Cisco Catalyst SD-WAN Basic System Overview

Cisco Catalyst SD-WAN Basic System Overview

Table 1: Feature History

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

System and Interfaces Overview

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

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

Host Properties

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

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

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

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

Time and NTP

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

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

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

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

Authorization determines whether a user is authorized to perform a given activity on a device. In the Cisco Catalyst SD-WAN software, authorization is implemented using role-based access. Access is based on groups that are configured on the devices. A user can be a member of one or more groups. User-defined groups are considered when performing authorization, that is, the Cisco Catalyst SD-WAN software uses group names

received from RADIUS or TACACS+ servers to check the authorization level of a user. Each group is assigned privileges that authorize the group members to perform specific functions on the corresponding device. These privileges correspond to specific hierarchies of the configuration commands and the corresponding hierarchies of operational commands that members of the group are allowed to view or modify.

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

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

Authentication for WANs and WLANs

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

IEEE 802.1X authentication requires three components:

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

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

Network Segmentation

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

Network Interfaces

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

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

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

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

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

Management and Monitoring Options

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

The following management interfaces are available:

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

CLI

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

up and configuring overlay network devices, including bulk operations for setting up multiple devices simultaneously.

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

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

IPFIX

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

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

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

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

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

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

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

RESTful API

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

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

SNMP

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

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

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

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

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

Syslog Messages

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

Cisco SD-WAN Manager

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

Basic Settings for Cisco SD-WAN Manager

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

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

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

Configure Organization Name

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

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

To configure the organization name:

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

Note technology-guides

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

Configure Cisco SD-WAN Validator DNS Name or IP Address

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

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

Configure Controller Certificate Authorization Settings

Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the Cisco SD-WAN Manager that you generate these certificates and install them on the controller devices—Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers. You can use certificates signed by Symantec, or you can use enterprise root certificates.

The controller certification authorization settings establish how the certification generation for all controller devices will be done. They do not generate the certificates.

You need to select the certificate-generation method only once. The method you select is automatically used each time you add a device to the overlay network.

To have the Symantec signing server automatically generate, sign, and install certificates on each controller device:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Symantec Automated** (Recommended). This is the recommended method for handling controller signed certificates.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to confirm that you wish to have the Symantec signing server automatically generate, sign, and install certificates on each controller device.
4. Enter the first and last name of the requester of the certificate.

5. Enter the email address of the requester of the certificate. This address is required because the signed certificate and a confirmation email are sent to the requester via email; they are also made available though the customer portal.
6. Specify the validity period for the certificate. It can be 1, 2, or 3 years.
7. Enter a challenge phrase. The challenge phrase is your certificate password and is required when you renew or revoke a certificate.
8. Confirm your challenge phrase.
9. In **Certificate Retrieve Interval**, specify how often the Cisco SD-WAN Manager server checks if the Symantec signing server has sent the certificate.
10. Click **Save**.

To manually install certificates that the Symantec signing server has generated and signed:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Symantec Manual**.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to manually install certificates that the Symantec signing server has generated and signed.
4. Click **Save**.

To use enterprise root certificates:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Enterprise Root Certificate**.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to confirm that you wish to use enterprise root certificates.
4. In the **Certificate** box, either paste the certificate, or click **Select a file** and upload a file that contains the enterprise root certificate.
5. By default, the enterprise root certificate has the following properties: To view this information, issue the **show certificate signing-request decoded** command on a controller device, and check the output in the Subject line. For example:
   - Country: United States
   - State: California
   - City: San Jose
   - Organizational unit: ENB
   - Organization: CISCO
   - Domain Name: cisco.com
   - Email: cisco-cloudops-sdwan@cisco.com

```
vSmart# show certificate signing-request decoded
    ...
    Subject: C=US, ST=California, L=San Jose, OU=ENB, O=CISCO, CN=vsmart-uuid
```

```
.cisco.com/emailAddress=cisco-cloudops-sdwan@cisco.com
    ...
```

To change one or more of the default CSR properties:

a. Click **Set CSR Properties**.

b. Enter the domain name to include in the CSR. This domain name is appended to the certificate number (CN).

c. Enter the organizational unit (OU) to include in the CSR.

d. Enter the organization (O) to include in the CSR.

e. Enter the city (L), state (ST), and two-letter country code (C) to include in the CSR.

f. Enter the email address (emailAddress) of the certificate requester.

g. Specify the validity period for the certificate. It can be 1, 2, or 3 years.

