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 ; and creating network interfaces.

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

Host Properties

All devices have basic system-wide properties that specify information that the Cisco 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 vBond Orchestrator for the network domain, or a Domain Name System (DNS) name that resolves to one or more IP addresses for Cisco vBond Orchestrators. A Cisco vBond Orchestrator 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 vSmart Controllers to locate each other.

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

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

Time and NTP

The Cisco SD-WAN software implements the Network Time Protocol (NTP) to synchronize and coordinate time distribution across the Cisco 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 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 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 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 SD-WAN Release 20.5.1, 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 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. You can enable 802.1X on vEdge router interfaces to have the router act as an 802.1X authenticator, responsible for authorizing or denying access to network devices.

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 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 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 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 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 SD-WAN is achieved through VPNs on Cisco vEdge devices.

Network Interfaces

In the Cisco 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 SD-WAN devices use VRFs in place of VPNs. When you complete the configuration on Cisco vManage, 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.
- **VPN 512**: **Management VPN**, that carries out-of-band network management traffic among the Cisco 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 SD-WAN devices except for Cisco vEdge 100. For controller devices, by default, VPN 512 is not configured.
- **Service VPNs**: VPNs 1 through VPN 65535 except for VPN 0 and VPN 512. All service-side interfaces activated in these VPNs connect to a local or branch network that is generally located at the same site as the Cisco SD-WAN router. These interfaces carry data traffic throughout the overlay network.

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 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 vManage

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 SD-WAN network devices from Cisco vManage, which provides views of network-wide operations and device status, including detailed operational and status data. In addition, Cisco vManage 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 SD-WAN device. For a hardware vEdge router, you can also connect to the device's console port.

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

IPFIX

The IP Flow Information Export (IPFIX) protocol, also called cflowd, is a tool for monitoring the traffic flowing through Cisco 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 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 SD-WAN devices do not cache any of the records that are exported to a collector.

The Cisco 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 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 vManage or from the device's CLI.

RESTful API

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

The Cisco SD-WAN RESTful API calls expose the functionality of the Cisco 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 SD-WAN devices in the overlay network. The Cisco 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 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 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 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 SD-WAN device or to a remote host.

Cisco vManage

Cisco vManage is a centralized network management system that allows configuration and management of all the Cisco 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 vManage servers are consolidated into a Cisco vManage cluster to provide scalability and management support for up to 6,000 Cisco SD-WAN devices, to distribute Cisco vManage functions across multiple devices, and to provide redundancy of network management operations.

- Basic Settings for Cisco vManage, on page 5
- Configure Basic System Parameters, on page 12
- Configure Global Parameters, on page 21
- Configure NTP Servers Using Cisco vManage, on page 25
- Configure NTP using CLI , on page 28
- Configuring Time Using CLI on Cisco vEdge Device, on page 30
- Configure GPS Using CLI on Cisco vEdge Device, on page 30
- Configure System Logging, on page 31
- SSH Terminal, on page 40
- HTTP/HTTPS Proxy Server for Cisco vManage Communication with External Servers, on page 40
- Bulk API Rate Limit for a Cisco vManage Cluster, on page 42

Basic Settings for Cisco vManage

The System template is used to configure system-level Cisco vManage workflows.

Use the Settings screen to view the current settings and configure the setting for Cisco vManage parameters, including the organization name, vBond orchestrator's 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 vManage menu, choose **Administration** > **Settings**.
2. From **Organization Name**, 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 vBond orchestrator.
4. In **Confirm Organization Name**, re-enter and confirm your organization name.
5. Click **Save**.

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

Configure Cisco vBond DNS Name or IP Address

1. From **vBond**, click **Edit** .
2. In **vBond DNS/IP Address: Port**, enter the DNS name that points to the vBond orchestrator or the IP address of the Cisco vBond orchestrator 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 vBond Orchestrator IP addresses that DNS has to resolve, otherwise the control connection for Cisco vManage 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 vBond 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 vManage that you generate these certificates

and install them on the controller devices—Cisco vBond orchestrators,Cisco vManage, and Cisco vSmart 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 vManage 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 SD-WAN hosted service, you can enforce a version of the Cisco 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 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 vManage software image repository:
   a. From the Cisco vManage 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 vManage, Remote Server, or Remote Server - vManage.

   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 vManage menu, choose **Administration** > **Settings**.
3. From **Enforce Software Version (ZTP)**, click **Edit**.
4. In **Enforce Software Version**, click **Enabled**.
5. From the **Version** drop-down list, select the version of the software to enforce on the device when they join the network.
6. Click **Save**.

