.
DHCP Pool	
DHCP Pool	Enable a DHCP pool for NAT.

Parameter Name	Description
DHCP Network Pool	IP address pool, in classless interdomain routing (CIDR) format.
Lease Days	Days for DHCP lease time Range: 0 to 365
Lease Hours	Hours for DHCP lease time. Range: 0 to 23
Lease Minutes	Minutes for DHCP lease time. Range: 0 to 59
PAT Configuration	
PAT Configuration	Enable port address translation (PAT).
Add PAT Config	Click this to add one or more PAT configurations.
Description	Description of the PAT configuration.
Protocol	Choose **TCP** or **UDP**.
LocalAddress	IPv4 format address.
LocalPort	Port number. Range: 0 to 65535
InterfaceName	Preconfigured as Cellular1/0, which is the WAN interface for the cellular gateway.
GlobalPort	Global port number. Range: 1 to 65535

Table 48: NTP Servers

Parameter Name	Description
NTP	To configure a network time protocol (NTP) server, enter an IPv4 address or a DNS name. Maximum number of NTP servers: 4

Step 3 (Optional) To add CLI configuration commands, follow these steps:

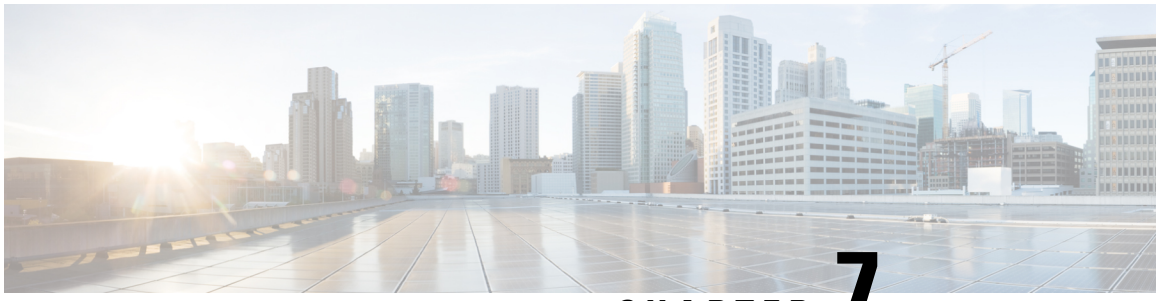
a) Open the **CLI Add-on Profile**.
b) Click **Add Feature**.
c) In the **Type** dropdown list, choose **Config**.
d) Enter a name for the feature.
e) Click **Save**.

Note

CLI configuration commands in the CLI Add-on Profile override any configuration done using the Global Profile.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.



CHAPTER 7

CLI Templates For Cisco IOS XE Catalyst SD-WAN Devices

CLI templates for Cisco IOS XE Catalyst SD-WAN devices

Table 49: Feature History Table

Feature Name	Release Information	Description
Device Configuration CLI Templates	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco vManage 20.1.1	The CLI Templates feature has been updated to support device configuration-based CLIs. You can use these templates to push the device configuration (yang-cli) to devices directly.
CLI Template for Cisco XE SD-WAN Routers	Cisco IOS XE Release 16.11.1a Cisco SD-WAN release 19.1	The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allow to you configure intent-based CLI templates for Cisco XE SD-WAN routers using Cisco SD-WAN Manager.
VRF Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Support for VRF configuration increased from a total of 100 to a total of 300 VRFs. Supported on: Cisco ASR 1001-HX and Cisco ASR 1002-HX

You can configure CLI templates for Cisco IOS XE Catalyst SD-WAN devices in the following ways:

- Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices
- Intent-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices

Note If you generate a CLI template in a higher version of Cisco SD-WAN Manager and then try to apply it in a lower version, it may not be supported depending on the configuration. In this case, Cisco SD-WAN Manager might also deny access and generate an error message. It is recommended that you use a CLI template generated in an earlier version of Cisco SD-WAN Manager. For example, if you are using Cisco vManage Release 20.7.x, you can use a CLI template generated in Cisco vManage Release 20.6.x and earlier releases.

Benefits of CLI templates

- You can reuse any Cisco vEdge-specific Cisco SD-WAN Manager feature templates for Cisco IOS XE Routers. When you create a device template using Cisco XE SDWAN Feature Templates, Cisco SD-WAN Manager displays the intent-based configuration (vEdge CLI syntax) and the corresponding device-based (Cisco XE SDWAN Routers) configuration. You can examine the intent-based configuration and repurpose that to create a separate CLI template for XE SDWAN routers.
- You can make multiple changes to a CLI template in a single edit.
- You can use a single configuration across multiple devices of the same device models. Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.
- You can define custom length for variables in CLI Templates.
- You can use any existing IOS-XE device intent configuration as input for CLI template.
- Content of a CLI template can be used across multiple IOS-XE device types (common CLIs like VPN, VPN interface, BGP, OSPF and so on).

