



System and Interfaces Overview

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

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, which provides a fixed location of the device in the overlay network. This address, whose function is similar to that of 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 each device's TLOC property.

A second host property that must be set on all devices is the IP address of the vBond orchestrator for the network domain, or a DNS name that resolves to one or more IP addresses for vBond orchestrators. The vBond orchestrator automatically orchestrates the bringup of the overlay network, admitting a new device into the overlay and providing the introductions that allow device and vSmart controllers to locate each other.

Two other system-wide host properties are required on all devices, except for the 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 Bringup* .

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 applicable time servers and avoid issues caused due to network latency. The servers also can 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 devices on the network. AAA, in combination with RADIUS and TACACS+ user authentication, controls which users are allowed access to devices and what operations they are authorized to perform once they are logged in or connected to the devices.

Authentication refers to the process by which the user trying to access the device is authenticated. To access devices, users log in with name and a password. The local device can authenticate users, or authentication can be performed by a remote device, either by a Remote Authentication Dial-In User Service (RADIUS) server or by a Terminal Access Controller Access-Control System (TACACS+), or by both in sequence.

Authorization determines whether the user is authorized to perform a given activity on the 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. External groups are also considered when performing authorization; that is, the Cisco SD-WAN software retrieves group names from RADIUS or TACACS+ servers. Each group is assigned privileges that authorize the group members to perform specific functions on the 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.

The Cisco SD-WAN software does not implement AAA accounting.

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.

IEEE 802.1X authentication requires three components:

- **Supplicant**—Client device, such as a laptop, that requests access to the 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, the 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 running authentication software that validates and authenticates supplicants 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 router and assigns the interface to a 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 prevents 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 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 either using preshared keys or through RADIUS authentication.

Network Segmentation

The Layer 3 network segmentation in Cisco SD-WAN is achieved through VRFs on Cisco IOS XE SD-WANs. When you configure the Network Segmentation on Cisco IOS XE SD-WAN device using Cisco vManage the system automatically maps the VPN configurations to VRF configurations.

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.

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



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.

- **VPN 0—Transport VPN**, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled. This is the global VRF on Cisco IOS XE SD-WAN software.
- **VPN 512—Management VPN**, which 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. For controller devices, by default, VPN 512 is not configured. On Cisco IOS XE SD-WAN device the management VPN is converted to VRF Mgmt-Intf.

For each network interface, you can configure a number of interface-specific properties, such as DHCP clients and servers, VRRP, interface MTU and speed, and 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 you can manage and monitor a router. Management interfaces provide access to devices in 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:

- Command-line interface (CLI)
- IP Flow Information Export (IPFIX)
- RESTful API
- SNMP
- System logging (syslog) messages
- vManage web server

CLI

You can access a command-line interface (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. While a CLI is available, it is strongly recommended that you configure and monitor all Cisco SD-WAN network devices from a Cisco vManage web server, which provides visual views of network-wide operations and device status, including drill-downs that display details operation and status data. In addition, the vManage web server provides straightforward tools for bringing up and configuring overlay network devices, including bulk operations for setting up multiple devices simultaneously.

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

For a Cisco SD-WAN device that is being managed by a vManage NMS, if you create or modify the configuration from the CLI, those changes are overwritten by the configuration that is stored in the 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 routers in the overlay network and exporting information about the traffic to a flow collector. The exported information is sent in template reports, which contain both information about the flow and data extracted from the IP headers of the packets in the flow.

The Cisco SD-WAN cflowd performs 1:1 traffic sampling. Information about all flows is aggregated in the cflowd records; flows are not sampled. Cisco SD-WAN routers 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 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 routers without configuring data policy so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN. You then monitor the traffic from the vManage GUI or from the router'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 access the RESTful API through the vManage web server.