Banner

Use the Banner template for Cisco vBond Orchestrators, Cisco vManages, Cisco vSmart Controllers, Cisco vEdge devices, and s.

You can configure two different banner text strings, one to be displayed before the CLI login prompt on a Cisco SD-WAN device and the other to be displayed after a successful login to the device.

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

Configure a Banner

1. From the Cisco vManage 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 1: Parameters to be configured while setting a banner:

Parameter Name	Description
MOTD Banner	On a Cisco vEdge device enter message-of-the-day text to display after a successful login. 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 text | motd text}
```

Release Information

Introduced in Cisco vManage NMS in Release 15.2.

Create a Custom Banner

To create a custom banner that is displayed after you log in to the Cisco vManage:

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 vManage menu, choose **Administration** > **Settings**.
2. To modify the settings for collecting device statistics, click **Statistics Setting**, and click **Edit**.

   Tip To view the configured settings, click **View**.

   By default, for every group of statistics (such as **Aggregated DPI** 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 vAnalytics, 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 vManage menu, choose **Administration** > **Settings**.

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

Tip To view the configured time interval, click **View**.

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 vManage Server Maintenance Window

You can set or cancel the start and end times and the duration of the maintenance window for the vManage server.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. From **Maintenance Window**, click **Edit**.

   To cancel the maintenance window, click **Cancel**.
3. Click the **Start date and time** drop-down list, and select the date and time when the **Maintenance Window** will start.
4. Click the **End date and time** drop-down list, and 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 vManage Dashboard displays a maintenance window alert notification.

Configure Basic System Parameters

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

To configure system-wide parameters using Cisco vManage 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 vBond Orchestrator IP address on the Cisco vManage. These settings are appended to the device templates when the templates are pushed to devices.

Create System Template

1. From the Cisco vManage 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 2:

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 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 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.

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Basic System-Wide Configuration

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

Table 3:

Parameter Field	Description
Site ID* (on routers, vManage instances, and vSmart controllers)	Enter the identifier of the site in the Cisco 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 SD-WAN devices that reside in the same site.*Range:* 1 through 4294967295 ($2^{32} – 1$)
System IP*	Enter the system IP address for the Cisco 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 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 vSmart 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). *Default:* 115200 bps
Maximum OMP Sessions	Set the maximum number of OMP sessions that a router can establish to a Cisco vSmart Controller. *Range*: 0 through 100. *Default:* 2
Dedicated Core for TCP Optimization (optional, on vEdge 1000 and 2000 routers only)	Click **On** to carve out a separate CPU core to use for performing TCP optimization.

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

CLI equivalent:

```
 system
clock timezone timezone
 console-baud-rate rate
controller-group-list numbers
description text
device-groups group-name
host-name string
location string
max-omp-sessions  number
site-id site-id
system-ip ip-address
tcp-optimization-enabled
```

To configure the DNS name or IP address of the Cisco vBond Orchestrator in your overlay network, go to **Administration** > **Settings** screen and 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 vManage network map. Setting the location also allows Cisco vManage to send a notification if the device is moved to another location.

Table 4:

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**.

CLI equivalent:

```
system  gps-location  (latitude decimal-degrees | longitude decimal-degrees)
```

Configure Interface Trackers for NAT Direct Internet Access

Table 5: Feature History

Feature Name	Release Information	Description
Support for Interface Status Tracking on Cisco vEdge Devices	Cisco vManage Release 17.2.2	This feature supports interface tracking on Cisco vEdge devices.
Dual Endpoint Support for Interface Status Tracking on Cisco vEdge Devices	Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature allows you to configure tracker groups with dual endpoints using the **Cisco System** template and associate each template group to an interface. The dual endpoints provide redundancy for tracking the status of transport interfaces to avoid false negatives.

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.

Starting Cisco SD-WAN Release 20.6.1 you can configure a tracker group with dual endpoints on Cisco vEdge devices (using two trackers) and associate this tracker group to an interface. Dual endpoints help in avoiding false negatives that might be introduced regarding unavailability of the internal or external network.

Restrictions for Configuring Tracker Groups for Dual Endpoints

A tracker group with dual endpoints can only be configured on the following types of interfaces:

- Ethernet Interfaces
- Subinterfaces
- PPPoE Interfaces

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.

Parameter Field	Description
Tracker Type	Choose an interface, static route, or a tracker group. Starting Cisco SD-WAN Release 20.6.1 you can configure a tracker group with dual endpoints on Cisco vEdge devices and associate this tracker group to an interface. Choose **Tracker** type as **Interface** for NAT DIA and dual endpoint tracker configuration.
Tracker Type: Tracker Elements	This field is displayed only if you chose **Tracker Type** as a tracker-group. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers and you can then associate the tracker group to an interface.
Tracker Type: Tracker Boolean	This field is displayed only if you chose **Tracker Type** as a tracker-group. Select **AND** or **OR** explicitly. An **OR** operation ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group report that the interface is active. If you select the **AND** operation, the transport interface status is reported as active if both the associated trackers of the tracker group report that the interface is active.
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
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