Limitations of CLI templates

Auxiliary ports: When using a CLI template for Cisco Integrated Services Routers that have an auxiliary port, do not include commands for auxiliary ports, such as `line aux 0`. Doing so results in an error. These commands may be executed directly on the device.

When you import the CLI template configuration using the command, `show sdwan running-config`, you need to add quotes manually for the CLI template on the Cisco SD-WAN Manager.

From Cisco IOS XE Catalyst SD-WAN Release 17.12.x, policies configured using a Cisco Catalyst SD-WAN Controller template are ignored. To configure policies, navigate to **Configuration** > **Policies** > **Custom Options** > **CLI Policy**, add the policy and activate it for Cisco Catalyst SD-WAN Controller.

CLI templates in Cisco SD-WAN Manager

You can configure CLI templates in Cisco SD-WAN Manager using these two methods:

- Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices
- Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

A device configuration-based CLI Template for Cisco IOS XE Catalyst SD-WAN devices is a configuration management tool that:

- enables Cisco SD-WAN Manager (vManage 20.1.1 and later) to specify CLI templates using yang-cli,
- pushes only the difference between device and template configurations to Cisco IOS XE Catalyst SD-WAN devices, and
- provides a preview of configuration changes before deployment.

These templates are used alongside feature templates and policies, including localized and security policies, in Cisco SD-WAN Manager.

Note To configure features not accessible using Cisco SD-WAN Manager, we recommend doing the following:

1. Use the relevant feature template in addition to a CLI add-on feature template.
2. For situations where the previous option is not sufficient, use the device configuration-based CLI templates as described in this section.

Configure device configuration-based CLI templates

Procedure

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

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

Step 2 From the **Create Template** drop-down list, select **CLI Template**.

Step 3 From the **Device Model** drop-down list, select the type of device for which you are creating the template.

Step 4 In the **Template Name** and **Template Description**, enter a name upto 128 alphanumeric characters and a description upto 2048 alphanumeric characters.

Step 5 Choose **Device configuration**. Using this option, you can provide IOS-XE configuration commands that appear in the output of the `show sdwan running-config` command.

(Optional) To load the running config of a connected device, select it from the Load Running config from reachable device list and click **Search**.

Step 6 In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

Step 7 To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**.

You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{*hostname*}}.

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

Step 8 Click **Add** to save the feature template.

The new device template is displayed in the Device Template table.

Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

An intent-based CLI Template for Cisco IOS XE Catalyst SD-WAN devices is a configuration management tool that:

- allows Cisco SD-WAN Manager to configure CLI templates using intent-based commands,
- supports vEdge device syntax for command input, and
- pushes vEdge syntax-based commands to Cisco IOS XE Catalyst SD-WAN devices in IOS XE syntax.

Intent-based CLI templates enable configuration of Cisco IOS XE Catalyst SD-WAN devices using vEdge syntax via Cisco SD-WAN Manager.

With the support of device configuration-based CLI templates, the intent-based CLI templates will be deprecated. We recommend using the device configuration-based CLI templates as described in Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices.

Using Cisco SD-WAN Manager CLI templates significantly reduces the effort to configure feature templates.

Configure intent-based CLI templates

Procedure

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

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

Step 2 From the **Create Template** drop-down list, select **CLI Template**.

Step 3 From the **Device Model** drop-down list, select the type of device for which you are creating the template.

Step 4 In the **Template Name** and **Template Description**, enter a name upto 128 alphanumeric characters and a description upto 2048 alphanumeric characters.

Step 5 The configuration of the CLI template can either be intent-based or based on the device configuration:

- **Intent**: If you specify **Intent**, you specify commands in the Cisco vEdge format. If the device you've selected is a Cisco IOS XE Catalyst SD-WAN device, Cisco SD-WAN Manager converts the configuration for the device.
- **Device configuration**: This option is available from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and onwards and only for Cisco IOS XE Catalyst SD-WAN devices. For this option, you must specify the entire device configuration as it appears in `show sd-wan running config`.

Note
You can only use this feature with the qualified CLIs described in the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.

Example:

You can upload a configuration file using **Select a File** or copy and paste the CLI configuration. Following is an example of an intent-based CLI with variables.

```
system

   host-name {{hostname}}
   system-ip {{system_ip}}
   domain-id 1

   site-id {{site_id}}
   port-offset           1
   admin-tech-on-failure
   organization-name "XYZ"
   logging
    disk
     enable
! !
```

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

Step 6 To save the feature template, click **Add**.