The Cisco SD-WAN RESTful API calls expose the functionality of Cisco SD-WAN software and hardware features and of 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 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 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 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 which priority of syslog messages are logged. Messages can be logged to files on the Cisco SD-WAN device or to a remote host.

vManage NMS

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

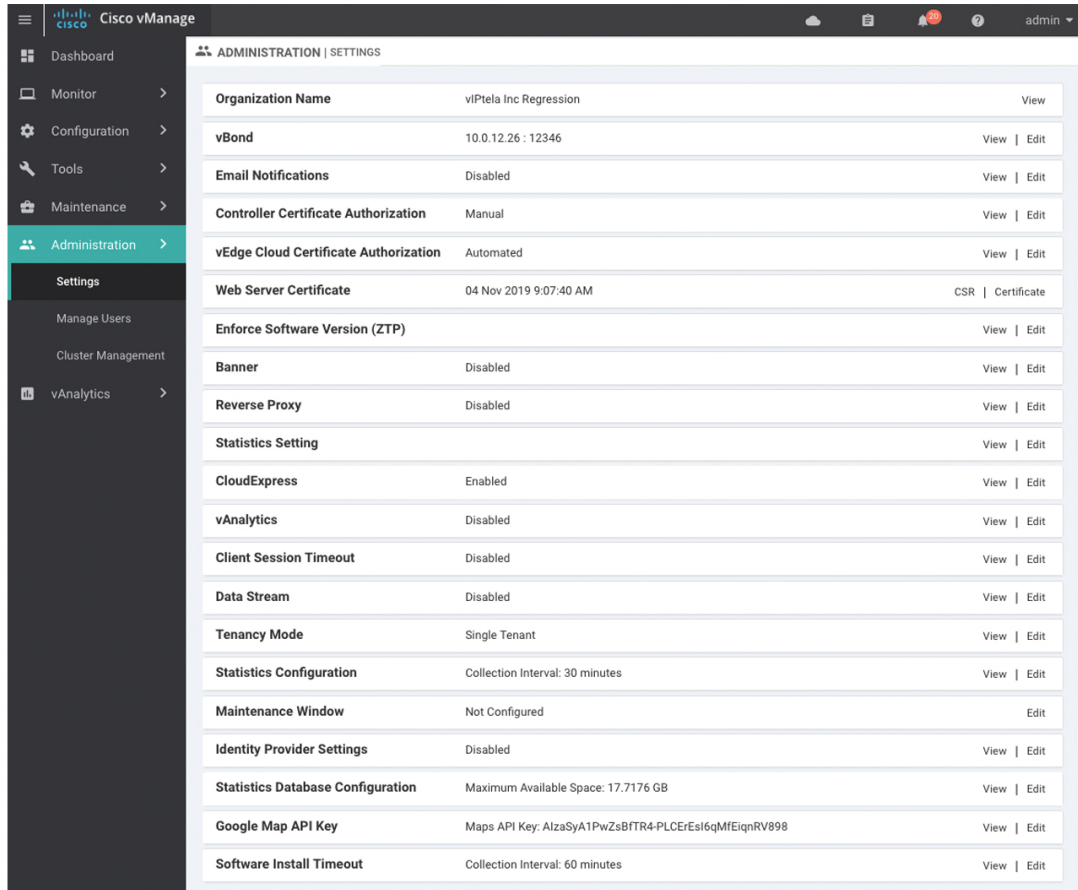
- [Basic Settings for Cisco vManage, on page 5](#)
- [Configure Basic System Parameters, on page 11](#)
- [Configure Global Parameters, on page 15](#)
- [Configure NTP using Cisco vManage, on page 18](#)
- [Configure NTP, on page 21](#)
- [Configure Time using CLI, on page 21](#)
- [Configure GPS Using Cisco vManage, on page 21](#)
- [Configure System Logging Using CLI, on page 22](#)
- [SSH Terminal, on page 23](#)
- [Tenant Management, on page 23](#)

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.