```
system
   tracker tracker-name
   endpoint-dns-name dns-name
   endpoint-ip ip-address
   interval seconds
   multiplier number
   threshold milliseconds
```

Configure tracker group and assign it to an interface

Note You can configure only one endpoint per tracker.

```
system
 tracker nat-tracker1
  endpoint-ip 10.1.1.1
 !
 tracker nat-tracker2
  endpoint-ip 10.2.2.2
 !
 tracker nat-tracker3
  tracker-type tracker-group
  boolean or
  tracker-elements nat-tracker1 nat-tracker2
  !
 !
vpn 0
 interface ge0/1
  nat
  tracker nat-tracker3
  !
 !
```

Verify dual endpoints configuration

```
vEdge1# show running-config system | begin tracker

 tracker nat-tracker1
  endpoint-ip 10.1.1.1
 !
 tracker nat-tracker2
  endpoint-ip 10.2.2.2
 !
 tracker nat-tracker3
  boolean          or
  tracker-type     tracker-group
  tracker-elements nat-tracker1 nat-tracker2
 !

vEdge1# show tracker tracker-group

                                                                  TRACKER  TRACKER
                                                TRACKER           ELEMENT  ELEMENT
VPN  INTERFACE  TRACKER NAME  BOOLEAN  STATUS  ELEMENT NAME      STATUS   RTT
-------------------------------------------------------------------------------
```

```
0    ge0_1      nat-tracker3  or       DOWN    nat-tracker1  DOWN     Timeout
                                               nat-tracker2  DOWN     Timeout
```

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.

A tracker group with dual endpoints can only be configured on the following types of interfaces:

- Ethernet Interfaces
- Subinterfaces
- PPPoE Interfaces

Monitor NAT DIA Endpoint Tracker Configuration

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco vManage 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 **Dual 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
MTU of DTLS Tunnel	Specify the MTU size to use on the DTLS tunnels that send control traffic between Cisco SD-WAN devices. *Range:* 500 through 2000 bytes. *Default:* 1024 bytes
Port Hopping	Click **On** to enable port hopping, or click **Off** to disable it. When a Cisco 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 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 vManage devices and Cisco vSmart Controllers).

Parameter Name	Description
Port Offset	Enter a number by which to offset the base port number. Configure this option when multiple Cisco 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
DNS Cache Timeout	Specify when to time out the Cisco vBond Orchestrator addresses that have been cached by the device. *Range:* 1 through 30 minutes. *Default:* 30 minutes
Track Transport	Click **On** to regularly check whether the DTLS connection between the device and a Cisco vBond Orchestrator is up. Click **Off** to disable checking. By default, transport checking is enabled.
Local vBond (only on routers acting as vBond orchestrators)	Click **On** to configure the router to act as a Cisco vBond Orchestrator. Then specify the DNS name for the Cisco vBond Orchestrator or its IP address, in decimal four-part dotted notation.
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
Multicast Buffer	Specify the percentage of interface bandwidth that multicast traffic can use. *Range:* 5% through 100% *Default:* 20%
USB Controller (on vEdge 1000 and 2000 series routers only)	Click **On** to enable or click **Off** to disable the USB controller, which drives the external USB ports. If you enable the USB controller, the vEdge router reboots when you attach the device template to the device. *Default:* Disabled
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
Host Policer Rate (on vEdge routers only)	Specify the maximum rate at which a policer delivers packets to the control plane. *Range:* 1000 through 20000 pps. *Default:* 5000 pps
ICMP Error Rate (on vEdge routers only)	Specify how many ICMP error messages a policer can generate or receive. *Range:* 1 through 200 pps *Default:* 100 pps
Allow Same-Site Tunnel (on vEdge routers only)	Click **On** to allow tunnels to be formed between vEdge routers in the same site. Note that no BFD sessions are established between the two collocated vEdge routers. *Default:* Off
Route Consistency Check (on vEdge routers only)	Click **On** to check whether the IPv4 routes in the device's route and forwarding table are consistent.
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.

Parameter Name	Description
Eco-Friendly Mode (on vEdge Cloud routers only)	Click **On** to configure a Cloud router not to use its CPU minimally or not at all when the router is not processing any packets.

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 route-consistency-check
   system-tunnel-mtu bytes timer
    dns-cache-timeout minutes track-default-gateway
    track-interface-tag number

   track-transport  upgrade-confirm minutes [no] usb-controller (on Cisco vEdge 1000 and
Cisco vEdge2000 routers only)
   vbond  (dns-name | ip-address) local (on Cisco vEdge routers acting as Cisco vBond
controllers)
```