What to do next

Sample configurations for CLI templates

System level configuration

Table 50: System level parameters

CLI Template Configuration	Configuration on the Device
system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name "XYZ Inc Regression" organization-name "XYZ Regression" console-baud-rate 115200 vbond 10.0.12.26 port 12346	system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name “XYZ Inc Regression” organization-name “XYZ Inc Regression” console-baud-rate 11520 vbond 10.0.12.26 port 12346

AAA Configuration - authentication, authorization, and accounting (AAA) with RADIUS and TACACS+

Table 51: AAA configuration

CLI Template Configuration	Configuration on the Device

aaa
 auth- order local radius tacacs
 usergroup basic
  task system read write
 task interface read write
!
usergroup netadmin
!
 usergroup operator
task system read
task interface read
task policy read
task routing read
task security read
!
user admin password
 	
6nbbLkA==$ae/DO78l/wluPUohhBU2L6h/
Q.PLkurGvxjRlS9OWB9iTtFwSGNQcABV6F
MW57vuEHvo3zp3qdYVinLmMIu/p/
secret
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
 	
! !
radius
 server 10.99.144.200
  source-interface GigabitEthernet0/0/1
 exit
 server 10.99.144.201
 	
  source-interface GigabitEthernet0/1/0
 exit
!
tacacs
 server 10.0.1.1
  auth-port 50
  vpn 0
  source-interface GigabitEthernet0/0/1
  key 1
  secret-key
8Kcuva0CM871E8czESwV5g/YX4Q8pY1LSNk/+PIDrpCg=
 	
 exit !
!
	aaa group server tacacs+ server-10.0.1.1
	  server-private 10.0.1.1 timeout 5 key
	8vs5hzVg/Z6EeuUdNHTzOwWPsUv9V/50xmcRfShWp3YI=
	
	 ip tacacs source-interface
	GigabitEthernet0/0/1
	!
	aaa group server radius server-10.99.144.200
	 server-private 10.99.144.200 auth-port 1812
	 timeout 5 retransmit 3
	 ip radius source-interface
	GigabitEthernet0/0/1
	!
	aaa group server radius server-10.99.144.201
	
	 server-private 10.99.144.201 auth-port 1812
	 timeout 5 retransmit 3
	 ip radius source-interface
	GigabitEthernet0/1/0
	!
	aaa authentication login default local group
	 radius group tacacs+
	aaa authorization exec default local group
	radius group tacacs+ a
	aa session-id common --- added by default
	
	username admin privilege 15 secret 9
	$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c

Logging configuration - configures logging to either the local hard drive or a remote host

Table 52: Logging configuration

CLI Template Configuration	Configuration on the Device
logging disk enable file size 12 file rotate 6 ! server 192.168.13.1 vpn 0 source-interface Loopback1 priority alert exit !	logging disk enable ! ! logging persistent size 75497472 filesize 12582912 logging buffered 512000 --- added by default logging host 192.168.13.1 no logging rate-limit logging source-interface Loopback1 logging persistent

Switch port and VLAN configuration

Table 53: Switch port configuration

CLI Template Configuration	Configuration on the Device
interface GigabitEthernet0/1/4 switchport mode trunk access vlan vlan 10 access vlan name "DHCP Vlan" trunk allowed vlan 10 ! no shutdown vpn 10 name "DHCP VPN" interface Vlan10 description "Vlan 10 Mgmt interface" ip address 10.29.35.1/24 no shutdown ! !	interface GigabitEthernet0/1/4 switchport ios-sw:mode trunk switchport ios-sw:trunk allowed vlan 10 no shutdown no ip address exit interface Vlan10 description Vlan 10 Mgmt interface no shutdown arp timeout 1200 vrf forwarding 10 ip address 10.29.35.1 255.255.255.0 ip mtu 1500 exit

Cellular configuration

Table 54: Cellular configuration - configures cellular controllers and cellular interfaces

CLI Template Configuration	Configuration on the Device

vpn 0
  interface Cellular0/2/0
  description "Cellular interface"
  no shutdown
  !
 	
  controller cellular 0/2/0
  lte sim max-retry 1
  lte failovertimer 7
  profile id 1 apn Broadband
  !
	interface Cellular0/2/0
	  description Cellular interface
	  no shutdown
	  ip address negotiated
	  ip mtu 1428
	  mtu 1500
	  exit
	
	  controller Cellular 0/2/0
	  lte sim max-retry 1
	  lte failovertimer 7
	  profile id 1 apn Broadband authentication
	  none pdn-type ipv4

BGP, OSPF, and EIGRP - configures BGP, OSPF, and EIGRP routing protocols under transport or service VPN