6. Click **Import & Save**.

Enforce Software Version on Devices

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

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

- The bootflash and flash on the router must have enough free space to support the upgrade
- The version of the SD-WAN image that is on the device before the upgrade must be a lower version than the enforced SD-WAN version you specify in the following procedure

To enforce a version of the Cisco Catalyst SD-WAN software to run on a router when it first joins the overlay network, follow these steps:

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

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

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

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

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

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

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

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

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

(In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, locate **Enforce Software Version (ZTP)** and click **Edit**.)

4. For a specific platform, enable enforcing the software version.
5. Do one of the following:
   - Use an image on a local server:
     a. In the **Image Location** field, choose **Local Server**.
     b. In the **Version/Image Name** field, choose an image.
   - Use an image on a remote server:
     a. In the **Image Location** field, choose **Remote Server**.
     b. In the **Remote Server Name** field, choose a server.
     c. In the **Image Filename** field, choose an image.
6. Click **Save**.

Banner

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

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

Configure a Banner

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and click **Create Template.**

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Additional Templates** or scroll to the **Additional Templates** section.
6. From the **Banner** drop-down list, click **Create Template**. The **Banner** template form is displayed. This form contains fields for naming the template, and the fields for defining Banner parameters.
7. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

   When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the **Scope** drop-down list.

9. To set a banner, configure the following parameters:

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

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

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

CLI equivalent:

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

Create a Custom Banner

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

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

Collect Device Statistics

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

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

   By default, for every group of statistics (such as **Aggregated SAIE** and **AppHosting**), collection of statistics is enabled for all devices.
3. To enable the collection of a group of statistics for all devices, click **Enable All** for the particular group.
4. To disable the collection of a group of statistics for all devices, click **Disable All** for the particular group.

5. To enable the collection of a group of statistics for all devices only for consumption by Cisco SD-WAN Analytics, click **vAnalytics only** for the particular group.
6. To enable or disable the collection of a group of statistics for specific devices in the overlay network, click **Custom** for the particular group.

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

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

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

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

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

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

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

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

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

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

Configure the Time Interval to Collect Device Statistics

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. To modify the time interval at which device statistics are collected, click **Statistics Configuration**.
3. Enter the desired **Collection Interval** in minutes.
   - Default value: 30 minutes
   - Minimum value: 5 minutes
   - Maximum value: 180 minutes
4. To apply the modified settings, click **Save**.

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

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

Configure or Cancel Cisco SD-WAN Manager Server Maintenance Window

You can set or cancel the start and end times and the duration of the maintenance window for the Cisco SD-WAN Manager server.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Maintenance Window**. (If you are using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier, click **Maintenance Window** and then click **Edit**.)

   To cancel the maintenance window, click **Cancel**.
3. Click the **Start Date** and **Start Time** drop-down list. Select the date and time when the **Maintenance Window** will start.
4. Click the **End Date** and **EndTime** drop-down list. Select the date and time when the **Maintenance Window** will end.
5. Click **Save**. The start and end times and the duration of the maintenance window are displayed in the **Maintenance Window** bar.

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

Configure Basic System Parameters

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

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

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

Create System Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and click **Create Template**.

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. To create a custom template for System, select the **Factory_Default_System_Template** and click **Create Template**.

The System template form is displayed. This form contains fields for naming the template, and fields for defining the System parameters.

6. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Table 3:

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

Basic System-Wide Configuration

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

Table 4:

Parameter Field	Description
Site ID* (on routers, Cisco SD-WAN Manager instances, and Cisco SD-WAN Controller)	Enter the identifier of the site in the Cisco Catalyst SD-WAN overlay network domain in which the device resides, such as a branch, campus, or data center. The site ID must be the same for all Cisco Catalyst SD-WAN devices that reside in the same site.*Range:* 1 through 4294967295 ($2^{32} – 1$)

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

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

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

Configure the GPS Location

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

Table 5:

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

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

Configure Interface Trackers for NAT Direct Internet Access

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

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

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

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

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

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

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

Configure NAT DIA Tracker

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

Table 6:

Parameter Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Tracker Type	Choose an interface, static route.
Threshold	How long to wait for the probe to return a response before declaring that the transport interface is down. *Range:* 100 through 1000 milliseconds. *Default:* 300 milliseconds.
Interval	How often probes are sent to determine the status of the transport interface. *Range:* 10 through 600 seconds. *Default:* 60 seconds (1 minute)
Multiplier	Number of times to resend probes before declaring that the transport interface is down. *Range:* 1 through 10. *Default:* 3

Parameter Field	Description
End Point Type: IP Address	IP address of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. **Note** In Cisco SD-WAN Release 20.5.1 and later releases, if the tracker receives an HTTP response status code, which is less than 400, the endpoint is reachable. Prior to Cisco SD-WAN Release 20.5.1, the endpoint is reachable if the tracker receives an HTTP response status code of 200.
End Point Type: DNS Name	DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.