Release Information

Introduced in Cisco vManage in Release 15.2. In Releases 15.3.8 and 15.4.3, add Track Interface field. In Release 17.1.0, add Route Consistency Check and Collect Admin Tech on Reboot fields. In Release 17.2.0, add support for CLI idle timeout and eco-friendly mode. In Release 17.2.2, add support for interface status tracking.

Configure Global Parameters

Use the Global Settings template to configure a variety of global parameters for all Cisco IOS XE 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 vManage:

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

Create Global Settings Feature Template

1. From the Cisco vManage 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.

Parameter	Description
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	
Other Settings	
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.
NAT64	
UDP Timeout	NAT64 translation timeout for UDP Range: 1 to 65536 (seconds) Default: 300 seconds (5 minutes) **Note** Starting from Cisco IOS XE 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).

Parameter	Description
TCP Timeout	NAT64 translation timeout for TCP Range: 1 to 65536 (seconds) Default: 3600 seconds (1 hour) **Note** Starting from Cisco IOS XE 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	
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
```

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 vManage

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

Note For the NTP to properly function when using VPN0 on the Cisco vEdge 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 vManage 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 vManage 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 8: 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.

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

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 9: 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 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the **Trusted Keys** field, under **Authentication**(discussed below).
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 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**.

CLI equivalent:

```
system  ntp
   server (dns-server-address | ip-address)
     key key-id
     prefer
```

```
source-interface interface-name
version number
vpn vpn-id
```

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 10: Parameters for Configuring NTP Authentication Keys

Parameter Name	Description
Authentication Key ID*	Enter the following values: • Authentication Key: Enter an MD5 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 MD5 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 11: Parameters for Configuring Trusted Keys

Parameter Name	Description
Trusted Keys*	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 **Authentication Key ID** field under **Server**.

CLI equivalent:

```
system
 ntp
   keys
     authentication key-id md5 md5-key
     trusted key-id
```

Configure NTP using CLI

Configure Network-Wide Time with NTP

To coordinate and synchronize time across all devices in the Cisco SD-WAN overlay network, configure the IP address or DNS server address of an NTP server on each device. If necessary, specify the VPN through which the server is reachable.

```
vEdge(config)# system ntp server (dns-server-address | ipv4-address)
vEdge(config-system)# ntp server (dns-server-address | ipv4-address) vpnvpn-id
```

You can configure up to four NTP servers, and they must all be located or reachable in the same VPN. The software uses the server at the highest stratum level. If more than one server is at the same stratum level, you can configure the preference to use a specific server:

```
vEdge(config-ntp)# ntp
server  (dns-server-address | ipv4-address) prefer
```

You can configure an MD5 authentication key to use as a password to access an NTP server:

```
vEdge(config-system)# ntp keys
vEdge(config-keys)# authentication key-id md5 md5-key
```

key-id is a number that identifies the MD5 authentication key. It can be a number from 1 through 65535.

md5-key is the MD5 authentication key. You can enter it as cleartext or as an AES-encrypted key.

To use an MD5 authentication key for an NTP server, the key must be configured to be trusted:

```
vEdge(config-system)# ntp keys trusted key-id
```

Finally, associate the MD5 authentication key with the NTP time server:

```
vEdge(config-system)# ntp server (dns-server-address |ipv4-address) key key-id
```

You can configure NTP packets to exit from a specific interface on the router. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.