Table 55: BGP, OSPF, and EIGRP configuration

CLI Template Configuration	Configuration on the Device

CLI Template Configuration	Configuration on the Device

vpn1
  bgp 2
  shutdown
  distance external 30
  distance internal 250
  distance local 10
  address-family ipv4-unicast
  network 10.0.100.0/24
  redistribute static route-policy route_map
  redistribute connected route-policy route_map
  !
  neighbor 10.0.100.1
  no shutdown
  remote-as 3
  timers
  keepalive 12
  holdtime 20
  connect-retry 300
  advertisement-interval 123
  !
  update-source GigabitEthernet0/0/1
  ebgp-multihop 1
  password $8$9pou4PH9b60B072hcw3MmSSdLCfJk8bVys12lLVb+08=
 	
  address-family ipv4-unicast
 	
vpn 1
  router
  ospf
  router-id 172.16.255.15
  compatible rfc1583
  timers spf 200 1000 10000
  redistribute connected route-policy route_map
  max-metric router-lsa administrative
  area 23
  stub
  interface GigabitEthernet0/0/1
  cost 23
  authentication type message-digest
  authentication authentication-key key1
 	
  exit
  exit
  !
 	
vpn 1
router
  eigrp 1
  af-interface GigabitEthernet0/0/2
  no split-horizon
  exit-af-interface
  !
address-family ipv4 network 10.1.10.1/32
address-family ipv4 topology base
redistribute omp
exit-af-topology	

CLI Template Configuration	Configuration on the Device
	router bgp 2 bgp log-neighbor-changes distance bgp 30 250 10 address-family ipv4 unicast vrf 1 neighbor 10.0.100.1 remote-as 3 neighbor 10.0.100.1 activate neighbor 10.0.100.1 ebgp-multihop 1 neighbor 10.0.100.1 maximum-prefix 2147483647 100 neighbor 10.0.100.1 password 0 password neighbor 10.0.100.1 send-community both neighbor 10.0.100.1 timers 12 20 neighbor 10.0.100.1 update-source GigabitEthernet0/0/1 network 10.0.100.0 mask 255.255.255.0 redistribute connected redistribute static route-map route_map exit-address-family ! timers bgp 60 180 router ospf 1 vrf 1 auto-cost reference-bandwidth 100 max-metric router-lsa timers throttle spf 200 1000 10000 router-id 172.16.255.15 default-information originate distance ospf external 110 distance ospf inter-area 110 distance ospf intra-area 110 redistribute connected subnets route-map route_map ! interface GigabitEthernet0/0/1 no shutdown arp timeout 1200 vrf forwarding 1 ip address 10.1.100.14 255.255.255.0 ip redirects ip mtu 1500 ip ospf 1 area 23 ip ospf network broadcast mtu 1500 negotiation auto exit ! router eigrp eigrp-name address-family ipv4 vrf 1 autonomous-system 1 af-interface GigabitEthernet0/0/2 hello-interval 5 hold-time 15 no split-horizon exit-af-interface ! network 10.1.10.1 0.0.0.0 topology base redistribute omp exit-af-topology ! exit-address-family

CLI Template Configuration	Configuration on the Device
	! !

VPN, Interface, and tunnel configuration for WAN and LAN interfaces

Table 56: VPN, Interface, and Tunnel configuration

CLI Template Configuration	Configuration on the Device

vpn 0
  interface GigabitEthernet0/2/0
  ip address 10.1.14.14/24
  tunnel-interface
  encapsulation ipsec
  color lte
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  !
  autonegotiate
  no shutdown
  !
  ip route 0.0.0.0/0 10.1.14.13
 	
vpn 512
interface GigabitEthernet0
  ip dhcp-client
ipv6 dhcp-client autonegotiate
no shutdown
! !
	ip route 0.0.0.0 0.0.0.0 10.1.14.13 1
	
	interface GigabitEthernet0/2/0
	  no shutdown
	  arp timeout 1200 – added by default
	  ip address 10.1.14.14 255.255.255.0
	  ip redirects --> added by default
	  ip mtu 1500
	  mtu 1500
	  negotiation auto --> added by default
	  exit
	
	interface Tunnel20 ---> based on the interface 0/2/0
	  no shutdown
	  ip unnumbered GigabitEthernet0/2/0
	  no ip redirects
	  ipv6 unnumbered GigabitEthernet0/2/0
	  no ipv6 redirects
	  tunnel source GigabitEthernet0/2/0
	  tunnel mode sdwan
	
	sdwan
	  interface GigabitEthernet0/2/0
	  tunnel-interface
	  encapsulation ipsec weight 1
	  color lte
	  no last-resort-circuit
	  vmanage-connection-preference 5
	  no allow-service all
	  no allow-service bgp
	  allow-service dhcp
	  allow-service dns
	  allow-service icmp
	  no allow-service sshd
	  no allow-service netconf
	  no allow-service ntp
	  no allow-service ospf
	  no allow-service stun
	
	interface GigabitEthernet0
	no shutdown
	arp timeout 1200
	vrf forwarding Mgmt-intf
	ip address dhcp client-id GigabitEthernet0 ip redirects
	ip dhcp client default-router distance 1 ip
	mtu 1500
	mtu 1500
	negotiation auto