Setting	Value	Actions
Organization Name	vIPtela Inc Regression	View
vBond	10.0.12.26 : 12346	View Edit
Email Notifications	Disabled	View Edit
Controller Certificate Authorization	Manual	View Edit
vEdge Cloud Certificate Authorization	Automated	View Edit
Web Server Certificate	04 Nov 2019 9:07:40 AM	CSR Certificate
Enforce Software Version (ZTP)		View Edit
Banner	Disabled	View Edit
Reverse Proxy	Disabled	View Edit
Statistics Setting		View Edit
CloudExpress	Enabled	View Edit
vAnalytics	Disabled	View Edit
Client Session Timeout	Disabled	View Edit
Data Stream	Disabled	View Edit
Tenancy Mode	Single Tenant	View Edit
Statistics Configuration	Collection Interval: 30 minutes	View Edit
Maintenance Window	Not Configured	Edit
Identity Provider Settings	Disabled	View Edit
Statistics Database Configuration	Maximum Available Space: 17.7176 GB	View Edit
Google Map API Key	Maps API Key: AlzaSyA1PwZsBFTR4-PLCERes16qMfEiqnRV898	View Edit
Software Install Timeout	Collection Interval: 60 minutes	View Edit

368729

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. Click the **Edit** button to the right of the **Organization Name** bar.
2. In the **Organization Name** field, enter the name of your organization. The organization name must be identical to the name that is configured on the vBond orchestrator.
3. In the **Confirm Organization Name** field, re-enter and confirm your organization name.
4. Click **Save**.

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

Configure Cisco vBond DNS Name or IP Address

1. Click the **Edit** button to the right of the vBond bar.
2. In the vBond **DNS/IP Address: Port** field, 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**.

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. Click the **Edit** button to the right of the **Controller Certificate Authorization** bar.
2. Click **Symantec Automated** (Recommended). This is the recommended method for handling controller signed certificates.
3. In the **Confirm Certificate Authorization Change** popup, 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 requestor of the certificate.
5. Enter the email address of the requestor of the certificate. This address is required because the signed certificate and a confirmation email are sent to the requestor via email; they are also made available through 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 the Certificate **Retrieve Interval** field, 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. Click the **Edit** button to the right of the **Controller Certificate Authorization** bar.
2. Click **Symantec Manual**.

3. In the **Confirm Certificate Authorization Change** popup, click **Proceed** to manually install certificates that the Symantec signing server has generated and signed.
4. Click **Save**.

To use enterprise root certificates:

1. Click the **Edit** button to the right of the **Controller Certificate Authorization** bar.
2. Click **Enterprise Root Certificate**.
3. In the **Confirm Certificate Authorization Change** popup, 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 requestor.
 - 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 do so:

1. Ensure that the software image for the desired device software version is present in the vManage software image repository:
 - a. In Cisco vManage, select the **Maintenance > Software Repository** screen.
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. Click **Add** to play the image in the repository.
2. In the **Administration > Settings** screen, click the **Edit** button to the right of the Enforce Software Version (ZTP) bar.
3. In the **Enforce Software Version** field, click **Enabled**.
4. From the **Version** drop-down, select the version of the software to enforce on the device when they join the network.
5. Click **Save**.

If you enable this feature on the Cisco vManage, any device joining the network is configured with the version of the software specified in the **Enforce Software Version** field regardless of whether the device was running a higher or lower version of Cisco SD-WAN software.

Banner

Use the Banner template for Cisco vBond Orchestrators, Cisco vManages, Cisco vSmart Controllers, s, and Cisco IOS XE SD-WAN devices.

- 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, go to **Administration > Settings**.

Configure a Banner

1. In Cisco vManage, 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. Click the **Additional Templates** tab located directly beneath the Description field, or scroll to the **Additional Templates** section.
6. From the **Banner** drop-down, click **Create Template**. The **Banner** template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Banner parameters.
7. 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.
8. 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.

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 IOS XE SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type <code>\n</code> .
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 <code>\n</code> .