```
vEdge(config-system)# ntp server (dns-server-address | ipv4-address) source-interface
interface-name
```

The following example displays configuration three NTP servers. One of the NTP servers is at the NTP pool project at the Network Time Foundation and uses no authentication. The other two are internal servers and are configured with MD5 authentication:

```
vEdge# show running-config system ntp
system
 ntp
  keys
   authentication 1001 md5 $4$KXLzYT9k6M8zj4BgLEFXKw==
   authentication 1002 md5 $4$KXLzYTxk6M8zj4BgLEFXKw==
   authentication 1003 md5 $4$KXLzYT1k6M8zj4BgLEFXKw==
   trusted 1001 1002
  !
  server 192.168.15.243
   key     1001
   vpn     512
   version 4
  exit
  server 192.168.15.242
   key     1002
   vpn     512
   version 4
  exit
  server us.pool.ntp.org
   vpn     512
   version 4
  exit
 !
!
```

Configuring NTP on a Cisco SD-WAN device allows that device to contact NTP servers to synchronize time. Other devices are allowed to ask a for the time, but no devices are allowed to use the Cisco SD-WAN as an NTP server.

Configuring Time Using CLI on Cisco vEdge Device

Configure the Timezone

The default timezone on all Cisco vEdge devices is UTC.If your devices are located in multiple timezones (and even if they are not), we recommend that you use the default timezone, which is UTC, on all device so that the times in all logging and archive files are consistent.

To change the timezone on a device:

```
vEdge(config-system)# clock timezone timezone
```

Set the Time Locally

For Cisco vEdge devices that are part of a test or local network, you can set the time locally without using NTP because 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, and this time will be overwritten by the official NTP time once the device contacts the NTP server.

To set the local time and date, issue the following operational commands:

```
vEdge# clock set timehh:mm:ss[.sss]
vEdge# clock set date ccyy-mm-dd
```

You can also issue these commands as a single command:

```
vEdge# clock set date ccyy-mm-dd time hh:mm:ss[.sss]
```

or

```
vEdge# clock set time hh:mm:ss[.sss] date ccyy-mm-dd
```

To set the timezone, specify it in the configuration:

```
vEdge(config)# system clock timezone timezone
```

Configure GPS Using CLI on Cisco vEdge Device

Configuring geographic location for a device by setting its latitude and longitude allows the device to be placed properly on the Cisco vManage network map.

To set a device's latitude and longitude:

```
vEdge(config-system)# gps-location latitude degrees.minutes-and-seconds longitude
degrees.minutes-and-seconds
```

You can also set these values using two separate commands:

```
vEdge(config-system)# gps-location latitude degrees . minutes-and-seconds
vEdge(config-system)# gps-location longitude degrees . minutes-and-seconds
```

For example:

```
vEdge(config-system)# gps-location latitude 37.0000 longitude 122.0600
or
vEdge(config-system)# gps-location latitude 37.000
vEdge(config-system)# gps-location longitude 122.0600
vEdge(config-system)# show full-configuration
```

```
system
 host-name         vEdge
 gps-location latitude 36.972
 gps-location longitude 122.0263
 ...
```

You can also configure a text description of the device's location:

```
vEdge(config-system)# location "description of location"
```

For example:

```
vEdge(config-system)# location "UCSC in Santa Cruz, California"
vEdge(config-system)# show full-configuration
system
 host-name         vEdge
 location          "UCSC in Santa Cruz, California"
 gps-location latitude 37.0000
 gps-location longitude 122.0600
 ...
```

Configure System Logging

System logging operations use a mechanism similar to the UNIX syslog command to record system-wide, high-level operations that occur on Cisco SD-WAN devices in the overlay network. The log levels (priorities) of the messages are the same as standard UNIX commands, and you can configure the priority of syslog messages. Cisco SD-WAN devices can send log messages to a UNIX-style syslog service.

Cisco vEdge devices send syslog messages to syslog servers using UDP. TCP is not supported.

The syslog service accepts messages and stores them in files on the Cisco SD-WAN device or to a remote host.

Syslog Message Format, Syslog Message Levels, and System Log Files

Syslog Message Format

Syslog messages begin with a percent sign (%) and following are the syslog message formats:

- Syslog message format

  seq no:timestamp: %facility-severity-MENEMONIC:description (hostname-n)

The field descriptions of syslog messages are:

Table 12: Field Descriptions of Syslog Message Format

Field	Description
facility	Sets the logging facility to a value other than 20, which UNIX systems expect.
severity	The importance or severity of the message is categorized by the numerical code from 0 through 7. A lower number in this range indicates greater severity of the system condition.

Field	Description
description	A text string that describes the condition of syslog server. This portion of the syslog message sometimes includes IP addresses, interface names, port numbers, or usernames.

Usually, the syslog messages are preceded by extra text.

- The following is an example of a system logging message preceded by a priority value, sequence number, and time stamp:

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

Syslog Message Levels

All syslog messages are associated with priority levels that indicate the severity of syslog messages to save. The default priority value is "informational", so by default, all syslog messages are recorded. The priority level can be one of the following in order of decreasing severity:

- Emergency—System is unusable (corresponds to syslog severity 0).
- Alert—Ensure that you act immediately (corresponds to syslog severity 1).
- Critical—A serious condition (corresponds to syslog severity 2).
- Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3).
- Warning—A minor error condition (corresponds to syslog severity 4).
- Notice—A normal, but significant condition (corresponds to syslog severity 5).
- Informational—Routine condition (the default) (corresponds to syslog severity 6).

System Log Files

All syslog messages that are at or above the default or configured priority value are recorded in a number of files in the `/var/log` directory on the local device of the syslog server. The following are the contents of the log files:

- auth.log—Login, logout, and superuser access events, and usage of authorization systems
- kern.log—Kernel messages
- messages.log—Consolidated log file that contains syslog messages from all sources.
- vconfd.log—All configuration-related syslog messages
- vdebug.log—All debug messages for modules whose debugging is turned on and all syslog messages that are above the default priority value. The debug log messages support various levels of logging based on the module. The different modules implement the logging levels differently. For example, the system manager (sysmgr) has two logging levels (on and off), while the chassis manager (chmgr) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. Therefore, to enable debugging, use the **debug** operational command.

- vsyslog.log—All syslog messages from Cisco SD-WAN processes (daemons) that are above the configured priority value. The default priority value is "informational", so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages are saved.
- vmanage-syslog.log—Cisco vManage NMS Audit log messages

The following are the standard LINUX files that Cisco SD-WAN does not use and are available in the `/var/log` directory.

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

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

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

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

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

The maximum length of a log message for Cisco vManage NMS audit logs is 1024 bytes. The longer messages are truncated into smaller fragments and each of these fragments are indicated by an identifier. The identifiers are, fragment 1/2, fragment 2/2, and so on. For example, a long audit log message when truncated into smaller fragments appears as:

```
local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-1/2: {“logid”:
“d9ed576a-43ae-49ce-921b-a51c1ed40698”, “entry_time”:
1576605512190, “statcycletime” 34542398334245, “logmodule”:”maintenance”, “logfeature”:
“upgrade”, “loguser”: “admin”, “logusersrcip”:
“10.0.1.1”, “logmessage”: “Device validation Upgrade to version — Validation success”,
“logdeviceid”:”Validation”, “auditdetails” :
[“[18-Oct-2020 17:42:08 UTC] Published messages to vmanage(s)”, “auditdetails”:[“[18-Oct-2020
 17:42:07 UTC] Software image: vmanage-99.99.999-
x86_64.tar.gz”, “Software image download may take up to 60}