Network Address Translation (NAT) over Direct Internet Access (DIA)

Table 57: NAT over DIA

CLI Template Configuration	Configuration on the Device
vpn 201 interface GigabitEthernet0/0/2.2901 description gigi21 ip address 10.201.201.1/24 mtu 1496 no shutdown vrrp 100 track-omp ipv4 10.201.201.3 ! ! ! dhcp-server address-pool 10.201.201.0/24 exclude 10.201.201.1-10.201.201.10 10.201.201.20-10.201.201.22 offer-time 600 lease-time 86400 admin-state up options default-gateway 10.201.201.1 dns-servers 10.99.139.201 tftp-servers 10.99.139.201 ! ! ! ip route 0.0.0.0/0 vpn 0 ! vpn 0 interface GigabitEthernet0/0/0 ip address 172.16.10.1/24 nat udp-timeout 3 tcp-timeout 40 respond-to-ping ! !	interface GigabitEthernet0/0/2.2901 no shutdown encapsulation dot1Q 2901 vrf forwarding 201 ip address 10.201.201.1 255.255.255.0 ip mtu 1496 vrrp 100 address-family ipv4 vrrpv2 address 10.201.201.3 priority 100 track omp shutdown exit exit ip dhcp excluded-address vrf 201 10.201.201.1 10.201.201.10 ip dhcp excluded-address vrf 201 10.201.201.20 10.201.201.22 ip dhcp pool vrf-201-GigabitEthernet0/0/2.2901 option 150 ip 10.99.139.201 vrf 201 lease 1 0 0 default-router 10.201.201.1 dns-server 10.99.139.201 network 10.201.201.0 255.255.255.0 exit ip dhcp use hardware-address client-id no ip dhcp use class ip dhcp use vrf remote ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload ip nat translation tcp-timeout 40 ip nat translation udp-timeout 3 ip nat route vrf 201 0.0.0.0 0.0.0.0 global interface GigabitEthernet1/0/2 no shutdown arp timeout 1200 ip address 10.1.15.15 255.255.255.0 ip nat outside ip redirects ip mtu 1500 mtu 1500 negotiation auto

NAT64 configuration

Table 58: NAT64 configuration

CLI Template Configuration	Configuration on the Device

vpn 1
  nat64
  v4 pool pool1 start-address 10.1.1.10
  v4 pool pool1 end-address 10.1.1.100
  !
  interface GigabitEthernet3
  ip address 10.1.19.15/24
  nat64
  !
  autonegotiate
  no shutdown
  !
	interface GigabitEthernet3
	  no shutdown
	  arp timeout 1200
	  vrf forwarding 1
	  ip address 10.1.19.15 255.255.255.0
	  negotiation auto
	  nat64 enable
	  nat64 prefix stateful 2001::F/64 vrf 1
	
	  nat64 v4 pool pool1 10.1.1.10 10.1.1.100
	  nat64 v6v4 list global-list pool pool1 vrf
	1
	  nat64 translation timeout tcp 60
	  nat64 translation timeout udp 1

Multilink and T1/E1 - configures T1/E1 controller and serial, multilink interfaces

Table 59: Configuring Multilink

CLI Template Configuration	Configuration on the Device

card type t1 0 2
  controller T1 0/2/0
  framing esf
  clock source internal
  linecode b8zs
  cablelength long 0db
  channel-group 1 timeslots 15
  channel-group 2 timeslots 12
  channel-group 3 timeslots 10
  channel-group 4 timeslots 10
!
interface Multilink1
  no shutdown
  encapsulation ppp
  ip address 10.1.10.30 255.255.255.0
  ppp pap sent-username admin password admin
ppp authentication pap
  ppp multilink
  ppp multilink links minimum 1
  ppp multilink fragment disable
  ppp multilink group 1
exit
interface Serial0/2/0:1
  no shutdown
  encapsulation ppp
  bandwidth 1536
  no ip address
  load-interval 30
  ppp pap sent-username admin password admin
ppp authentication pap
  ppp multilink
  ppp multilink group 1
exit
	interface Multilink1
	ip address 10.1.10.30/24 shutdown
	controller T1 0/2/0
	  linecode b8zs
	  channel-group 1
	  channel-group 3
	!
	ppp pap sent-username admin password admin
	ppp authentication pap
	ppp multilink
	ppp multilink group 1