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

CLI equivalent:

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

Create a Custom Banner

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

1. Click the **Edit** button to the right of the Banner bar.
2. In the **Enable Banner** field, click **Enabled**.
3. In the **Banner Info** text box, 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

To enable or disable the collection of statistics for devices in the overlay network:

1. Click the **Edit** button to the right of the **Statistics Settings** bar. By default, all statistics collection settings are enabled for all Cisco SD-WAN devices.
2. To set statistics collection parameters for all devices in the network, click **Disable All** for the parameter you wish to disable statistics collection for. To return to the saved settings during an edit operation, click **Reset**. To return the saved settings to the factory-default settings, click **Restore Factory Default**.
3. To set statistics collection parameters for individual devices in the network, click **Custom** to select devices on which to enable or disable statistics collection. The **Select Devices** popup screen opens listing the hostname and device IP of all devices in the network. Select one or more devices from the **Enabled Devices** column on the left and click the arrow pointing right to move the device to the **Disabled Devices** column on the right. To move devices from the **Disabled Devices** to the **Enabled Devices** column, select one or more devices and click the arrow pointing left. To select all devices in the **Select Devices** popup screen, click the **Select All** checkbox in either window. Click **Done** when all selections are made.
4. Click **Save**.

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. In vManage NMS, select the **Administration > Settings** screen.
2. Click the **Edit** button to the right of the Maintenance Window bar.
To cancel the maintenance window, click **Cancel**.
3. Click the **Start date and time** drop-down, and select the date and time when the maintenance window will start.
4. Click the **End date and time** drop-down, 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 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 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 vManage NMS. These settings are appended to the device templates when the templates are pushed to devices.

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 System, select the **Factory_Default_System_Template** and click **Create Template**. The System template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining System parameters.
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 and select one of the following:

Table 2:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>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.</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

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 NMSs, 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. <i>Range:</i> 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 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. <i>Values:</i> 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps) <i>Default:</i> 115200 bps
Maximum OMP Sessions	Set the maximum number of OMP sessions that a router can establish to a vSmart controller. <i>Range:</i> 0 through 100 <i>Default:</i> 2

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

To configure the DNS name or IP address of the vBond orchestrator in your overlay network, go to the **Administration > Settings** screen and click **vBond**.

Configure Interface Trackers

To track the status of transport interfaces that connect to the internet, click the **Tracker** tab. Then click **Add New Tracker** and configure the following parameters:

Table 4:

Parameter Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Threshold	How long to wait for the probe to return a response before declaring that the transport interface is down. <i>Range:</i> 100 through 1000 milliseconds <i>Default:</i> 300 milliseconds

Parameter Field	Description
Interval	How often probes are sent to determine the status of the transport interface. <i>Range:</i> 10 through 600 seconds <i>Default:</i> 60 seconds (1 minute)
Multiplier	Number of times to resend probes before declaring that the transport interface is down. <i>Range:</i> 1 through 10 <i>Default:</i> 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. For each tracker, you must configure either one DNS name or one IP address.
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. For each tracker, you must configure either one DNS name or one IP address.

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

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

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.

Configure Advanced Options

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

Table 5:

Parameter Name	Description
Control Session Policer Rate	Specify a maximum rate of DTLS control session traffic, to police the flow of control traffic. <i>Range:</i> 1 through 65535 pps <i>Default:</i> 300 pps
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. <i>Default:</i> Enabled (on routers); disabled (on vManage NMSs and vSmart controllers)
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. <i>Values:</i> 0 through 19
Track Transport	Click On to regularly check whether the DTLS connection between the device and a vBond orchestrator is up. Click Off to disable checking. By default, transport checking is enabled

Parameter Name	Description
Track Interface	Set the tag string to include in routes associated with a network that is connected to a non-operational interface. <i>Range:</i> 1 through 4294967295
Gateway Tracking	Click On to enable or click Off to Disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the device's route table. <i>Default:</i> Enabled
Collect Admin Tech on Reboot	Click On to collect admin-tech information when the device reboots.
Idle Timeout	Set how long the CLI is inactive on a device before the user is logged out. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires. <i>Range:</i> 0 through 300 seconds <i>Default:</i> CLI session does not time out

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

CLI equivalent:

```

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

  icmp-error-pps rate

  idle-timeout seconds multicast-buffer-percent percentage

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

  track-transport upgrade-confirm minutes

```

Configure Global Parameters

Use the Global Settings template to configure global parameters for all Cisco SD-WAN devices.

