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 1: 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 2: 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 3: 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 4: 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 5: 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 6: 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 7:

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 8:

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 9:

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 20.

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 14 or Configure device basic system settings using templates, on page 16.

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 10: 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 11: 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 12: Authentication

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

d) Configure SSH.

Table 13: SSH Version

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

e) Configure other settings.

Table 14: 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 15: 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 16: 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 17: 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 18: 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 19: 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 20: 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 21: 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 39.

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 37.

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)
```