Local QoS policy

Table 60: Local QoS policy

CLI Template Configuration	Configuration on the Device

CLI Template Configuration	Configuration on the Device

vpn 1
  interface GigabitEthernet0/0/1
  ip address 10.2.54.15/24
  no shutdown
  access-list MyACL in
  !
policy
  class-map
  class best-effort queue 3
  class bulk-data queue 2
  class critical-data queue 1
  class voice queue 0
  !
  access-list MyACL
  sequence 10
  match
  dscp 46
  !
  action accept
  class voice
  !
  !
  sequence 20
  match
  source-ip 10.1.1.0/24
  destination-ip 192.168.10.0/24
  !
  action accept
  class bulk-data
  set
  dscp 32
  !
  !
  !
  sequence 30
  match
  destination-ip 192.168.20.0/24
  !
  action accept
  class critical-data
  set
  dscp 22
  !
  !
  !
  sequence 40
  action accept
  class best-effort
  set
  dscp 0
  !
  !
  !
  default-action accept
  !
  qos-scheduler be-scheduler
  class best-effort
  bandwidth-percent 20
  buffer-percent 20
  drops red-drop
  !
  qos-scheduler bulk-scheduler
	interface GigabitEthernet0/0/1
	  access-list MyACL in
	  exit
	  class-map match-any best-effort
	  match qos-group 3
	  !
	  class-map match-any bulk-data
	  match qos-group 2
	  !
	  class-map match-any critical-data
	  match qos-group 1
	  !
	  class-map match-any voice
	  match qos-group 0
	  !
	  policy-map MyQoSMap
	  class best-effort
	  random-detect
	  bandwidth percent 20
	  !
	  class bulk-data
	  random-detect
	  bandwidth percent 20
	  !
	  class critical-data
	  random-detect
	  bandwidth percent 40
	  !
	  class voice
	  priority percent 20
	  !
	  !
	  policy
	  no app-visibility
	  no flow-visibility
	  no implicit-acl-logging
	  log-frequency 1000
	  class-map
	  class best-effort queue 3
	  class bulk-data queue 2
	  class critical-data queue 1
	  class voice queue 0
	  !
	  access-list MyACL
	  sequence 10
	  match
	  dscp 46
	  !
	  action accept
	  class voice
	  !
	  !
	  sequence 20
	  match
	  source-ip 10.1.1.0/24
	  destination-ip 192.168.10.0/24
	  !
	  action accept
	  class bulk-data
	  set
	  dscp 32
	  !

CLI Template Configuration	Configuration on the Device
class bulk-data bandwidth-percent 20 buffer-percent 20 drops red-drop ! qos-scheduler critical-scheduler class critical-data bandwidth-percent 40 buffer-percent 40 drops red-drop ! qos-scheduler voice-scheduler class voice bandwidth-percent 20 buffer-percent 20 scheduling llq ! qos-map MyQoSMap qos-scheduler be-scheduler qos-scheduler bulk-scheduler qos-scheduler critical-scheduler qos-scheduler voice-scheduler ! ! ! !	! ! sequence 30 match destination-ip 192.168.20.0/24 ! action accept class critical-data set dscp 22 ! ! ! sequence 40 action accept class best-effort set dscp 0 ! ! ! default-action accept ! ! ! !

Security policy (ZBFW, IPS/IDS, URL-Filtering) configuration

Table 61: Security policy (ZBFW, IPS/IDS, URL-Filtering)

CLI Template Configuration	Configuration on the Device
policy zone internet vpn 0 ! zone zone1 vpn 1 ! zone zone2 vpn 2 ! zone-pair ZP_zone1_internet_fw_policy source-zone zone1 destination-zone internet zone-policy fw_policy ! zone-pair ZP_zone1_zone2_fw_policy source-zone zone1 destination-zone zone2 zone-policy fw_policy ! zone-based-policy fw_policy sequence 1 match source-data-prefix-list subnet1 ! action inspect ! ! default-action pass ! zone-to-nozone-internet deny lists data-prefix-list subnet1 ip-prefix 10.0.10.0/24 ! ! url-filtering url_filter web-category-action block web-categories games block-threshold moderate-risk block text "<![CDATA[<h3>Access" to the requested page has been denied]]>" target-vpns 1 ! intrusion-prevention intrusion_policy security-level connectivity inspection-mode protection log-level err target-vpns 1 ! failure-mode open ! ! !	