To configure global settings using 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 View Configuration Differences feature to review the differences between the configuration currently on the device and the configuration to be sent to the device (overwriting its existing configuration).

Limitations

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

Create Global Settings Feature Template

1. In vManage, select **Configuration** (gear icon) ► **Templates**.
2. Click the **Feature** tab.
3. Click **Add Template**.
4. In the left pane, select a device type.
5. In the right pane, 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/disable HTTP server.
HTTPS Server	Enable/disable secure HTTPS server.
Passive FTP	Enable/disable passive FTP.
IP Domain-Lookup	Enable/disable domain name server (DNS) lookup.
Arp Proxy	Enable/disable proxy ARP.
RSH/RCP	Enable/disable remote shell (RSH) and remote copy (RCP) on the device.
Telnet (Outbound)	Enable/disable outbound telnet.
CDP	Enable/disable Cisco Discovery Protocol (CDP).
Other Settings	
TCP Keepalives (In)	Enable/disable generating keepalives on idle incoming network connections.
TCP Keepalives (Out)	Enable/disable generating keepalives on idle outgoing network connections.
TCP Small Servers	Enable/disable small TCP servers (for example, ECHO).
UDP Small Servers	Enable/disable small UDP servers (for example, ECHO).
Console Logging	Enable/disable console logging. By default, the router sends all log messages to its console port.
IP Source Routing	Enable/disable the originator of a packet to determine which path to use to get to the destination.

Parameter	Description
VTY Line Logging	Enable/disable the device to display log messages to a VTY session in real time.
SNMP IFINDEX Persist	Enable/disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots.
Ignore BOOTP	Enable/disable BOOTP server. This enables the device to listen for the bootp packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets.
NAT 64	
UDP Timeout	NAT64 translation timeout for UDP Range: 1 to 65536 (seconds)
TCP Timeout	NAT64 translation timeout for TCP Range: 1 to 65536 (seconds)
HTTP Authentication	
HTTP Authentication	HTTP authentication mode Possible values: Local, AAA

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

CLI Equivalent

Services:

```
[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
(Telnet outbound enable) line vty 0 4, transport input telnet ssh
(Telnet outbound disable) line vty 0 4, transport input ssh
[no] cdp run eable
```

Other settings:

```
[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:

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

HTTP Authentication:

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

Configure NTP using Cisco vManage

Configure network time protocol (NTP) servers on your devices in order to synchronize time across all 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 the Cisco SD-WAN device as an NTP server.

To configure NTP using Cisco vManage templates:

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

Navigate to the Template Screen and Name the Template

1. In Cisco 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. Select the **Basic Information** tab.
6. Under **Additional System Templates**, located to the right of the screen, click **NTP**.
7. From the **NTP** drop-down, click **Create Template**. The NTP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining NTP parameters.
8. 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.
9. 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 and select one of the following:

Table 6:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 Viptela device to a device template .</p> <p>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 Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

Configure NTP Servers

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

Table 7:

Parameter Name	Description
Hostname/IP Address*	Enter the IP address of an NTP server or of a DNS server that knows how to reach the NTP server.
Authentication Key*	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 the Authentication tab (discussed below).
VPN ID*	Enter the number of the VPN to use to reach the NTP server or the VPN in which the NTP server is located. If you configure multiple NTP servers, they must all be located or reachable in the same VPN. <i>Range: 0 through 65530</i>
Version*	Enter the version number of the NTP protocol software. <i>Range: 1 through 4</i> <i>Default: 4</i>
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.

Parameter Name	Description
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 with the highest stratum level.

To add the 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**.

Configure NTP Authentication

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

Table 8:

Parameter Name	Description
Authentication Key*	Select the following values: <ul style="list-style-type: none"> • Authentication Key—Enter an MD5 key ID. It can be a number from 1 through 65535. • Authentication Value—Enter either a cleartext key or an AES-encrypted key.
Authentication Value*	Enter an MD5 authentication key. For the key to be used, you must designate it as trusted. To associate a key with a server, enter the same value as you use for the the Authentication Key field on the Server tab.

To configure trusted keys used to authenticate NTP servers, in the Authentication tab, click the **Trusted Keys** tab and configure the following parameters;

Table 9:

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 as you use for the the Authentication Key field on the Server tab.

Configure NTP

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.