local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-2/2: { minutes”, “logprocessid”:
 “software_install-7de0ec44-d290-4429-b24532435324”, “tenant”:, “default”}
```

The syslog messages related to AAA authentication and Netconf CLI access and usage are placed in the auth.log and messages.log files. Each time a Cisco vManage NMS logs into a router to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. So, over time, these messages can fill the log files. To prevent these messages from filling the log files, you can

disable the logging of AAA and Netconf syslog messages by using the following commands from Cisco vManage NMS:

Disable logging of AAA and Netconf Syslog Messages

1. `vManage# config`

   Enters the configuration mode terminal

2. `vManage(config)# system aaa logs`

   Configures the logging of AAA and Netconf system logging (syslog) messages

3. `vManage(config-logs)# audit-disable`

   Disable logging of AAA events

4. `vManage(config-logs)# netconf-disable`

   Disable logging of Netconf events

5. `vManage(config-logs)# commit`

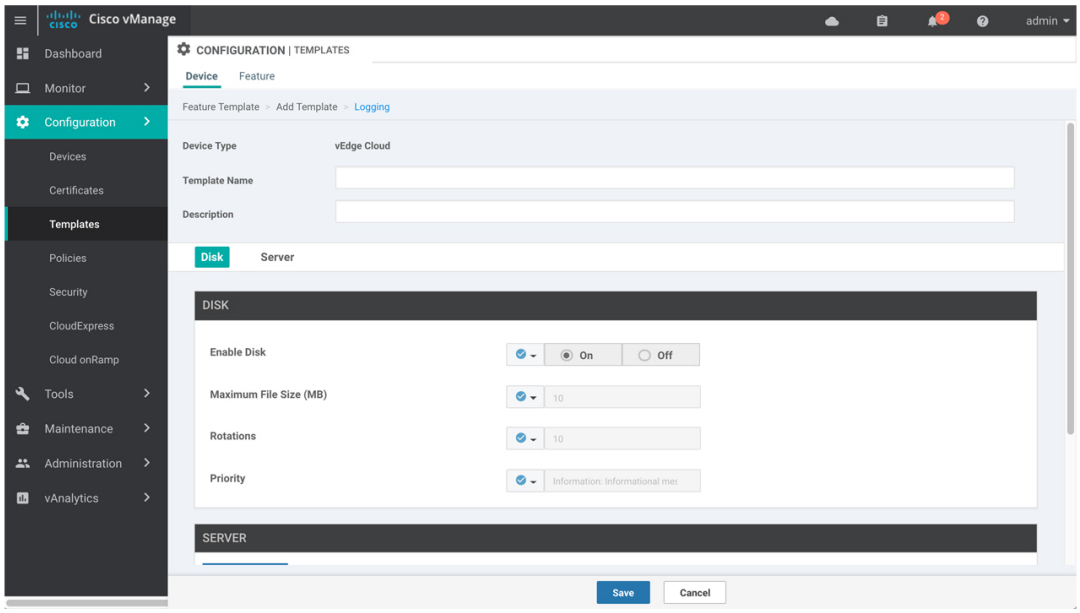
   Commit complete.

Configure Logging Using Cisco vManage

Use the Logging template for all Cisco SD-WANs to configure logging to either the local hard drive or a remote host.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the **Configuration ► Templates** screen.
2. In the **Device** tab, click **Create Template**.
3. From the **Create Template** drop-down, select **From Feature Template**.
4. From the **Device Model** drop-down, select the type of device for which you are creating the template.
5. To create a custom template for Logging, select the **Factory_Default_Logging_Template** and click **Create Template**. The Logging template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Logging parameters. You may need to click a tab or the plus sign (+) to display additional fields.



369421

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

Minimum Logging Configuration

The following logging parameters are configured by default:

- Log event notification system log (syslog) messages are logged to a file on the local device's hard disk, at a priority level of "information."
- Log files are placed in the directory /var/log on the local device.
- Log files are readable by the "admin" user.

Configure Logging to the Local Disk

To configure logging of event notification system log messages to the local device's hard disk, select the **Disk** tab and configure the following parameters:

Table 13:

Parameter Name	Description
Enable Disk	Click **On** to allow syslog messages to be saved in a file on the local hard disk, or click **Off** to disallow it. By default, logging to a local disk file is enabled on all Viptela devices.

Parameter Name	Description
Maximum File Size	Enter the maximum size of syslog files. Syslog files are rotated on an hourly basis based on the file's size. When the file size exceeds configured value, the file is rotated and the syslogd process is notified.*Range:* 1 through 20 MB*Default:* 10 MB
Rotations	Enter the number of syslog files to create before discarding the oldest files.*Range:* 1 through 10*Default:* 10
Priority	Select the priority level of the syslog message to save to the log files. The severity indicates the seriousness of the event that generated the message. The default priority value is "informational", so, by default, all syslog messages are recorded. The priority level can be one of the following (in order of decreasing severity): • Emergency—System is unusable (corresponds to syslog severity 0). • Alert— Action must be taken immediately (corresponds to syslog severity 1). • Critical—Critical: A serious condition (corresponds to syslog severity 2). • Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3). • Warning—A minor error condition (corresponds to syslog severity 4). • Notice—A normal, but significant condition (corresponds to syslog severity 5). • Informational—Routine condition (the default) (corresponds to syslog severity 6).

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

CLI equivalent:

```
system
 logging
    disk
     enable
     file
       rotate numbersize megabytes priority priority
```

Configure Logging to Remote Severs

To configure logging of event notification system log messages to a remote server, click the **Server** tab. Then click **Add New Server** and configure the following parameters:

Table 14:

Parameter Name	Description
Hostname/IP Address	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached.*Range:* 0 through 65530
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Parameter Name	Description
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. *priority* can be one of the following: • Emergency—System is unusable (corresponds to syslog severity 0). • Alert— Action must be taken immediately (corresponds to syslog severity 1). • Critical—Critical: A serious condition (corresponds to syslog severity 2). • Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3). • Warning—A minor error condition (corresponds to syslog severity 4). • Notice—A normal, but significant condition (corresponds to syslog severity 5). • Informational—Routine condition (the default) (corresponds to syslog severity 6). Click Add to save the logging server.

To edit a logging server, click the pencil icon to the right of the entry.

To remove a logging server, click the trash icon to the right of the entry.

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

CLI equivalent:

```
system
 logging
    server  (dns-name | hostname | ip-address)
     priority priority
     source-interface interface-name
     vpn vpn-id
```

Release Information

Introduced in Cisco vManage NMS in Release 15.2.

Export Cisco vManage NMS Audit Log to Syslog Server

Table 15: Feature History

Feature Name	Release Information	Description
Export vManage Audit Log as Syslog	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	The Cisco vManage NMS exports audit logs in syslog message format to a configured external syslog server. This feature allows you to consolidate and store network activity logs in a central location.

On Cisco IOS XE SD-WAN devices and Cisco vEdge devices, you can log event notification system log (syslog) messages to files on a local device, or to files on a remote host using CLI. These event notification logs are converted to system log files and exported to the syslog server. You can then retrieve system log information from the syslog server.

Configure System Logging Using CLI

Log Syslog Messages to a Local Device

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

1. **logging disk**

   Logs syslog messages on a hard disk

   Example:

   ```
   vm01(config-system)# logging disk
   ```

2. **enable**

   Enables logging to a disk

   Example:

   ```
   vm01(config-logging-disk)# enable
   ```

3. **file size** *size*

   Specifies the size of syslog files in megabytes (MB) By default, the syslog files are 10 MB. You can configure the size of syslog files to be 1–20 MB.

   Example:

   ```
   vm01(config-logging-disk)# file size 3
   ```

4. **file rotate** *number*

   Rotates syslog files on an hourly basis based on the size of the file By default, 10 syslog files are created. You can configure the rotate command to be a number from 1 through 10.

   Example:

   ```
   vm01(config-logging-disk)# file rotate 3
   ```

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

Log Syslog Messages to a Remote Device

To log event notification system log (syslog) messages to a remote host, use the following commands:

1. **logging server**

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

   Example:

   ```
   vm01(config-system)# logging server 192.168.0.1
   ```

2. (Optional) **vpn** *vpn-id*

   Specifies the VPN ID of the syslog server

3. (Optional) **source interface** *interface-name*

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

Example:

```
vm01(config-server-192.168.0.1)# source interface eth0
```

4. **priority** *priority*

   Specifies the severity of the syslog message to be saved. The default priority value is "informational" and by default, all syslog messages are recorded.

   Example:

   In the following example, set the syslog priority to log alert conditions.

   ```
   vm01(config-server-192.168.0.1)# priority alert
   ```

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

View System Logging Information

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

```
vm01(config-server-192.168.0.1)# show logging

System logging
    server 192.168.0.1
    source interface eth0
    exit
!
!
```

To view the contents of the syslog file, use the **show log** command. For example:

```
vm01(config-server-192.168.0.1)# show log nms/vmanage-syslog.log tail 10
```

To view the configured system logging settings from Cisco vManage, see Audit Log.

To view device-specific syslog files from Cisco vManage, perform the following steps:

1. From the Cisco vManage menu, choose **Administration** > **Settings**, and ensure that you enable **Data Stream**.
2. From the Cisco vManage menu, choose **Monitor** > **Devices**, and choose a Cisco vEdge device

   Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor** > **Network**, and choose a Cisco vEdge device.
3. Click **Troubleshooting**.
4. From **Logs**, click **Debug Log**.
5. From **Log Files**, select a name of the log file to view the log information.

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 vManage 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 vManage Communication with External Servers

Table 16: Feature History

Feature Name	Release Information	Description
HTTP/HTTPS Proxy Server for Cisco vManage Communication with External Servers	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	Cisco vManage 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.

The following are some instances in which Cisco vManage 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 vAnalytics

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 vManage instance. Beginning Cisco vManage 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 vManage checks whether the configured HTTP/HTTPS proxy server is reachable. If the proxy server is unreachable, Cisco vManage raises the alarm `HTTPS proxy server {IP} not reachable`.

Restrictions

- When configured to communicate with external servers via an HTTP/HTTPS proxy server, Cisco vManage resolves FQDNs locally or through configured DNS servers, bypassing the proxy server. Cisco vManage 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 vManage 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 vManage and external services.

Configure HTTP/HTTPS Proxy Server

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. For the **HTTP/HTTPS Proxy** setting, click **Edit**.
3. For the **Enable HTTP/HTTPS Proxy** setting, click **Enabled**.
4. Enter the **HTTP/HTTPS Proxy IP Address** and **Port** number.
5. Click **Save**.

Note Cisco vManage 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 vManage 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 vManage displays an error message on the GUI indicating the reason for failure.

Bulk API Rate Limit for a Cisco vManage Cluster

Table 17: Feature History

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