CLI Template Configuration	Configuration on the Device
	ip access-list extended fw_policy-seq-1-acl_ 11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl 10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_ match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy class fw_policy-seq-1-cm_ inspect ! class class-default pass ! ! object-group service fw_policy-seq-1-service-og_ ip ! parameter-map type inspect-global alert on log dropped-packets multi-tenancy vpn zone security ! parameter-map type umbrella global token A5EA676087BF66A42DC4F722C2AFD10D00256274 dnscrypt vrf 1 dns-resolver umbrella match-local-domain-to-bypass ! ! zone security internet vpn 0 ! zone security zone1 vpn 1 ! zone security zone2 vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2 service-policy type inspect fw_policy ! app-hosting appid utd app-resource package-profile cloud-low app-vnic gateway0 virtualportgroup 0 guest-interface 0

CLI Template Configuration	Configuration on the Device
	guest-ipaddress 192.168.1.2 netmask 255.255.255.252 ! app-vnic gateway1 virtualportgroup 1 guest-interface 1 guest-ipaddress 192.0.2.2 netmask 255.255.255.252 ! start ! utd multi-tenancy utd engine standard multi-tenancy web-filter block page profile block-url_filter text <\![CDATA[Access to the requested page has been denied Please contact your Network Administrator]]> ! web-filter url profile url_filter categories block games ! block page-profile block-url_filter log level error reputation block-threshold moderate-risk ! ! threat-inspection profile intrusion_policy threat protection policy connectivity logging level err ! utd global ! policy utd-policy-vrf-1 all-interfaces vrf 1 threat-inspection profile intrusion_policy web-filter url profile url_filter exit !

Configuring NTP

Table 62: Configuring NTP

CLI Template Configuration	Configuration on the Device
ntp server 10.29.43.1 source-interface GigabitEthernet1 version 4 exit ! !	ntp server 198.51.241.229 source GigabitEthernet1 version 4

IPv6 configuration

Table 63: IPv6 configuration

CLI Template Configuration	Configuration on the Device
vpn 1 interface GigabitEthernet3 ipv6 address 2671:123A::1/128 shutdown ! !	interface GigabitEthernet3 shutdown arp timeout 1200 vrf forwarding 1 no ip address ip redirects ip mtu 1500 ipv6 address 2671:123A::1/128 ipv6 redirects mtu 1500 negotiation auto exit vrf definition 1 rd 1:1 address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! !

Service configuration

In Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and earlier, only the following configurations under **service** can be configured via CLI templates:

```
service pad
service config
service tcp-keepalives-in
service tcp-keepalives-out
service tcp-small-servers
service udp-small-servers
```

VRF configuration

Configure up to 300 VRFs, with a corresponding subinterface for each VRF. The example configures two VRFs.

Warning Do not configure VLAN 1. It is reserved for the native VLAN.

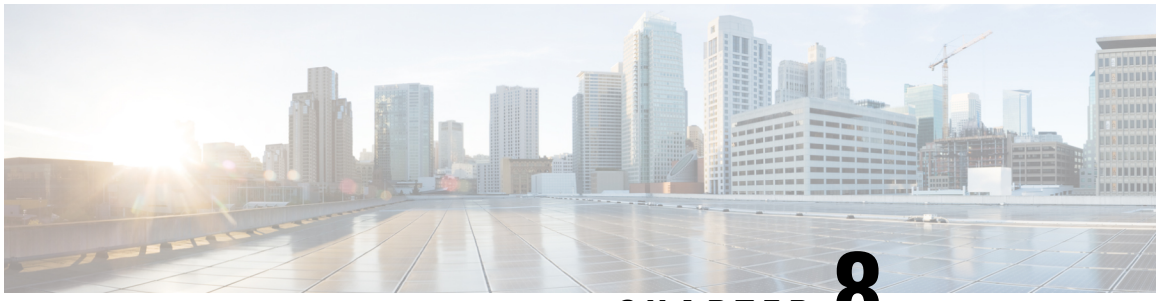
Table 64: VRF configuration

CLI Template Configuration	Configuration on the Device
! vpn 2 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.2.2 no shutdown remote-as 2 ! ipv6-neighbor 2001:DB8:2::2 remote-as 2 ! ! interface GigabitEthernet0/0/0.2 ip address 192.0.2.1/24 ipv6 address 2001: DB8:2::1/64 mtu 1496 no shutdown ! ! vpn 3 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.3.2 no shutdown remote-as 3 ! ipv6-neighbor 2001: DB8:3::2 remote-as 3 ! ! interface GigabitEthernet0/0/0.3 ip address 192.0.3.1/24 ipv6 address 2001: DB8:3::1/64 mtu 1496 no shutdown !	