```
config-terminal
 ntp server 198.51.241.229 source GigabitEthernet1 version 4
```

Configure Time using CLI

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

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

Configure GPS Using Cisco vManage

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

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

Navigate to the Template Screen and Name the Template

1. In Cisco 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. Select the **Cellular** tab.
6. In **Additional Cellular Controller Templates**, click **GPS**.
7. To create a custom template for GPS, click the **GPS** drop-down and then click **Create Template**. The GPS template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining GPS parameters.
8. 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.
9. 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 and select either **Device Specific** or **Global**.

Configure GPS

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

Table 10:

Parameter Name	Description
GPS	Click On to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: <ul style="list-style-type: none"> • MS-based—Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, cell tower data is used to enhance the quality and precision in determining location, which is useful when satellite signals are poor. • Standalone—Use satellite information when determining position.
NMEA	Click On to enable the use of NMEA streams to help in determining position. NMEA streams data from the router's 4G LTE NIM to any marine device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address	Enter the IP address of the interface that connects to the router's NIM.
Destination Address	Enter the IP address of the marine NMEA server.
Destination Port	Enter the number of the port to use to send NMEA data to the server.

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

Release Information

Introduced in Cisco vManage Release 18.1.1.

Configure System Logging Using CLI

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

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

SSH Terminal

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

Establish an SSH Session to a Device

To establish an SSH session to a device:

1. From the left pane, select the device on which 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 on the device to select it.
2. Enter the username and password to log in to the device.

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

Tenant Management

Use the Tenant Management screen to add tenants to a Cisco vManage server that is operating in multitenant mode.

Add a Tenant

1. In the left pane, click the **Add Tenant** button.
2. In the **Add Tenant** window:
 - a. Enter a name for the tenant. It can be up to 128 characters and can contain only alphanumeric characters.
 - b. Enter a description for the tenant. It can be up to 256 characters and can contain only alphanumeric characters.
 - c. Enter the name of the organization. The name is case-sensitive. It is the name in the certificates for all Cisco SD-WAN network devices, and it must be identical on all devices in the overlay network.
 - d. In the URL subdomain field, enter the domain name for the tenant. The domain name must include the provider's domain name. You must also configure this same domain name when you enable multitenancy mode, in **vManage Administration > Settings > Tenancy Mode**
 - e. Click **Save**.
3. The Create Tenant screen is displayed, and the Status column shows In progress. To view status messages related to the creation of the tenant, click the > to the left of the status column. After about 1 minute, the Status column changes to Success, and the tenant table shows the tenant's system IP address.

View All Tenants

To view a summary of information about all tenants, in the center of the top bar, click the provider name.

View a Single Tenant

To view a summary of information about a single tenant:

1. In the center of the top bar, click the provider name.
2. In the table of tenants, click the tenant name. The summary information displays to the right of the name.
3. To hide the summary information, click the tenant name a second time.

To view the Cisco vManage dashboard for a single tenant:

1. In the center of the top bar, click **Select Tenant** to the right of the provider name.
2. Select the tenant name from the drop-down.

Edit a Tenant

1. In the left pane, click the name of the tenant.
2. In the right pane, click the Pencil icon to the right of the tenant's name.
3. In the **Edit Tenant** popup, modify the tenant's name, description, or domain name.
4. Click **Save**.

Remove a Tenant

1. In the left pane, click the name of the tenant.

2. In the right pane, click the **Trash** icon to the right of the tenant's name.
3. In the **Delete Tenant** popup, enter your Cisco vManage password and click **Save**.