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

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

Configure NAT DIA Tracker Using the CLI

Configure NAT DIA tracker

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

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

Apply Tracker to an Interface

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

Monitor NAT DIA Endpoint Tracker Configuration

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

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

2. Choose a device from the list of devices.
3. Click **Real Time**.
4. From the **Device Options** drop-down list, choose **Endpoint Tracker Info**.

Configure Advanced Options

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

Table 7:

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

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

CLI equivalent:

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

   icmp-error-pps rate
```

```
idle-timeout seconds multicast-buffer-percent percentage

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

track-transport  upgrade-confirm minutes
```

Configure Global Parameters

Table 8: Feature History

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

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

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

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

To configure global settings using Cisco SD-WAN Manager:

1. Create a feature template to configure global settings.
2. Create a device template and include the Global Settings feature template.
3. (Recommended) Before applying the device template to a device, use the Preview Device Configuration and View Configuration Differences feature to review the differences between the configuration currently

on the device and the configuration to be sent to the device. This step is recommended because applying the device template overwrites the existing configuration on a device.

Limitations

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

Create Global Settings Feature Template

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

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

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

Parameter	Description
Services	
HTTP Server	Enable or disable HTTP server.
HTTPS Server	Enable or disable secure HTTPS server.
Passive FTP	Enable or disable passive FTP.
IP Domain-Lookup	Enable or disable domain name server (DNS) lookup.
Arp Proxy	Enable or disable proxy ARP.
RSH/RCP	Enable or disable remote shell (RSH) and remote copy (RCP) on the device.
Telnet (Outbound)	Enable or disable outbound telnet.
CDP	Enable or disable Cisco Discovery Protocol. Starting from Cisco SD-WAN 17.3 release, CDP on interfaces is enabled when the **cdp run** command is executed globally on Cisco ASR 1000 series devices.
Other Settings	
TCP Keepalives (In)	Enable or disable generation of keepalive timers when incoming network connections are idle.

Parameter	Description
TCP Keepalives (Out)	Enable or disable generation of keepalive timers when outgoing network connections are idle.
TCP Small Servers	Enable or disable small TCP servers (for example, ECHO).
UDP Small Servers	Enable or disable small UDP servers (for example, ECHO).
Console Logging	Enable or disable console logging. By default, the router sends all log messages to its console port.
IP Source Routing	Enable or disable IP source routing. IP source routing is a feature that enables the originator of a packet to specify the path for the packet to use to get to the destination.
VTY Line Logging	Enable or disable the device to display log messages to a VTY session in real time.
SNMP IFINDEX Persist	Enable or disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots.
Ignore BOOTP	Enable or disable BOOTP server. When enabled, the device listens for the bootp packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets.
NAT64	
UDP Timeout	NAT64 translation timeout for UDP Range: 1 to 65536 (seconds) Default: 300 seconds (5 minutes) **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default UDP Timeout value for NAT64 has been changed to 300 seconds (5 minutes).
TCP Timeout	NAT64 translation timeout for TCP Range: 1 to 65536 (seconds) Default: 3600 seconds (1 hour) **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default TCP Timeout value for NAT64 has been changed to 3600 seconds (1 hour).
HTTP Authentication	
HTTP Authentication	HTTP authentication mode Accepted values: Local, AAA Default: Local
SSH Version	

Parameter	Description
SSH version	Specify an SSH version. Default value: Version 2

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

CLI Equivalent

Services (enable):

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

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

Telnet outbound enable:

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

Services (disable):

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

Telnet outbound disable:

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

Other settings (enable):

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