CLI Template Configuration	Configuration on the Device

	vrf definition 2
	rd 1:2
	address-family ipv4
	  route-target export 1000:2
	  route-target import 1000:2
	  exit-address-family
	!
	address-family ipv6
	  exit-address-family
	!
	!
	router bgp 1000
	bgp log-neighbor-changes
	distance bgp 20 200 20
	!
	address-family ipv4 vrf 2
	  redistribute omp
	  neighbor 192.0.2.2 remote-as 2
	  neighbor 192.0.2.2 activate
	  neighbor 192.0.2.2 send-community both
	exit-address-family
	!
	address-family ipv6 vrf 2
	  redistribute omp
	  neighbor 2001:DB8:2::2 remote-as 2
	  neighbor 2001: DB8:2::2 activate
	  neighbor 2001: DB8:2::2 send-community both
	exit-address-family
	!
	interface GigabitEthernet0/0/0.2
	encapsulation dot1Q 2
	vrf forwarding 2
	ip address 192.0.2.1 255.255.255.0
	ip mtu 1496
	ipv6 address 2001:DB8:2::1/64
	end
	
	vrf definition 3
	rd 1:3
	address-family ipv4
	  route-target export 1000:3
	  route-target import 1000:3
	  exit-address-family
	!
	address-family ipv6
	  exit-address-family
	!
	!
	router bgp 1000
	bgp log-neighbor-changes
	distance bgp 20 200 20
	!
	address-family ipv4 vrf 3
	  redistribute omp
	  neighbor 192.0.3.2 remote-as 3
	  neighbor 192.0.3.2 activate
	  neighbor 192.0.3.2 send-community both
	exit-address-family
	!
	address-family ipv6 vrf 3
	  redistribute omp
	  neighbor 2001:DB8:3::2 remote-as 3

CLI Template Configuration	Configuration on the Device
	neighbor 2001: DB8:3::2 activate neighbor 2001: DB8:3::2 send-community both exit-address-family ! interface GigabitEthernet0/0/0.3 encapsulation dot1Q 3 vrf forwarding 3 ip address 192.0.3.1 255.255.255.0 ip mtu 1496 ipv6 address 2001:DB8:3::1/64 end



CHAPTER 8

CLI Add-On Feature Templates

Feature history for CLI add-on feature templates

Table 65: Feature History Table

Feature Name	Release Information	Description
CLI Add-On Feature Templates	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco vManage 20.1.1	This feature adds a new feature template called the CLI add-on feature template. You can use this feature template to attach specific CLI configurations to a device. If a configuration cannot be specified using Cisco SD-WAN Manager but can be configured using the CLI on the device, then you can use this feature template to specify such configurations. You can also use CLI add-on feature templates to add small pieces of CLI configuration, instead of an entire running configuration. This feature is not intended to replace existing feature templates but instead to enhance their functionality. Note that not all CLIs are qualified. For more information, see Qualified CLIs for Cisco IOS XE Release 17.2.1r.

Feature Name	Release Information	Description
Additional Commands Qualified for CLI Add-On Feature Templates	Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x Cisco SD-WAN Release 20.1.12	With each release, we qualify commands for use with the CLI add-on feature templates feature. In this release, we qualified additional commands. See the Appendix in the Cisco IOS XE SD-WAN Qualified Command Reference Guide.

CLI add-on feature templates for Cisco SD-WAN

The CLI add-on feature template is a template that:

- Allows you to add custom device commands not available in standard feature templates.
- Gives the commands in it priority over those present in the feature templates during merges.

When you specify commands using the template, always use the commands as per the syntax displayed in the **show sdwan running-config** output.

For example, for Cisco AAA, the `attempts login` command is not available in Cisco SD-WAN Manager.

By using a CLI add-on feature template, you can specify the `aaa authentication attempts login number` command for a device.

After you create the feature template, ensure that you add it to the device template.

You must define the CLI add-on feature template before you use it in a device template.

Restrictions for add-on feature templates

The CLI add-on feature templates:

- Are supported only on devices running Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later.
- Allow only one CLI add-on template per device template.
- Require verification of each command by logging in and running it on the intended device before adding it to the CLI add-on feature template.
- Include only supported commands. Using unsupported commands cause errors and configuration failures.

  For example, "`login local`" is not supported.

Create a CLI add-on feature template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates** > **Add Template** to select an appropriate device model.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

Step 2 From **Select Devices**, select the devices for which you are creating the template.

Step 3 From **Select Template**, scroll down to the **OTHER TEMPLATES** section.

Step 4 Click **CLI Add-On Template**.

Step 5 In the mandatory **Template Name** field, enter a name for the feature template; In the mandatory **Description** field, enter a description for the device template.

This **Template Name** field can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It does not support spaces or any other characters. The **Description** field can only contain any characters and spaces.

Step 6 In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

Step 7 To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable.** You can also type the variable name directly, in the format `{{variable-name}}`.

Step 8 Click **Save**. The new feature template is displayed in the **Feature Template** table.

Step 9 To use the CLI add-on feature template, edit the device template as follows:

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

b) Click **Device Templates**.

In Cisco SD-WAN Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

Qualified CLI commands for CLI add-on feature templates

For a release-wise list of CLI commands that are qualified for use in SD-WAN Manager CLI templates, see the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.