```
    snmp-server ifindex persist
    ip bootp server
```

Other settings (disable):

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

NAT 64:

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

HTTP Authentication:

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

Configure NTP Servers Using Cisco SD-WAN Manager

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

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

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

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

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

Name the Template

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

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

3. From the **Create Template** drop-down list, choose **From Feature Template**.

4. From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.
5. Click **Basic Information**.
6. From **Additional Cisco System Templates**, click **NTP**.
7. From the **NTP** drop-down list, choose **Create Template**.

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

   The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default value or to enter a value, click the scope drop-down list to the left of the parameter field and select one of the following:

Table 9: Setting Parameter Scope

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Create a Template Variables Spreadsheet. 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.

Configure an NTP Server

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

Table 10: Parameters for Configuring an NTP Server

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

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

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

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

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

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

Configure NTP Authentication Keys

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

Table 11: Parameters for Configuring NTP Authentication Keys

Parameter Name	Description
Authentication Key ID*	Enter the following values: • Authentication Key: Enter an authentication key ID. Valid range is from 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**.

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

Table 12: Parameters for Configuring Trusted Keys

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

Configure a Router as an NTP Primary

Table 13: Feature History

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

You can configure one or more supported routers as an NTP primary router in a Cisco Catalyst SD-WAN deployment. A router that is configured in this way acts as the NTP server to which other nodes in the deployment synchronize their clocks.

Configuring a router as an NTP primary router is useful if you do not have an NTP server in your deployment.

To configure a router as an NTP primary router, you create a template that includes configured parameters for the NTP primary router. To do so, follow these steps:

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

2. Perform either of these actions:
   - To create a new template, under **Feature Templates**, click **Add Template**, choose the type of device to be the NTP primary router, and then choose the **NTP** template in the group of **Basic Information** templates.

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

   - To update an existing template, click **...**, and click **Edit**.

3. Configure options for the template as desired, and in the Master tab, perform these actions:
   a. For the Master option, choose **Global** from the drop-down list, and then choose **On**.
   b. (Optional) In the **Stratum** field, enter the stratum value for the NTP primary router.

      The stratum value defines the hierarchical distance of the router from its reference clock.

      Valid values: Integers 1 through 15. If you do not enter a value, the system uses the router internal clock default stratum value, which is 8.
   c. (Optional) In the **Source** field, enter the name of the exit interface for NTP communication.

      If configured, the system sends NTP traffic to this interface.

      For example, enter **GigabitEthernet1** or **Loopback0**.

4. Click **Save** (for a new template) or **Update** (for an existing template).

CLI equivalent:

```
ntp master [stratum-number]
ntp source source-interface
```

Configure NTP Servers for Cisco SD-WAN Control Components

Configure NTP Servers Using CLI Commands

Before You Begin

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

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

Configure NTP Servers for Cisco SD-WAN Control Components

1. Enter system configuration mode.

   system

2. Enter NTP configuration mode.

   ntp

3. Enter keys configuration mode.

   keys

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

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

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

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

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

6. Exit keys configuration mode.

   exit

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

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

Example

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

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

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

Configure Time using CLI

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

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

Configure GPS Using Cisco SD-WAN Manager

Use the GPS template for all Cisco cellular routers running Cisco Catalyst SD-WAN software.

For Cisco devices running Cisco Catalyst SD-WAN software, you can configure the GPS and National Marine Electronics Association (NMEA) streaming. You enable both these features to allow 4G LTE routers to obtain GPS coordinates.

Note You can configure GPS using Cisco SD-WAN Manager starting from the Cisco vManage Release 20.6.1 and onwards.

Device configuration using the CLI or a CLI template is available starting from the Cisco IOS XE Catalyst SD-WAN Release 17.6.1a only and onwards.

You can configure GPS using a Cisco SD-WAN Manager feature template. For geofencing to work, you need to configure GPS. To configure a GPS feature template, navigate to **Configuration** > **Templates** > **Feature Templates** > **GPS**.

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

For more information on geofencing, see Configure Geofencing.

Navigate to the Template Screen and Name the Template

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

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

3. Click **Create Template**.
4. From the **Create Template** drop-down list, choose **From Feature Template**.

5. From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.
6. Click **Cellular**.
7. In **Additional Cellular Controller Templates**, click **GPS**.
8. To create a custom template for GPS, click the **GPS** drop-down list and then click **Create Template**. The GPS template form is displayed. This form contains fields for naming the template, and fields for defining the GPS parameters.
9. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
10. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to **Default** (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list to the left of the parameter field and select either **Device Specific** or **Global**.

Configure GPS

To configure GPS parameters for the cellular router, configure the following parameters. Parameters marked with an asterisk are required to configure the GPS feature.

Table 14:

Parameter Name	Description
GPS	Click **On** to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: • **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.
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.

Parameter Name	Description
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.

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

Configure Automatic Bandwidth Detection

Table 15: Feature History

Feature Name	Release Information	Description
Day 0 WAN Interface Automatic Bandwidth Detection	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature enables a device to automatically determine the bandwidth for WAN interfaces in VPN0 during day 0 onboarding by performing a speed test using an iPerf3 server.

You can configure the Cisco VPN Interface Ethernet template to cause a device to automatically detect the bandwidth for WAN interfaces in VPN0 during its day 0 onboarding. If you configure a template in this way, a Cisco IOS XE Catalyst SD-WAN device attempts to determine the bandwidth for WAN interfaces in VPN0 after completing the PnP process.

Automated bandwidth detection can provide more accurate day 0 bandwidth configuration than manual configuration because there is limited user traffic that can affect results.

A device determines the bandwidth by performing a speed test using an iPerf3 server. iPerf3 is a third-party tool that provides active measurements of bandwidth on IP networks. For more information, see the Iperf.fr website.

If a device has a connection to the internet, the device uses a public iPerf3 server for automatic bandwidth detection, unless you specify a private iPerf3 server. If a device has a connection to a private circuit and no internet connection, you must specify a private iPerf3 server for automatic bandwidth detection.

We recommend that you specify a private iPerf3 server. If a private iPerf3 server is not specified, the device pings a system defined set of public iPerf3 servers and selects for the speed test the public server with the minimum hops value or, if all servers have the same minimum hops value, the server with the minimum latency value. If the speed test fails, the device selects another public server from the list. The device continues to select other public iPerf3 servers until the speed test is successful or until it has tried all servers. Therefore, a speed test on a public iPerf3 server can use a server that is far away, resulting in a larger latency than the minimum.

The set of system defined public iPerf3 servers includes the following:

- iperf.scottlinux.com
- iperf.he.net
- bouygues.iperf.fr
- ping.online.net

- iperf.biznetnetworks.com

The following settings on the Cisco SD-WAN Manager VPN Interface Ethernet template control bandwidth detection. These settings are supported for WAN interfaces in VPN0 only.

- **Auto Detect Bandwidth**—When enabled, the device detects the bandwidth.
- **Iperf Server**—To use a private iPerf3 server for automatic bandwidth detection, enter the IPv4 address of the private server. To use a public iPerf3 server for automatic bandwidth detection, leave this field blank.

  The private iPerf3 server should run on port 5201, which is the default iPerf3 port.

In addition, automatic bandwidth detection requires that the allow-service all command be configured for the tunnel interface. See "VPN, Interface, and Tunnel Configuration for WAN and LAN interfaces."

The device writes the results of a speed test to the auto_speedtest.json file in its bootflash directory. It also displays the results in the **Auto Upstream Bandwidth (bps)** and **Auto Downstream Bandwidth (Mbps)** areas on the **Monitor** > **Devices** > **Interface** page of Cisco SD-WAN Manager.

If a device does not receive a response from an iPerf3 server, an error is recorded in the auto_speedtest.json file and displays on the **Monitor** > **Devices** > **Interface** page of Cisco SD-WAN Manager.

Note In Cisco vManage Release 20.6.x and earlier releases, the speed test results are displayed on the **Monitor** > **Network** > **Interface** page.

CLI Equivalent

auto-bandwidth-detect

iperf-server *ipv4-address*

There also is a no auto-bandwidth-detect form of this command.

Example

```
Device# show sdwan running-config sdwan
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation gre
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
  auto-bandwidth-detect
  iperf-server 192.0.2.255
 exit
```

```
appqoe
 no tcpopt enable
 no dreopt enable
```

Configure System Logging Using CLI

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

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

SSH Terminal

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

Establish an SSH Session to a Device

To establish an SSH session to a device:

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

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

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

Table 16: Feature History

Feature Name	Release Information	Description
HTTP/HTTPS Proxy Server for Cisco SD-WAN Manager Communication with External Servers	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	Cisco SD-WAN Manager uses HTTP/HTTPS to access some web services and for some REST API calls. With this feature, you can channel the HTTP/HTTPS communication through an HTTP/HTTPS proxy server.
Cisco SD-WAN Manager HTTP/HTTPS Proxy Server Support Over IPv6	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can now configure an IPv6 address when configuring an HTTP/HTTPs proxy server.

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

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

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

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

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

- microsoftonline.com

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

Restrictions

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

Configure HTTP/HTTPS Proxy Server

Prerequisites

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

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

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

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

Note Cisco SD-WAN Manager uses TCP port 7 echo request to validate reachability of the proxy server. Ensure that you configure your firewall and proxy server to allow the echo requests to make the destination host ports accessible.

Cisco SD-WAN Manager verifies that the HTTP/HTTPS proxy server is reachable and saves the server details in the configuration database. HTTP/HTTPS connections and REST API calls to external servers are directed through the proxy server.

If the HTTP/HTTPS proxy server is not reachable, Cisco SD-WAN Manager displays an error message on the GUI indicating the reason for failure.

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

Table 17: Feature History

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

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

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

Configure Bulk API Rate Limit

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

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

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

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

   Enter **n**.

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

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

   Enter **y**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

View Bulk API Rate Limit

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

The following is a sample command output:

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

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